University of London Press
Institute of Advanced Legal Studies

Chapter Title: Electronic signatures
Chapter Author(s): Stephen Mason

Book Title: Electronic Evidence and Electronic Signatures
Book Editor(s): Stephen Mason, Daniel Seng
Published by: University of London Press, Institute of Advanced Legal Studies. (2021)
Stable URL: https://www.jstor.org/stable/j.ctv1vbd28p.14

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at https://about.jstor.org/terms

This book is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0). To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/.

University of London Press, Institute of Advanced Legal Studies are collaborating with JSTOR to digitize, preserve and extend access to *Electronic Evidence and Electronic Signatures*

JSTOR

www.manaraa.com

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7

Electronic signatures

Stephen Mason

The purpose of a signature

7.1 Legislation providing for electronic signatures has, essentially, been directed to provide for the authenticity of the person using the signature, although various statutes provide for additional uses, such as providing for the integrity of a message or document. Authentication can be the process by which a person or legal entity seeks to verify the validity or genuineness of a particular piece of information. Alternatively, it can mean the formal assertion of validity, such as the signing of a certificate: we authenticate what it certifies. In certain circumstances, there may also be a need to verify the identity of an individual or legal entity, although what is meant by 'identity' will also depend on the reason for ascertaining the identity. For example, with a cheque, the signature serves to link the name of the person printed on the cheque with the person who claims to have the authority to draw money from the account indicated on the cheque. In the past, the existence of the cheque guarantee card with a manuscript signature on the reverse served to reinforce the link between the card and the cheque, although the signature did not necessarily identify the person signing the cheque, even if the signature on the reverse of the cheque guarantee card matched the signature on the cheque. In cheque cases, the printed name on a cheque is not necessarily accepted as a form of signature, although it can contribute to authenticity. For instance, in *Ringham v Hackett*,[1] Lawton LJ considered the issue of authenticity in relation to a cheque with a name printed on it, and suggested that 'A printed name accompanied by a written signature was prima facie evidence that the cheque was being drawn on the account it purported to be drawn on',[2] although in the South African case of *Akasia Finance v Da Souza*,[3] Leveson J indicated, at 338 G–H, why he did not consider the name printed on the cheque could be a signature:

> At the foot of each cheque, where the signature of the drawer is normally to be found, appear the words, 'Domestic Homes (Pty) Ltd, Registration No 73/0541'. The words are printed and are plainly printed by machine.
>
> It is well known that for several years past banks have been issuing cheque books to their customers with the customer's name machine-printed thereon in the same space as the cheques in the present case. The printing is usually computer-controlled. This is done as part of a design to facilitate the modern banking system. Of importance is the fact that the printing is not done by the customer. It is therefore not the company's signature in the sense that, if put there by a person authorised by a corporate customer, it would constitute the company's signature or seal under the provisions of the Companies Act 61 of 1973.

1 [1980] 1 WLUK 323, (1980) 124 SJ 201, Times, 9 February 1980, [1980] CLY 158.

2 (1980) 124 SJ 201 at 202(a). In *Central Motors (Birmingham) v PA & SNP Wadsworth (trading as Pensagain)* [1982] 5 WLUK 265, [1983] CLY 6u, [1982] CAT 231, 28 May 1982; (1983) 133 NLJ 555, a

Stephen Mason, 'Electronic signatures', in Stephen Mason and Daniel Seng (eds.), *Electronic Evidence and Electronic Signatures* (5th edn, University of London 2021) 279–396.
This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

second account holder was held jointly liable for a cheque that he did not sign under the provisions of the Bills of Exchange Act 1882.
3 1993 (2) SA 337 (W).

7.2 The function of a signature is generally determined by the nature and content of the document to which it is affixed.

7.3 It is thought that the act of a person fixing their name to a document is well understood by lawyers and non-lawyers alike. However, a consideration of the case law demonstrates the range of issues that have arisen in relation to what seems, at first glance, a relatively simple concept. The means by which judges have tested the validity of a signature has altered over time. From concentrating on the form a signature takes, judges went on to question its validity by considering the function the signature performs.[1] The analysis in the move from form to function applies equally to the analysis of electronic signatures. The perceptive comments from the sound dissenting judgment of Bell J in 1855 in the South African case of *Van Vuuren v Van Vuuren*,[2] at 121, provides a useful summary with which to begin:

> the expression 'to sign' a document has no strict legal or technical meaning different from the popular meaning, viz., to authenticate by that which stands for or is intended to represent the name of the person who is to authenticate. If you say to the most illiterate person 'Sign this paper', if he cannot write, he will put a cross to it, and if he do not know how to do this the most experienced man of business cannot tell him to do more. If the party have learned a little writing, or if rheumatism of hard labour have cramped the nerves of his hand, and you ask him to sign a document, he will put the initial capital letters of his Christian and surname, while he will not venture upon writing the other more minute and therefore more difficult to be executed letters of these names, and he will feel satisfied that he has 'signed'. If the man of business doubt this, and, seeing he can write so far as to be able to make the capital letters, think it will not be sufficient without the smaller letters, and insist upon his making them, should the party say he cannot, the lawyer will be content. On the other hand, should the party make the attempt and produce a scrawl more or less legible, so again the man of business will be content – whether the scrawl be legible or illegible, he will be satisfied that the man has 'signed'. Such is the popular and professional practice, and the decision of the Courts had been conformably to it.

1 Chris Reed, 'What is a signature?' (2000) 3 *Journal of Information, Law and Technology (JILT)*, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/.
2 2 Searle 116.

Dictionary definitions

7.4 The *Oxford English Dictionary* offers a number of definitions of the word 'signature' as a noun and a verb.[1] The earliest references relate to signatures of a public nature that are intended to have legal effect. The first definition of a signature as a noun is that of 'A writing prepared and presented to the Baron of Exchequer by a writer to the signet, as the ground of a royal grant to the person in whose name it is presented'. An illustration for 1534 refers to 'To pass with writings and signaturis to be subscrivit be the Kingis grace'. The remaining references for this entry also relate to royal signatures in the public domain. The second and third definitions continue with the same meaning. Item 2(a) is defined as 'The name (or special mark) of a person written with his or her

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

own hand as an authentication of some document or writing', and is illustrated from Hollyband of 1580, referring to 'the signature or marke of a Notaries', with the next illustration from Coke dated 1633 referring to 'A bill superscribed with the signature or signe manuall, or royall hand of the King'. The third reference, item 2(b), 'The action of signing one's name, or of authenticating a document by doing so', is also illustrated by an early reference to Lord Keeper Williams from 1621: 'Some things wee must offer to the kings signature when the clarkes are not to bee found.' The law dictionaries vary in their treatment of the definition of 'signature'.[2]

1 *Oxford English Dictionary* (2nd edn on CD-ROM, version 4.0, 2009).
2 Bryan A. Gardner (ed), *Black's Law Dictionary* (11th edn, West Group 2019); Daniel Greenberg (ed), *Stroud's Judicial Dictionary of Words and Phrases* (11th edn, Sweet & Maxwell 2019); David Hay, *Words and Phrases Legally Defined* (5th edn, LexisNexis Butterworths 2018).

The manuscript signature

7.5 The epitome of a signature is the act of an individual writing their name in their own hand on a document, usually in the form of a manuscript signature.[1] More widely, it is the action of a person affixing a permanent imprint upon a document. In the world before the invention of electricity and computers, an imprint was required to have the characteristic of permanency because it was necessary to retain tangible evidence of intention. In addition, the parties to the document may consider it necessary to retain the evidence for a sufficient length of time in order to enforce any rights or obligations evidenced in the record.

1 Although the *tuğra* (a cipher or imperial monogram) of the Ottoman sultans that served as the signature of the sultan was drawn up by a court official and affixed to official documents. Over time, it was also carved on seals and stamped on coins, and artists illuminated later *tuğra*.

7.6 Before the development of the telegraph, a document would normally be considered something written onto a material, mainly paper. Although a number of people may be involved with the framing of a document and its subsequent manifestation in its final physical form, the document will have been created physically. Thus, if an instruction was passed from one party to another by means of the operators of semaphore, the sending operator could give evidence of the instructions received from the instructing party and the signals they used to transmit the message, and the receiving operator could give evidence of the signals they observed and noted down on paper. With the development of communications over the electric telegraph, the same principles would apply as with semaphore, but the electronic pulses of the telegraph would be interpreted in the light of the code used by the sending and receiving operators. The use of the telegraph meant that the message was encoded into electronic pulses, but the pulses were not stored. The receiving operator transferred the evidence of the message to a carrier. In contrast, software code transmits and stores the data in digital form, but the data are not visible to the human eye. A combination of the interpretation and use of hardware and software to make the data visible to the human are required.

7.7 In a world that relied on physical and permanent evidence of proof of intent, the requirement for an enduring record is understandable. While the legal consequences of a signature will differ when fixed to artefacts, such as items of pottery, paintings, sculpture and carvings on surfaces such as stone, marble, glass and wooden furniture,

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

nevertheless a signature is capable of establishing the identity of the creator of the article and is also capable of authenticating the provenance of the object.[1]

1 The copy of a painting with a false signature painted on it with the intention of passing off the painting as by the genuine painter was determined to be a cheat at common law by Cockburn LCJ and his fellow judges in *Regina v Thomas Closs* (1858) LRCCR 460, Dears & B 460.

7.8 A document usually exists on a carrier, typically paper. The carrier is marked permanently with content, usually with ink, either in the form of handwriting or by means of a printing press. This process alters the carrier physically. The content imprinted on the carrier may include a range of information, depending on the nature of the document, including information about the person who created, issued or initiated the content. Over time, the carrier will include additional information as it is handled, including coffee or tea stains, scratches, additional content, fingerprints and DNA. Finally, a person or legal entity might sign the carrier with a signature. The reason for signing the document will depend on the nature of the document and the purpose for which the person is signing. When brought together, these components comprise the document in its entirety.[1]

1 For the meaning of a 'document', see Stephen Mason, 'Documents signed or executed with electronic signatures in English law' [2018] 34(4) Computer Law and Security Report 933.

Statutory definition of signature

7.9 There does not appear to be a statutory definition of the term 'signature', and Ashman J commented in 1892 in a case regarding probate that there was no judicial formula either:[1]

> Exactly what constitutes a signature has never been reduced to a judicial formula … The principle upon which these cases proceeded was that whatever the testator of grantor was shown to have intended as his signature was a valid signing, no matter how imperfect or unfinished or fantastical or illegible, or even false, the separate characters or symbols he used might be, when critically judged.

1 Mitchell J quoted these comments of Ashman J (whose decision was reversed) in *In re Plate's Estate*, 148 Pa. 55, 23 A. 1038.

7.10 The Interpretation Act 1978 does not provide a definition, although Professor Reed noted there were 15 statutory definitions of 'signature' or 'signing' in force in 1996, 11 of which adopted an identical or similar variation to the following: ' "signature" includes a facsimile of a signature by whatever process reproduced'.[1] This particular definition is sufficiently general to include a representation of a signature in electronic form. The most obvious example is that of a manuscript signature that is scanned and converted into digital form. Such a representation can be attached to a document produced on a computer, or it could be the image of the signature as sent and received by a facsimile machine. It is estimated that there are in the region of 40,000 references to the requirement for a manuscript signature.[2] However, whether a personal signature is required depends upon the wording of the statute or from the context of the requirement.[3] With respect to legislation, Professor Reed notes that the statutory provisions relating to the provision of a signature fall into three broad categories:

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Where documents that have been signed are admissible in evidence, or create evidential presumptions. The evidential presumptions are either that the document is conclusive proof of its contents, or it is clear evidence of the facts set out in the document.

Where documents have to be signed for the purpose of authentication, either expressly or from the context of the requirement.

Where a signature is required to exercise a statutory power.[4]

1 Water Resources Act 1991 (c 57) Schedule 4, Part II, Proceedings of Flood Defence Committees, quoted in Chris Reed, *Digital Information Law: Electronic Documents and Requirement of Form* (Centre for Commercial Law Studies 1996) 225; table 5.1, 262–263 for the full list.
2 HC Official Report (6th series) col 41, 29 November 1999; note also Reed, *Digital Information Law*, 239 and n 41; Reed, 'What is a signature?', 3.1.2 and n 68.
3 Reed, *Digital Information Law*, 233–234 and nn 23 and 24.
4 Reed, *Digital Information Law*, 240–241. Professor Reed provides examples at 42–52.

The functions of a signature

7.11 A signature can serve a number of functions, each of which can have varying degrees of importance,[1] including complying with a legal requirement that something be signed.

1 Lon L. Fuller, 'Consideration and form' (1941) 42 Columbia Law Review 799 refers to the evidentiary, cautionary function and channelling functions; Ashbel G. Gulliver, 'Classification of gratuitous transfers (with Catherine J. Tilson)' (1941) 51 Yale Law Journal 1; John H. Langbein, 'Substantial compliance with the Wills Act' (1975) 88(3) Harvard Law Review 489; Mark Sneddon, 'Legislating to facilitate electronic signatures and records: exceptions, standards and the impact on the statute book' (1998) 21(2) University of New South Wales Law Journal 334 part 2 IIA (i)–(iv), http://www.austlii.edu.au/au/journals/UNSWLJ/1998/59.html; Adrian McCullagh, Peter Little and William Caelli, 'Electronic signatures: understand the past to develop the future' (1998) 21 University of New South Wales Law Journal 56; UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998 (United Nations 1999) paras 48 and 53; UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 (United Nations 2002) para 29; *Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods* (United Nations 2009) 1–8; for a similar overview of the same topic and discussion of the development of signatures, see Lorna Brazell, *Electronic Signatures and Identities Law and Regulation* (3rd edn, Sweet & Maxwell 2018) 2-001.

The primary evidential function

7.12 It is suggested that the primary purpose of a signature serves to provide admissible and reliable evidence that comprises the following elements:

(1) To provide tangible evidence that the signatory approves and adopts the contents of the document.

(2) In so doing, the signatory agrees that the content of the document is binding upon them and will have legal effect.

(3) Further, the signatory is reminded of the significance of the act and the need to act within the provisions of the document.

7.13 The nature of the act of signing differs between the application of a manuscript signature and the use of an electronic signature. This is because a manuscript signature, if authentic, is biologically linked to a specific individual, but cryptographic

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

authentication systems bind signatures to individuals by way of software code and procedural mechanisms.

7.14 With electronic signatures, the person does not physically sign anything, but causes software to sign electronically using an untrustworthy machine for knowing what document has been signed[1] – even when using a biodynamic version of a manuscript signature. This is significant, because the act of signing using an electronic signature has a different symbolic meaning to that of a manuscript signature, and suggests a weaker sense of the involvement of the person in the process of signing, as noted by Professor Chou.[2]

1 Stephen Mason and Timothy S. Reiniger, '"Trust" between machines? Establishing identity between humans and software code, or whether you know it is a dog, and if so, which dog?' (2015) 21 Computer and Telecommunications Law Review 135.

2 Eileen Y. Chou, 'Paperless and soulless: e-signatures diminish the signer's presence and decrease acceptance' (2015) 6 Social Psychological and Personality Science 343. Professor Chou provides further citations.

Secondary evidential functions

7.15 A signature can also provide evidence of identification and proof of the following:

> (1) The signature can authenticate the identity of the person signing the document. One example would be to reinforce the causal link between the signature and a name printed on a document, such as a name printed on a chequebook or credit card.
>
> (2) The identity of a particular characteristic, or attribute, or status of the person such as a government minister or company director.
>
> (3) Where a person signing acknowledges, verifies or witnesses the record, but does not necessarily agree to be bound by the content of the document.
>
> (4) The existence of the document provides a record of the intent of the signatory, and, in turn, physical evidence of the originality and completeness of the document itself, including the time, date and place of the act of the affixing of the signature to the document.
>
> (5) Where a person is a witness to the signing of a document, the signature of the witness can provide for the authenticity and the voluntary nature of the signature of a third party.
>
> (6) It can demonstrate that the content of the document has not been altered subsequent to the affixing of the signature.
>
> (7) A signature can provide evidence that the record is a true copy of another record.
>
> (8) A signature can be used to confirm the receipt of something, or to obtain access to something.

Cautionary function

7.16 This function acts to reinforce the legal nature of the document, thereby encouraging the person affixing their signature that they should take care before committing themselves to the contents of the document.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Protective function

7.17 As a corollary to the cautionary function, the party receiving the document containing a manuscript signature recognizes that the other party affirms the content of the document and they have given their full attention to the content of the document. They can also be assured of the identity of the signatory, and are consequently in receipt of the proof of the source and contents of the document. This function is linked to the evidentiary function.[1]

1 Sneddon, 'Legislating to facilitate electronic signatures and records', Part 2 IIA (ii).

Channelling function

7.18 The formality of a manuscript signature helps to clarify the point at which a person recognizes the act has become legally significant. Also, the content of the document, by being recorded on a durable form, serves to concentrate the mind on the legally binding nature of the document, thus reducing the risks associated with oral recollections. This function is also linked to the evidentiary function.

Record-keeping function

7.19 Closely related to the evidentiary function, a document contained on a carrier manifest in physical form serves as a durable record of the terms of the agreement. It also enables governments to impose taxes on documents and permit audits based on the existence of documents having a physical existence.

Disputing a manuscript signature

Defences

7.20 A manuscript signature cannot be disputed unless the following defences can be established: the signature is a forgery;[1] the signature was conditional; the signature was obtained as a result of misrepresentation; the signature was obtained in such a circumstance that it was not the act of the person signing (*non est factum*); mental incapacity; mistake; where one party unilaterally added material terms to the writing after the other had signed the document; where the person signing the document did not realize the document they signed was a contractual document; by statute as being unreasonable or unfair. These defences are not dealt with in this chapter, other than a brief consideration of the disputes where a manuscript signature has been at issue. The reader is referred to the standard textbooks on the subject. It is well known that manuscript signatures can be and are forged. To prevent this problem, and to test both the validity and the effectiveness of a manuscript signature, some documents require the signature to be affixed in the presence of a witness or an authorized official, such as a notary.

1 In the case of *Brown v National Westminster Bank Ltd* [1964] 2 Lloyd's Rep 187, [1964] 6 WLUK 133, [1964] CLY 191, the bank paid sums of money on 329 cheques that were alleged to contain forged copies of Mrs Brown's signature. The bank admitted to paying out on 100 cheques that were forged, but put Mrs Brown to prove that the remaining cheques were forged. This was because the bank took measures, through the branch managers, to question Mrs Brown on a number of cheques that passed through her account. Mrs Brown failed to prove that she did not sign the remaining cheques. For similar facts in Australia, see *Tina Motors Pty. Ltd. v Australia and New Zealand Banking Group Ltd.* [1977] VR 205.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Evidence of the manuscript signature

7.21 Where a manuscript signature on a document is challenged, evidence will need to demonstrate the issues discussed below. It should be noted that the evidentiary burden is a factor in considering the precise nature of the signature. In the Canadian case of *Regina v Blumes*,[1] the signature on a vehicle registration document, issued by the Insurance Corporation of British Columbia, was challenged. It was alleged that the document was not admissible because it was not clear whether the signature was a manuscript signature, a rubber stamp or a facsimile signature. This document was afforded the presumption of regularity, which meant that a mere challenge was not sufficient to avoid the operation of regularity.

1 2002 BCPC 0045.

The identity of the person affixing the manuscript signature

7.22 Evidence will have to be adduced to show the signature affixed to the document is that of the signatory. In such cases, the signature in question will have to be compared to samples of the same signature. A signature may be forged or the signature could be that of the signatory, but they may have attempted to disguise their handwriting. Thus a handwriting analyst[1] will need to have two kinds of sample: 'request samples' which are produced for the examination and duplicate the material in question; and naturally occurring samples, made by the signatory without realizing the example will be examined. Two main factors can then be examined, the first being that of pictorial impression, which includes matters such as slope, size, margins, spacing and the position of the writing in relation to lines. Second, the construction of the letters can be examined, such as the direction in which the letter 'o' is formed, the way the letter 't' is crossed and the way in which the person has written letters that require more than one movement. Forgers tend to concentrate on the pictorial impression and fail to copy details of the way letters are constructed. Likewise, people trying to disguise their handwriting also concentrate on the pictorial impression, rather than changing the formation of their letters.

1 Recent research has demonstrated that the findings of experts across all forensic disciplines can be subject to bias as the result of cognitive factors, such that the same expert has reached the opposite conclusion with the same evidence, for which see Itiel D. Dror, Christophe Champod, Glenn Langenburg, David Charlton, Heloise Hunt and Robert Rosenthal, 'Cognitive issues of fingerprint analysis: inter- and intra-expert consistency and the effect of a "target" comparison' (2011) 208 Forensic Science International 10 and the references cited therein. Apparently the US Secret Service uses a software program called Forensic Information System for Handwriting (FISH) that enables document examiners to scan and digitize text writings such as threatening correspondence; for a claim of a forged signature on a facsimile transmission, see *Diya v Halifax Plc* [2009] EWCA Civ 183, [2009] 1 WLUK 245; for an electronic signature that was used without authority and a manuscript signature that was forged, see *Jones v Hamilton* [2017] EWHC 1065 (Ch), [2017] 5 WLUK 385.

7.23 Further analysis can be undertaken by considering the relative proportions of letters, the spaces between letters and pressure variations. The attributes of the instrument used to affix the signature to the document can also be considered, such as how smoothly the signature has been written, whether it is jagged or confident, whether there is a pause and where the instrument lifts off the surface. Further, the carrier itself can be examined, from the type of material used (physical properties, optical properties), any security features (watermarks), the printing process used

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

(the use and identification of a photocopier, computer or printer) and other evidence such as perforations and microscopic analysis that might reveal imperfections that may link the carrier to the person. Further examination can include the comparison of typescript; impressions by means of Electrostatic Detection Apparatus; whether more than one type of material was used to affix information on the carrier; whether any alterations were made or entries obliterated, and the sequence in which intersecting lines have been written.

7.24 Where the party relying on the authenticity of the manuscript signature successfully demonstrates the similarity of the manuscript signature to the sample signatures, the evidential burden will then fall upon the alleged signatory to prove the signature was forged. Although this point was made in *Saunders v Anglia Building Society*[1] in relation to the defence where the signature was obtained in such circumstances that it was not the act of the person signing, the principle applies to a forged signature.

1 [1971] AC 1004, [1970] 3 WLR 1078, [1970] 3 All ER 961, [1970] 11 WLUK 45, (1971) 22 P & CR 300, (1970) 114 SJ 885, Times, 10 November 1970, [1971] CLY 1805; Dr Charles Y. C. Chew, 'Mistake in its variety of forms: the injustice of giving securities supporting financial institution debts on an error of judgement or without informed consent' (2017) 32(6) JIBLR 221.

Intention to authenticate and adopt the document

7.25 Where a person affixes their manuscript signature to a document, it must be shown that they intended to sign the document. The case of *L'Estrange v F Graucob Limited*,[1] which predates the modern legislation, serves to illustrate the point. In this case, Miss L'Estrange carried on the business of a café. The defendants manufactured and sold automatic slot machines. In early 1933, Miss L'Estrange agreed to buy an automatic slot machine for cigarettes for a total of £81 5*s* 6*d*, payable over 18 months. She signed a form, printed on brown paper, headed 'Sales Agreement'. This document included a number of contract terms written in very small print, one of which included 'This agreement contains all the terms and conditions under which I agree to purchase the machine specified above, and any express or implied condition, statement, or warranty, statutory or otherwise not stated herein is hereby excluded'. The machine was installed on 29 March 1933. However, it failed to work, and she eventually initiated an action in the county court to recover the payments she had made. Judgment was made in her favour. The decision was reversed in the Divisional Court because Miss L'Estrange had signed the written contract, and in doing so acknowledged that she was bound by the terms. There was no misrepresentation that induced her to sign. It was irrelevant that she did not read the contract or know its contents.[2]

1 [1934] 2 KB 394, [1934] 2 WLUK 22; J. R. Spencer, 'Signature, consent, and the rule in *L'Estrange v Graucob*' 32(1) CLJ 104, notes at 104 that this was not the first case in which the rule was laid down, although it was the case that made the rule famous; see *Parker v The South Eastern Railway Company* (1877) 2 CPD 416; *The Luna* [1920] P 22 and *Blay v Pollard and Morris* [1930] 1 KB 628.
2 This decision, and the discussion of a fourth defence, that the signatory did not agree to the term, is discussed in Spencer, 'Signature, consent, and the rule in *L'Estrange v Graucob*'.

7.26 This was not the case in *Pryor v Pryor*.[1] Anthony Pryor made a will on 5 November 1859. One of the attesting witnesses was his daughter. The testator wanted his daughter's husband to sign the will as a witness, but because it was not known when he would return, he asked his daughter to sign her husband's name instead of her own. She did

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

so. Sir C Creswell refused to admit the will to probate because the subscription was not intended to represent her signature.

1 (1860) LJR 29 NS P, M & A 114.

7.27 Although a manuscript signature on a document may not be in dispute, the person signing the document may wish the other party to infer they had the authority to sign the document, as in the case of *Ringham v Hackett*.[1] The presumption may be rebutted by evidence. In this case, the name printed on the cheque in *Ringham* was that of a partnership, and the signature by one of the partners on the cheque was deemed to be sufficient evidence to intend the recipient to infer the cheque was drawn on the partnership. In the case of *Central Motors (Birmingham) v PA & SNP Wadsworth (trading as Pensagain)*,[2] Central Motors required a cheque for the payment for a motor car in the name of the firm. In accordance with this request, Mr Wadsworth gave Central Motors a cheque with his signature beneath the name of the firm, which was printed on the cheque, below that of the names of the defendants. It was held that by handing over a cheque signed in this way, Mr Wadsworth provided sufficient evidence from the circumstances to personally authenticate the document as being a cheque of the firm. By signing the cheque, Mr Wadsworth had the requisite intent to adopt the cheque as that of the firm.

1 [1980] 1 WLUK 323 (1980), 124 SJ 201, Times, 9 February 1980, [1980] CLY 158.
2 [1982] 5 WLUK 265, [1983] CLY 6u, [1982] CAT 231, 28 May 1982, (1983) 133 NLJ 555.

The electronic signature

7.28 An electronic signature can perform the same functions as a manuscript signature.[1] The difference is that the document to be signed does not exist as a physical object in the same way as the content of a document rendered on to a paper carrier, which means the quality and extent of the evidence to provide intent becomes vitally important in the event it is disputed that an electronic signature was affixed to a document or communication, was not bypassed by a third party,[2] or was affixed to the relevant document in a batch of documents.[3]

1 If there is a specific requirement for a handwritten signature, a laser signature is not acceptable, for which in the context of the law in Saudi Arabia, see *Golden Belt 1 Sukuk Company BSC(c) v BNP Paribas* [2017] WLR(D) 822, [2017] EWHC 3182 (Comm), [2018] 3 All ER 113, [2018] 1 All ER (Comm) 1126, [2018] Bus LR 816, [2017] 12 WLUK 159, [2018] 1 BCLC 385, [2018] CLY 1736.
2 *Sell Your Car With Us Ltd v Sareen* [2019] EWHC 2332 (Ch), [2019] 9 WLUK 397 [2019] BCC 1211, [2020] 1 CL 112.
3 *FHG Publications Ltd v Tee-Hillman* [2001] 11 WLUK 642, [2001] CLY 662, where a single Statement of Truth was sent accompanying a batch of proceedings to be issued.

7.29 When a manuscript signature is affixed to a physical carrier, two changes occur. First, the signature alters the carrier physically with the addition of a substance, such as ink, to the surface. Second, the signature increases the amount of information about the carrier, and thereby the document. An electronic signature, on the other hand, only tends to alter the information relating to the digital data, including the metadata that can include and be taken automatically from the originating application software or supplied by the person who originally created the record. As a result, a digital record will normally contain two main types of information: the content of the document and

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

its internal structure, and the metadata, which describes the record and each of the constituent parts.

Forms of electronic signature

7.30 Electronic signatures are manifest in a variety of forms, all of which can demonstrate the intent of the signing party to authenticate the data. Unfortunately, the terms 'electronic signature' and 'digital signature' tend to be used interchangeably.[1] This creates confusion.[2] In essence, a digital signature is data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data to prove the source and integrity of the data unit. The digital signature mechanism defines two processes, that of the purported signing of a data unit by the person initiating the signature, which is a private action, and the verification of a signed data unit by using the procedures and information publicly available. A digital signature is a signature that is specifically based on asymmetric cryptography, coupled with a one-way hash function. It is a particular type of signature that is usually brought about by the use of a public key infrastructure[3] and is not a plain sequence of numbers.[4] It is often asserted that the digital signature provides a higher degree of certainty for the recipient. However, little attention is paid to illustrating the significant technical and legal obstacles to this assertion; that the verification process is opaque, or that a digital signature, as with other forms of signature, can be removed from a document in electronic form without trace,[5] and that a public key infrastructure provides for encryption, not the process of signing.

1 This is also pointed out in paragraph 2.2 of the Final Report of the European Electronic Signature Standardization Initiative Expert Team dated 20 July 1999 , and on page 16 of OECD, 'A Global Action Plan for Electronic Commerce Prepared by Business with Recommendations from Governments', 7–9 October 1998, Ottawa, Canada (Directorate for Science, Technology and Industry Steering Committee for the Preparation of the Ottawa Ministerial Conference, SG/EC(98)11/REV2); see also GUIDEC II, 'General Usage for International Digitally Ensured Commerce' for further discussion of the terms. GUIDEC II does not use the term 'electronic signature' but 'digital signature', thus adding to the confusion. In addition, the Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures, dated 12–23 March 2001 (A/CN.9/WG.IV/WP.88) also appears to refer to digital signatures and electronic signatures interchangeably: see paragraphs 31 to 62. Yet further confusion is rendered with the title of at least one legal textbook: D. Campbell (ed), *E-Commerce and the Law of Digital Signatures* (Oceana Publications 2005).

2 Also noted by Carlisle Adams and Steve Lloyd, *Understanding PKI Concepts, Standards, and Deployment Considerations* (2nd edn, Addison-Wesley 2002), 184–185.

3 See also paragraph 33 to UNCITRAL Model Law on Electronic Signatures, Guide to Enactment.

4 In *Ontario Workplace Safety and Insurance Appeals Tribunal* Decision No. 2877/07R 2008 ONWSIAT 3111 (CanLII), an NSR (a seven-digit number), where 'NSR' stands for 'no signature required', is incorrectly described as a digital signature. In *1475182 Ontario Inc. o/a Edges Contracting v Ghotbi* 2021 ONSC 3477 (CanLII), Boswell J incorrectly determined, at [50], that when text messages are exchanged without a name appearing at the end of the text message, that the unique telephone number linked to a cellular telephone, taken together with the International Mobile Equipment Identifier number 'provide, in effect, a digital signature on every message sent by the user of that particular device.'

5 Adrian McCullagh, William Caelli and Peter Little, 'Signature stripping: a digital dilemma' (2001) 1 Journal of Information, Law and Technology, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/mccullagh.

7.31 By comparison, the term 'electronic signature' is anything in electronic form that can be used to demonstrate a signing entity intended their signature to have legal effect. An electronic signature, especially when defined in legislation, tends to represent a generic response to the concept of authentication, and is to be understood in such

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

a context. A signature can be manifest in different forms,[1] and the term 'electronic signature' is used to reflect methods other than the use of a public key infrastructure to sign a message or document, such as the typing of a name on an electronic document, or the capture of the dynamics of a manuscript signature.

1 The use of 's/' instead of '/s/' when indicating the electronic signature of an attorney is irrelevant: Federal, 3rd Circuit, *Xu v Naqvi*, 537 Fed.Appx. 76 (2013), 112 A.F.T.R.2d 2013–6538, 2013–2 USTC P 50, 556.

7.32 For the sake of clarity, the term 'electronic signature' is used to denote the generic concept of a signature that is brought about by the use of a computer or computer-like device, and includes a digital signature as one form of electronic signature.[1] We should also be alert to new forms of electronic signature as they are developed and used.[2] However, this does not prevent the terms used to describe electronic signatures from adding to or increasing the confusion for failing to describe the form of electronic signature at issue. This is illustrated in the Zimbabwean case of *Tedco Mgmt Svcs (PVT) Ltd v Grain Marketing Board*,[3] in which an employee stole a total of $204,818.61 by adding the electronic signature of an authorized signatory to a series of cheques. The signatures were described as 'machine' signatures printed from the computer, which implies that the company caused authorized images of manuscript signatures to be scanned and stored on a computer.

1 In the British Columbia case of *Ghaed v Telus Communications Co.* 2013 Carswell BC 2727, 2013 BCSC 1675, [2013] BCWLD 8841, 234 ACWS (3d) 897, a digital signature is referred to, but it is debatable whether this particular form of signature was being used by Dr Ghaed, given his lack of technical knowledge.
2 Jillian Friedman, 'Signing your next deal with your Twitter @username: the legal uses of identity based cryptography' (2015) 13 Canadian Journal of Law and Technology 33.
3 1996 (1) ZLR 109 (SC).

Authority, delegation and ratification

7.33 A person can be delegated to sign a document, as in the Australian case of *Whittaker v Child Support Registrar*[1] where a person affixed the scanned electronic signature of another to a letter with authority.[2] In contrast, the New Zealand case of *Gong v Zhang*[3] provides an example of an electronic signature used without authority. When forms of electronic signature are placed on a hard drive in such a way that there is no mechanism to prevent others from using the electronic signature of another person, they are exposed to being used without authority, as in the Canadian case of *Adamo v College of Physicians and Surgeons of Ontario*,[4] where the electronic signature of another doctor was affixed to a falsified record without permission.[5]

1 [2010] FCA 43 (5 February 2010).
2 In *Athena Brands Ltd v Superdrug Stores Plc* [2019] EWHC 3503 (Comm), [2019] 12 WLUK 279, His Honour Judge David Cooke concluded that employees had the authority to bind their respective organizations in email exchanges.
3 [2014] NZHC 2838.
4 2007 CanLII 9873 (ON SCDC).
5 For allegations that a scanned image of a manuscript signature was 'photoshopped' on to documents, see *R&D Arts Inc. v Feld* 2013 Carswell BC 3153, 2013 BCSC 1896, [2013] BCWLD 9633, [2013] BCWLD 9767, 235 ACWS (3d) 501.

7.34 Depending on the facts, a person can ratify the signature. For instance, in a 2013 case the Supreme Court, New York County, New York concluded that where a personal assistant electronically signs a document for the purchase of property using dedicated

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

electronic signature software without explicit authority, the signature is capable of being ratified by the principal.[1]

1 *In the Matter of an Article 75 Proceeding ADHY Investments Properties, LLC, Petitioner v Garrison Lifestyle Pierce Hill LLC*, 41 Misc.3d 1211(A), 980 N.Y.S.2d 274, 2013 N.Y. Slip Op. 51634(U).

Forged signatures

7.35 The use of electronic signatures can facilitate the smooth running of an organization, but undue pressure can be placed on employees who fail to act as they ought. This was illustrated in the Canadian case of *Re: Jade Truman Kaiser Mason*,[1] where Mr Mason affixed the electronic signature of a customer to electronic documents without their knowledge, although it is not clear what form the electronic signature took in this case.

1 2012 CanLII 42180 (CA MFDAC); 2012 CanLII 42181 (CA MFDAC).

7.36 An early case where the PIN to a corporate bank account was used without authority occurred in the Australian employment case of *H. Sayner and Joblink Plus Limited – re Termination of employment*,[1] where Joblink had an electronic transfer policy which stated that a member of the Board must enter a code into the system when transferring funds electronically. The codes were written on a piece of paper, placed in a sealed envelope and left with the Finance Manager to store in a safe location and to be opened in an emergency. The envelope had a direction written on the outside to the effect that the envelope was not to be opened except in an emergency. Ms Sayner used the corporate PIN to pay for a holiday for the then Finance Manager Mr Helanath Disanayake and his family to the Novotel Opal Cove Resort at Coffs Harbour using Joblink funds in the amount of A$2,241.50. This expenditure was improper and not approved by the Board.

1 PR950280 [2004] AIRC 748 (30 July 2004).

7.37 Other examples of forgery include the Australian case of *Salfinger v Niugini Mining (Australia) Pty Ltd (No 3)*,[1] which concerned the falsification of purported assignments, and *Re Macartney and Tax Agents' Board of Victoria*,[2] where the applicant obtained a copy of the letterhead of the firm he was working for, together with an electronic signature of one of the partners of the firm. He then forged a statement of employment using the letterhead and electronic signature of the partner.[3] A further example of a falsified electronic signature in the context of employment is provided in the British Columbia case of *Caravel Management Corp. v Roberts*,[4] where a senior employee used the electronic signature of an authorized signatory to steal.

1 [2007] FCA 1532 (8 October 2007).
2 [2008] AATA 210.
3 See also *Djordje Mitic v Eco Pro Australia Pty Ltd* [2009] AIRC 503 (26 May 2009) and *Williams Group Australia Pty Ltd v Crocker* [2015] NSWSC 1907, upheld on appeal *Williams Group Australia Pty Ltd v Crocker* [2016] NSWCA 265.
4 2014 CarswellBC 2249, 2014 BCSC 1419, [2014] BCWLD 6492, [2014] BCWLD 6586, [2014] BCWLD 6591, [2014] BCWLD 6594, 243 ACWS (3d) 766.

Evidence of intent to sign

7.38 An issue that can exercise the minds of the adjudicator is how to determine the actual act that constitutes the acceptance by the sender of the electronic signature,

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

when the act occurred, and whether a person affixed their electronic signature in circumstances where they deny the signature was theirs.[1] In the case of a manuscript signature, the person furnishes evidence of their intent by physically writing on a carrier, and providing there is sufficient text to link the person to the document, the proof of intent is demonstrated.[2] The question of intent is illustrated in the New Zealand case of *MFT Properties Limited v Country Club Apartments Limited*,[3] which concerned negotiations by email. One email was signed 'Gary'. It was not in dispute that this referred to Mr Gary McNabb, the sole director of MFT. The issue was whether he was expressing a personal view during the course of negotiations or whether he was expressing an intention to bind MFT to the reduced rent it had been receiving. Woolford J concluded, at [39], that:

> The name 'Gary' sufficiently identifies Mr McNabb but I am of the view that it does not evidence his intention to bind MFT to the contents of the document.

1 Where a person denied the electronic signature was applied with their authority to a witness statement, see *Zurich Insurance Plc v Romaine* [2019] EWCA Civ 851, [2019] 1 WLR 5224, [2019] 5 WLUK 279, [2019] CLY 314.
2 For an example of the failure to prove an electronic signature, see the Californian case of *Rosas v Macy's, Inc.*, 2012 WL 3656274.
3 HC Auckland CIV-2010-404-005913 [2011] NZHC 422 (13 April 2011).

7.39 In the digital context, the moment of authentication may be when the person actually types in their name or adopts the signature text at the end of the email, or at the moment the signature is put in automatically when a new email is begun where the program is set up to include a signature at the end of the email.

The automatic inclusion of the signature

7.40 The problems with the automatic inclusion of the signature block in facsimile transmissions, email and SWIFT communications has caused some differences in opinion between judges.

Facsimile transmission

7.41 It is useful to consider the historical cases of facsimile transmission first. The practice of programming the machine to include automatically the name of the sender on the top or bottom of each page was challenged in the New York case of *Parma Tile Mosaic & Marble Co., Inc. v Estate of Fred Short, d/b/a Sime Construction Co*.[1] In this instance, it was held that the automatic imprinting by the facsimile machine of the name of the sender at the top of each page transmitted did not satisfy the requirement that writing shall be subscribed. The decision in this case remains arguable on the facts. Miller J reached the same conclusion in the New Zealand case of *Welsch v Gatchell*.[2] Having analysed a number of electronic signature cases, he said, at [63]:

> It follows from what I have said that a name written on a fax may amount to a signature. But a fax header printed using the machine's capacity to add writing to the document as it is copied and sent cannot serve as a signature unless, perhaps, there is evidence that is was specifically inserted for the transaction concerned. A fax header identifies the owner of the sending machine, the sending number and the time of despatch. There is no reason to suppose that it serves the added purpose of a signature, because every fax does not require a signature. And where the header is added automatically, it cannot qualify as a signature because

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> it was not affixed to the particular writing with the intention that by adding his or her name the sender would adopt its contents.

1 155 Misc.2d 950, 590 N.Y.S.2d 1019 (Supp. 1992), motion for summary judgment affirmed, 209 A.D.2d 495, 619 N.Y.S.2d 628, reversed 663 N.E.2d 633 (N.Y. 1996), 640 N.Y.S.2d 477 (Ct.App. 1996), 87 N.Y.2D 524; this case was treated negatively in *Rosenfeld v Zerneck*, 776 N.Y.S.2d 458 (Sup. 2004), 4 Misc.3d 194.

2 [2007] NZHC 1898, [2009] 1 NZLR 241, (2007) 8 NZCPR 708, (2007) 5 NZ ConvC 194,549 (21 June 2007).

7.42 In this case, a contract for the sale of land was formed orally and by facsimile. The sale of land requires the adoption of the contract by way of a signature. The document was not signed, which means there was no evidence to demonstrate an intent to be bound by the transaction, because the name and number printed automatically only acted to identify the person sending and receiving the document.

Email

7.43 An identical legal question arises in the case of email. A human directs the software to include the signature block in an email when it is sent. There is little difference between manually typing a signature block into a series of emails and typing the block once and instructing a computer program to append it to future messages. The difference between an email program and a facsimile transmission is that to remove the information in a facsimile transmission would mean resetting the machine. In the case of an email (and depending on how the email client works), it is usually possible for a person to delete or amend the signature block when writing a new email or when replying to an email.

7.44 This issue arose in *Neocleous v Rees*,[1] where the claimant sought specific performance of an alleged contract of compromise that involved a disposition of an interest in land. The defendant contended that the contract failed to comply with the formalities required by s 2 of the Law of Property (Miscellaneous Provisions) Act 1989, and was therefore not enforceable. The issue was whether the signature included in the automatic footer of an email was sufficient to bind a party. The judge said that to suggest the text included in an email automatically should be ignored is incorrect. This is because the content of the footer was created and added to the software in a conscious action at some stage by a person. In addition, the sender knew their name was added to every email. It was also observed that the recipient of the email is not able to ascertain whether the footer was added because of an automatic rule or by the sender manually entering the content. When considered objectively, the judge concluded that the presence of the name in the footer indicated a clear intention to associate the sender with the email – and to authenticate or sign it. His Honour Judge Pearce concluded that the email was signed, as set out at [57]:

> In my judgment, no such difficulty arises if the email footer here is treated as being a sufficient act of signing:
>
> i) It is common ground that such a footer can only be present because of a conscious decision to insert the contents, albeit that that decision may have been made the subject of a general rule that automatically applied the contents in all cases. The recipient of such an email would therefore naturally conclude that the sender's details had been included as a means of identifying the sender with the contents of the email, since such a footer must have been added either as a result of a conscious decision in the particular case or a more general decision to add the footer in all cases.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> ii) The sender of the email is aware that their name is being applied as a footer. The recipient has no reason to think that the presence of the name as a signature is unknown to the sender.
>
> iii) The use of the words "*Many Thanks*" before the footer shows an intention to connect the name with the contents of the email.
>
> iv) The presence of the name and contact details is in the conventional style of a signature, at the end of the document. That contrasts with the name and contact address of Mr Hale, the person alleged to have signed the letter in *Firstpost*, whose name and address appeared above the text of the letter, in the conventional manner of inserting the addressee's details.

1 [2019] EWHC 2462 (Ch), [2019] 9 WLUK 295, [2020] 2 P & CR 4, [2020] 1 P & CR DG8.

7.45 Approaching the question from the point of view of how the technology is set up is one way of helping to determine this particular issue. Arguably, if an organization authorizes an employee to insert the name, address and contact details of the legal entity into an email program, then it must be appropriate for the organization to put recipients on notice that they can or cannot use this information as a form of signature, or to prove intent, or that the recipient cannot rely on such information to bind the company for any legal purpose. When reaching judgments on such issues, it cannot be correct to ignore the way the technology is set up and used.

SWIFT communications

7.46 In Singapore in 2003, Tay Yong Kwang JC held in the case of *Industrial & Commercial Bank Ltd v Banco Ambrosiano Veneto SpA*[1] that a message using an authentication code sent through the SWIFT (Society for Worldwide Interbank Financial Telecommunication) system has the legal effect of binding the sender bank according to its contents, and where a recipient bank undertakes further checks on credit standing or other aspects, this does not detract from the proposition. In England, Blair J reached the same conclusion in *WS Tankship II BV v The Kwangju Bank Ltd*.[2] A guarantee was issued by Kwangju Bank, but the guarantee was not signed. Even the words 'Kwangju Bank' did not appear on it; the bank was referred to as 'we' in the guarantee. The case for the bank was that the guarantee was therefore not signed and the bank was not bound. Blair J rejected this argument at [154], because the bank accepted that the guarantee was properly issued, fully authorized and intended the beneficiary to rely on it. In addition, it was sent by conventional means by way of the secure messaging system used between banks – that is, using a digital signature – and the words 'Kwangju Bank Ltd' were contained in the header to the SWIFT message. Blair J continued, at [155]:

> It is argued on behalf of Kwangju Bank that this is not text which it typed in, but an output message header, that is, text generated by the SWIFT messaging system. That may be correct, but the name appears, and in my opinion it is a sufficient signature for the purposes of the Statute of Frauds. The words 'Kwangju Bank Ltd' appear in the header, because the bank caused them to be there by sending the message. They were 'voluntarily affixed' in the words of the old cases (c.f. *J Pereira Fernandes SA v Mehta* [2006] 1WLR 1543 dealing with email addresses). Whether or not automatically generated by the system, and whether or not stated in whole, or abbreviated (in fact the name of the bank appeared here in complete form), this is in my judgment a sufficient signature for the purposes of the Statute of Frauds. The position is analogous to that considered by Christopher Clarke J

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

in *Golden Ocean Group Ltd v Salgaocar Mining Industries Pvt Ltd* [2011] EWHC 56 (Comm) who at [103] observed that 'an email, the text of which begins "Paul/ Peter", may be regarded as signed by Peter because by that form of wording Peter signifies that he is addressing Paul and authenticates the content of the whole of what follows'. Therefore, I reject Kwangju Bank's submissions in this regard.

1 [2003] 1 SLR 221.
2 [2011] EWHC 3103 (Comm), [2011] 11 WLUK 729, [2012] CILL 3155.

7.47 One commentator who agrees with the decision in this case suggests it is arguable that the reasoning is wrong. Richard Bethell-Jones suggests that 'The automatic insertion of a name in a header is hardly something that any person (including a company) would regard as having the solemn authenticating properties of a "signature" '.[1] It is suggested that accepting this argument is to ignore the underlying rationale of the SWIFT system between banks.

1 Richard Bethell-Jones, 'Digital signatures and the statutory signature requirement', [2012] LMCLQ 184, 186.

Partial document with separate signature page

7.48 As technology is developed and used, so individuals will adjust their behaviour and adapt accordingly. It is undoubtedly the experience of many lawyers across the world that some clients will expect them to work at an impossibly fast pace when negotiating and entering into contractual relationships. The need for speed has increased significantly since the world became networked digitally. For this reason, contracts will be formed and real estate purchased solely relying on documents in digital form. In most cases, a document in digital form is a perfectly acceptable way of entering into legal relations. However, the digital environment often means that our concept of a 'document' has had to change.

7.49 Technically, there is only digital data, but for the purposes of this discussion, let us consider only documents on paper – thus we associate a contract as recorded on paper and signed with manuscript signatures on the relevant page. In developing the terms of a contract, the signature page is often left until the document is finished to the satisfaction of the parties. What then occurs will depend on the parties and the advice they receive from their lawyers. There are a number of options: the signature page is signed with the manuscript signature of each party who happen to be physically together; the signature page, containing a number of signatures for people across continents, is signed by each on a separate piece of paper and then scanned; perhaps each signatory appends a digital signature at different times to the document. Whatever method is used, it is highly likely that the document and the signature pages might well be separate documents.[1] In such circumstances, it then becomes necessary to undertake appropriate measures to prevent additional pages from being added to the agreement that have not been agreed, and for the signature pages, or signatures generally, to be properly associated with the agreement,[2] and for draft signature pages to be dealt with appropriately.[3] In Scotland, this particular issue is now dealt with by the Legal Writings (Counterparts and Delivery) (Scotland) Act 2015.[4]

1 Much as painters once signed the frame, not the painting, which makes attribution difficult, for which see Louise C. Matthew, 'The painter's presence: signatures in Venetian Renaissance pictures' (1998) 80(4) The Art Bulletin 616.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

2 In the context of a lease, see *Garguilo v Gershinon and Brooks* [2012] EWLandRA 2011_0377 and *Gopaul v Naidoo* [2014] EWHC 2684 (QB), [2014] 7 WLUK 1132 regarding the redevelopment of two properties by conversion into six flats.
3 For draft signatures, see *Mercury Tax Group Ltd, R (on the application of) v HM Commissioners of Revenue & Customs* [2008] EWHC 2721 (Admin), [2009] STC 743, [2008] 11 WLUK 303, [2009] Lloyd's Rep FC 135, [2009] BTC 3, [2008] STI 2670, [2009] CLY 3928; Mason, 'Documents signed or executed with electronic signatures in English law'; Law Commission, *Electronic Execution of Documents* (Law Com No 386, HC 2624, 2019).
4 Hector MacQueen and Charles Garland, 'Signatures in Scots law: form, effect, and burden of proof' (2015) Juridical Review 107.

7.50 Signing a blank document cannot be correct in criminal matters. Morse J rejected an 'e-ticket' in the New York case of *People of the State of New York v Rose*,[1] where computer-generated simplified traffic information and supporting depositions were generated by a device. At the time, the e-ticket was 'signed' before any information was placed on the ticket. This meant the arresting officer was essentially signing a blank document.

1 11 Misc.3d 200 (2005), 805 N.Y.S.2d 506, 2005 N.Y. Slip Op. 25526.

The Electronic Communications Act 2000

7.51 In England and Wales,[1] the first draft of a bill, the Electronic Communications Bill, was published in July 1999. This Bill was withdrawn when it attracted a great deal of wrath regarding key escrow (which is now expressly excluded in the Act by s 14) and provisions that were later incorporated into the Regulation of Investigatory Powers Act 2000. The Electronic Communications Act received the royal assent on 25 May 2000, and extends to Northern Ireland.[2] Sections 7, 11 and 12 came into force on 25 July 2000 in accordance with the provisions of the Electronic Communications Act 2000 (Commencement No 1) Order 2000 (SI 2000/1798); s 4(2) was amended by s 82, Schedule 4(10) of the Regulation of Investigatory Powers Act 2000, s 15(1) was amended by s 406(1), Schedule 17(158) of the Communications Act 2003, and ss 11 and 12 were repealed by s 406(7), Schedule 19(1) of the Communications Act 2003. The Act was amended in 2016 by The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (SI 2016/696),[3] and The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/89).[4] The Explanatory Memorandum to the Statutory Instrument[5] makes an unsubstantiated assertion at paragraph 7.3, third bullet point, dealing with a qualified electronic signature:

> It is considered to be sufficiently secure to withstand repudiation in a court of law.

1 For a discussion of the topic in an international context, see Stephen Mason, 'International initiatives and electronic signatures' (2012) 27(2) Computer and Telecommunications Law Review 37.
2 Section 16(5).
3 Made on 30 June 2016; laid before Parliament 1 July 2016; into force on 22 July 2016.
4 Made on 22 January 2019, laid before Parliament 23 January 2019, coming into force in accordance with regulation 1 (that is, on exit day).
5 http://www.legislation.gov.uk/uksi/2019/89/pdfs/uksiem_20190089_en.pdf.

7.52 For the purposes of justice, the legal profession is supposed to base decisions on evidence. No evidence is offered for this bare claim, and the source and empirical

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

basis of the assertion 'it is considered' is not provided. Furthermore, the discussion about computers and reliability in Chapter 5 is ignored. It is to be inferred that the government considers that this unproven declaration will be complied with in the same way as the presumption that a computer is reliable is also acted upon, in the absence of evidence and with lethargic indifference to the truth.

7.53 Unless there is a specific statutory requirement for a document to be signed, English law does not require any document to be signed to be both valid and effective. Thus, in many instances it was possible to sign a document with an electronic signature before the passing of the Act. The signature at the end of an email, as in the case of *Hall v Cognos Limited*,[1] was sufficient, providing the person signing the document intended to sign it and intended their signature to affect the authenticity of the document. If the identity of the person signing the document is in doubt, further evidence can be adduced to identify the person who affixed their signature to the document.

1 Hull Industrial Tribunal, 1997, Case No 1803325/97.

The definition of an electronic signature

7.54 The amended definition of an electronic signature[1] reads in s 7(2) as follows:

> (2) For the purposes of this section an electronic signature is so much of anything in electronic form as–
>
> (a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and
>
> (b) purports to be used by the individual creating it to sign.

1 Amended by The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (SI 2016 No 696) (made on 30 June 2016; laid before Parliament 1 July 2016; in force on 22 July 2016).

7.55 An electronic communication is defined in s 15(1):[1]

> 'electronic communication' means a communication transmitted (whether from one person to another, from one device to another or from a person to a device or vice versa) –
>
> (a) by means of an electronic communications network; or
>
> (b) by other means but while in an electronic form;

1 As amended by s 406(1), Schedule 17(158) of the Communications Act 2003.

7.56 An electronic signature does not have the same characteristics as a manuscript signature, but it is the equivalent of a manuscript signature when it performs a similar function. The better view is to consider an electronic signature as a link between protocols of electronic devices that communicate via software, each with the other. The attention should be focused on the treatment of messages before they are transmitted and after they are received – the owner or user may not be aware that the computer cannot be trusted.

7.57 An electronic signature can be the equivalent of a manuscript signature where it performs a similar function, even though the two types of signature are conceptually different. The manuscript signature exists in the corporeal world and requires the

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

physical application of matter to alter the surface of a carrier. An electronic signature can only be defined within the operational boundaries of the binary numbers used by computers.

The elements of an electronic signature

So much of anything in electronic form

7.58 This is a wide-ranging provision that should ensure new concepts yet to be invented are covered by the term 'electronic form'.

Incorporation or logical association

7.59 The first element, 'so much of anything in electronic form' must either be incorporated or logically associated with any electronic communication or electronic data. This part of the requirement differs slightly from article 3(10) of EU Regulation 910/2014,[1] which refers to 'attached to or logically associated with'. However, the meaning of the word 'attached' is defined as 'joined functionally', which implies a similarity to the meaning of 'incorporated', which in turn is defined as to 'be included as part of a whole' or 'embodied'.[2] This seems to be a semantic difference that does not affect meaning. The signature could be incorporated by reference to the way it is created. For instance, with a digital signature incorporation is possible when the software takes part of the plaintext and encrypts it (creating the message authentication code), so the recipient can check if the message has been altered. In effect, the message authentication code is a separate part of the message, but is also incorporated into the message by taking the message and encoding it. Alternatively, a biometric measurement can be attached to a message. This is where the biometric measurement, if used, must be logically associated with the message, otherwise it will not serve any function. Although the discussion above is predicated on particular methods of producing electronic signatures, the underlying principles are the same for all methods, including a name typed into an email or an email address, although the functions of an electronic signature may differ between products and methods.

1 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L257, 28.8.2014, 73; S. Mason, 'Electronic signatures and the EU legislation' (2020) 26(3) CTLR 73.

2 Oxford English Dictionary, 2nd edition on CD-ROM (v. 4.0).

Purports to be used by the individual creating it to sign

7.60 This revised sub-clause recognizes that it does not follow that where an electronic signature was affixed to data, the person whose signature it purports to be was the person who caused the signature to be affixed. In the context of the Act, the meaning of authenticity relates to the single issue of verifying the person or entity, as provided for in s 15(2):

> (2) In this Act–
>
> (a) references to the authenticity of any communication or data are references to any one or more of the following–

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> (i) whether the communication or data comes from a particular person or other source;
>
> (ii) whether it is accurately timed and dated;
>
> (iii) whether it is intended to have legal effect;
>
> (b) references to the integrity of any communication or data are references to whether there has been any tampering with or other modification of the communication or data.

7.61 This definition relates to the evidential issues regarding the authentication of the communication or data. Where an electronic signature is in issue, whichever party has the burden of proof will be required to submit evidence in response to the guidance set out in s 15(2), together with any other extrinsic evidence that may be necessary to support the evidential burden.[1]

1 Nicholas Bohm and Stephen Mason, 'Electronic signatures and reliance' (2018, Summer) 110 Amicus Curiae The Journal of the Society for Advanced Legal Studies 1.

7.62 An electronic signature will have to be admissible before it can become legally effective.[1] In addition, it does not follow that the communication will have a legal effect unless it is intended to have such an effect,[2] and the provisions of s 7 do not address whether the signature is genuine. Section 7(1) of the Act provides for the admissibility of the electronic signature in two ways:

> 7(1) In any legal proceedings–
>
> (a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and
>
> (b) the certification by any person of such a signature,
>
> shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data.

1 Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions Advice from the Law Commission* (2001), 3.27.
2 Section 15(2)(a)(iii).

7.63 First, an electronic signature is admissible under the provisions of s 7(1)(a) where it is incorporated into or logically associated with a particular electronic communication or data. Alternatively, in accordance with the provisions of s 7(1)(b), the authenticity or the integrity of the communication or data can be admissible where any person certifies the signature. The certificate would normally be provided by an entity such as a trusted third party, although it does not follow that such a certificate has to be provided by a trusted third party. For instance, it is perfectly possible for Bob to certify that Alice signed an email she sent when she typed her name at the bottom of the text. It seems, therefore, that if a recipient receives an electronic communication which is signed with an electronic signature, and the certifying certificate relating to the electronic signature can be verified, the communication in question is admissible in evidence, subject to the provisions of s 15(2) of the Act.[1]

1 It should be noted that all this evidence would have been admissible anyway, just as it has been in the past.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.64 The certification by any person mentioned in s 7(1)(b) is satisfactory if the statement made includes the criteria set out in s 7(3), as follows:

> (3) For the purposes of this section an electronic signature incorporated into or associated with a particular electronic communication or particular electronic data is certified by any person if that person (whether before or after the making of the communication) has made a statement confirming that–
>
> (a) the signature,
>
> (b) a means of producing, communicating or verifying the signature, or
>
> (c) a procedure applied to the signature,
>
> is (either alone or in combination with other factors) a valid means of establishing the authenticity of the communication or data, the integrity of the communication or data, or both.

7.65 The person or organization certifying the electronic signature may need to certify before or after, or both before and after, sending the communication that the signature is authentic and the integrity of the data or communication is therefore not to be questioned. From a practical point of view, the certification process will probably occur before the sending of the communication, although there may be circumstances where the certification process can occur after the communication is sent. The actual certification will probably be an assertion, which ought to be substantiated by suitable evidence, by the person or organization certifying the signature that there is an association that links the verification key (if a digital signature) with an entity, and certifies that the use of the verification key is a valid way of verifying whether a private key issued to the person named was used in creating the signature. The link between the components of the key pair, if this were to be challenged, would have to be the subject of expert evidence. It is possible for a certificate in isolation to be sufficient in some instances. In all probability, where a party seeks to adduce evidence of a certificate as establishing the authenticity or integrity of the communication or message or both, additional evidence may be required. Hence the addition of the phrase 'alone or in combination with other factors' in s 7(3). It is the provision of this extrinsic evidence that is necessary to provide evidence of the user's identity.

7.66 From a practical point of view, it may be difficult to obtain such evidence if the communication in question is the subject of legal action years after it was sent. Even if such a certificate is accepted as evidence of the facts contained in the certificate, it will not link the act of signing with the individual or entity whose signature it is. Whether the certification is provided electronically or physically, it may have to be the subject of proof that part of the content of the certificate is acceptable as to the truth of the content, because the information relating to the subscribing party will be a hearsay statement in relation to any facts not within the knowledge of the certification service provider. It should be noted that the provisions of s 7 do not consider whether the signature is genuine, or if it demonstrates the necessary intent by the signing party. In dealing with admissibility, the section leaves the question of evidential weight to the adjudicator.

Liability of a certification service provider

7.67 The British government has set out the extent of the liability that a certification service provider faces when they issue a key pair that conforms to the criteria of an

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

advanced electronic signature under the provisions of the Electronic Signatures Regulations 2002 (SI 2002/318), which came into force on 8 March 2002. The liability of a certification service provider is not dealt with in this text, but it is interesting to note that a certification service provider who issues a qualified certificate will be liable to the relying party unless it can be demonstrated that the provider was not negligent.[1] The burden of proof is reversed from the normal standard for negligence, where the person suffering loss is usually required to prove negligence. This leads to the possibility that organizations that decide to issue qualified certificates may seek an indemnity from the subscribing party against claims by a receiving party.

1 Regulations 4(1)(d) and 4(3)(d).

The power to modify legislation

7.68 There are many thousands of references in statutes and statutory instruments which require the use of paper or can be interpreted to require the use of paper, as well as the use of manuscript signatures. Amending such provisions with an overall catch-all clause was not possible, nor desirable. However, it is pertinent to observe a comment by the Law Commission in relation to this issue:

> While section 7 deals with admissibility, it does not provide that electronic signatures will satisfy a statutory signature requirement. It does not, therefore, assist in determining to what extent existing statutory signature requirements are capable of being satisfied electronically.[1]

1 Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions Advice from the Law Commission* (2001), 3.27.

7.69 Power has been delegated to Ministers to modify, by order made by statutory instrument, the provisions of any enactment or subordinate legislation, or instruments made under such legislation, for which they are responsible. The authority granted to Ministers is provided by s 8(1). Ministers have the power to modify by statutory instrument the provisions of:[1]

> (a) any enactment or subordinate legislation, or
>
> (b) any scheme, licence, authorisation or approval issued, granted or given by or under any enactment or subordinate legislation, in such manner as he may think fit for the purpose of authorising or facilitating the use of electronic communications or electronic storage (instead of other forms of communication or storage) for any purpose mentioned in subsection (2).

1 By s 8(7), matters under the care and control of the Commissioners of the Inland Revenue or Customs and Excise are not included, because there are corresponding powers in s 132 of the Finance Act 1999 which have already been exercised by way of statutory instruments relating to electronic tax and VAT returns.

Limitation of powers

7.70 The power granted to the Minister is limited by the terms of s 8(3), where consideration must be given to the arrangements for record-keeping. Changes must not be made that make the new arrangements for record-keeping less satisfactory than before the changes were made. A further limitation is set out in s 8(6), which provides that an order 'shall not require the use of electronic communications or

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

electronic storage for any purpose'. This subsection is qualified by s 8(6)(b), which permits a period of notice to expire before effect is given to a variation or withdrawal of an election or other decision.

Purposes for which modification can be made

7.71 Modification of an enactment can be made for the following purposes, by permitting the use of electronic means as follows:

> (a) The doing of things that may need to be evidenced in writing or where a document, notice or instrument is required.[1]
>
> (b) Alternative means of delivery where the post or other specified means of delivery is required.[2]
>
> (c) Where there is a requirement for a matter to be authorized by a person's signature or seal, or where it is required to be delivered as a deed or witnessed.[3]
>
> (d) Where a statement may be required to be made under oath or to be contained in a statutory declaration.[4]
>
> (e) Where records have to be kept, maintained or preserved in relation to any account, record, notice instrument or other document.[5]
>
> (f) The provision, production or publication relating to any information or other matter.[6]
>
> (g) The making of any payment.[7]

1 Section 8(2)(a).
2 Section 8(2)(b).
3 Section 8(2)(c).
4 Section 8(2)(d).
5 Section 8(2)(e).
6 Section 8(2)(f).
7 Section 8(2)(g).

The provisions a Minister may make

7.72 The Act provides the Minister with a power to provide for a range of issues when drafting a statutory instrument. The list is set out in s 8(4). The provisions of s 8(4)(g) cross refer to s 8(5). These two sections provide Ministers with the powers to determine such issues as matters relating to the legal presumption and the burden of proof. Section 8(4)(g) reads as follows:

> (g) provision, in relation to cases in which the use of electronic communications or electronic storage is so authorised, for the determination of any of the matters mentioned in subsection (5), or as to the manner in which they may be proved in legal proceedings.

7.73 Section 8(5) provides:

> (5) The matters referred to in subsection (4)(g) are–
>
> (a) whether a thing has been done using an electronic communication or electronic storage;
>
> (b) the time at which, or date on which, a thing done using any such communication or storage was done;
>
> (c) the place where a thing done using such communication or storage was done;

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

(d) the person by whom such a thing was done; and

(e) the contents, authenticity or integrity of any electronic data.

7.74 These two sections, taken together, indicate that a Minister has a great deal of control over how electronic communications are to be handled, and what presumptions will apply when using electronic communications. The combined effect of s 8(4) and s 8(5) permits a Minister to impose rebuttable or irrebuttable presumptions, with the potential for shifting the risks from the receiving party to the purported signing party. This has the potential for doing great injustice. Arguably, the power is wider than just replacing paper documents with an electronic equivalent. An example would be replacing the circulation of statutory accounts to shareholders by post or as attachments to an email, with an electronic notice of their availability at a nominated uniform resource locator.

7.75 The Electronic Communications Act 2000 has not altered the underlying flexibility of the meaning of a signature. An electronic signature does not have to be in the specific form of digital signature for it to be accepted as a signature. By typing a name on an electronic document, all the person needs to do is intend the name they type to act as a means of authentication, and intend the recipient to act upon the content of the document. The act of typing a name in this fashion comes within the provisions of s 7(2) of the Electronic Communications Act 2000, because the typed signature is incorporated with the content of the document for the purpose of establishing the authenticity of the communication.[1] No further requirements are necessary to make a typed signature admissible.

1 In *Golden Ocean Group Limited v Salgaocar Mining Industries PVT Ltd* [2011] EWHC 56 (Comm), [2011] 1 WLR 2575, [2011] 2 All ER (Comm) 95, [2011] 1 WLUK 356, [2011] 1 CLC 125, [2011] CILL 3022, [2011] CLY 3112, Mr Justice Christopher Clarke indicated at 103 that 'an email, the text of which begins "Paul/Peter", may be regarded as signed by Peter because by that form of wording Peter signifies that he is addressing Paul and authenticates the content of the whole of what follows'.

Regulation of Investigatory Powers Act 2000

7.76 The Regulation of Investigatory Powers Act 2000 (RIPA), which extends to Northern Ireland, received royal assent on 28 July 2000. For the purposes of this chapter, the powers relating to the disclosure of a key are relevant. The power to require disclosure is provided in s 49, but of importance is the meaning of a key. What constitutes a key is widely defined, and includes codes and passwords. The definition in s 56(1) is as follows:

> in relation to any electronic data, means any key, code, password, algorithm or other data the use of which (with or without other keys) –
>
> (a) allows access to the electronic data, or
>
> (b) facilitates the putting of data into an intelligible form

7.77 In the context of digital signatures, any person or organization that obtains and uses private keys should ensure the key is only suitable for the purposes of a digital signature, and it cannot be used for any other purpose.[1] If a key can be used for purposes other than a digital signature, it may be the subject of a s 49 notice. Also, it will be important to ensure keys used for digital signatures are stored separately from any other types of private key used for other purposes.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

1 It is possible for encrypted data to be encoded in such a way that it can be decoded in two separate ways, one to reveal the secret message and the other to reveal an innocuous message, for which see Derrick Grover, 'Dual encryption and plausible deniability' (2004) 20 Computer Law & Security Report 37.

Possession of a key

7.78 A person has possession of a key in accordance with the provisions of s 56(2). A person may be deemed to have a key, even they do not have the key. The definition is as follows:

> References in this Part to a person's having information (including a key to protected information) in his possession include references–
>
> (a) to its being in the possession of a person who is under his control so far as that information is concerned;
>
> (b) to his having an immediate right of access to it, or an immediate right to have it transmitted or otherwise supplied to him; and
>
> (c) to its being, or being contained in, anything which he or a person under his control is entitled, in exercise of any statutory power and without otherwise taking possession of it, to detain, inspect or search.

7.79 This is a fairly important provision, because the officers of an organization, whatever the legal form the organization takes, are the ones responsible for the proper management of the private key.[1] This is because any s 49 notice will be served on an officer or senior manager. Control must, therefore, be exercised over the acquisition and use of private keys. For instance, a person at the highest level in an organization should be made responsible for this issue. Considerations on whether to use private keys will cover, but not be limited to:

> (1) Deciding if information sent electronically needs to be encrypted. If it does, whether there are more appropriate means of delivering the information to the intended recipient.
>
> (2) Deciding if documents or messages need to be digitally signed. If so, then the next question is whether a risk analysis has been conducted to determine the likely costs of resolving a dispute if a signature has been misused, bearing in mind the discussion elsewhere in this chapter relating to liability.
>
> (3) If private keys are to be used, whatever the purpose, sufficient consideration must be given to storage, access for appropriately authorized officers and employees, and the provision of checks and balances to provide for security.

1 Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd edn, Wiley 2008), ch 25 for a discussion on the principles involved in this process. (Professor Anderson was updating his book as this text was being updated. Some of his book will be available as open source at https://www.cl.cam.ac.uk/~rja14/book.html for a short period before the text is published. The entire book will be made available again as open source in 2023.)

Exclusion of electronic signatures

7.80 Where a key is used only for the purpose of generating a digital signature, it does not have to be disclosed in response to a notice, providing it has not been used for any other purpose.[1] It might be useful to recall that a key pair has more than the single function of producing a digital signature. The same key pair can be used to encrypt

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

a message, depending on the algorithm used. An electronic signature is defined in s 56(2) as follows:

> anything in electronic form which–
>
> (a) is incorporated into or logically associated with, any electronic communication or other data;
>
> (b) is generated by the signatory or other source of the communication or data; and
>
> (c) is used for the purpose of facilitating, by means of a link between the signatory or other source and the communication or data, the establishment of the authenticity of the communication or data, the establishment of its integrity, or both;

1 Section 49(9).

7.81 This exemption may be less effective than it seems. In a commercial context, where more than one person may properly have access to a key, the person served with the notice may not be able to be sure that a key, despite being intended for signature purposes, has never been used to decrypt a message encrypted with the corresponding public key. Although it is arguably for the prosecution to prove that a key has been used for such a purpose, and is therefore subject to seizure, the mere assertion of this fact by the person demanding access to the key would place the recipient of the notice in a position of impossible difficulty in resisting the demand.

Electronic sound

7.82 It is possible to record sounds digitally when a person speaks to software code. In the USA, electronic signatures are defined by s 106(5) of the Electronic Signatures in Global and National Commerce Act, 106-229, which provides:

> Electronic signature. – The term 'electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

7.83 In the 2007 9th circuit case of *Shroyer v New Cingular Wireless Services, Inc.*,[1] a person indicated their assent, and thereby executed an electronic signature over the telephone, by selecting the answer 'Yes' in response to the statement 'You agree to the terms as stated in the Wireless Service Agreement and terms of service'. Although the judgment of the Court of Appeals did not explicitly indicate that this form of electronic signature is valid under the Act, nevertheless this decision is in keeping with the definition of electronic signature, and is a perfectly acceptable form of electronic signature.

1 498 F.3d 976.

7.84 In December 2007, the Court of Appeals in Kansas also reached a similar conclusion. In the case of *In the Matter of the Marriage of Takusagawa*,[1] the appellant argued that the provisions of the Kansas Statute of Frauds required a written signature where an agreement to the transfer of land was part of the divorce settlement. The trial judge approved the terms of an oral separation agreement on the final day of the

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

hearing, and the details of the agreement were put on the record. Both parties stated under oath that what was recorded by the court was their understanding of the terms of the agreement. The transcript indicated that the judge asked the appellant 'Ma'am, is that your understanding of the agreement?' The appellant replied 'Yes'.[2] It is certain that the appellant did not affix her manuscript signature to any document. The issue was whether the oral response to a judge was a form of signature. Leben J, who wrote the judgment of the court, cited the 1921 decision of the Supreme Court of Kansas in *Whitlow v Board of Education*,[3] in which the members of the school board voted at a meeting to sell some land. When the appellant handed over her cheque in payment and to complete the transaction, the members of the board refused to complete the sale. The minutes of the meeting indicated that a motion to sell the land to Josephine Whitlow was made and passed, and that the members of the board authorized the president of the board to sign a deed in exchange for payment. The Supreme Court of Kansas rejected the argument of the school board that the Statute of Frauds prevented the agreement being enforced because the minutes of the board had not been signed. It was determined that the minutes as recorded by the clerk were an authentic record that the law required the board to keep. In this respect, the minutes constituted a sufficient memorandum of the contract to bind the board under the Statute of Frauds. In this instance, a signature was not necessary where a public record was maintained by law, which in turn provided authentication of the formation and terms of the contract. The members of the court considered that a properly certified transcript of a court hearing was superior to the minutes recorded by the clerk to the school board, and found that a signature was not necessary where 'a court transcript providing the terms of the agreement and the oral assent of the party to be charged with the agreement that has been fairly stated on the record of the proceeding'.[4]

1 38 Kan.App.2d 401, 166 P.3d 440.
2 38 Kan.App.2d 401 at 410.
3 108 Kan. 604, 196 P. 772.
4 38 Kan.App.2d 401 at 409.

7.85 However, the discussion did not end at this point. Leben J then went on to consider the provisions of the Uniform Electronic Transactions Act K. S. A. 2006 Supp 16-1601, on the assumption that the transcript of the agreement was recorded on equipment that required electricity to enable it to work. Based on this assumption, the judge then considered s 16-1602(f), (h) and (i), which reads as follows:

> (f) 'Electronic' means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.
>
> …
>
> (h) 'Electronic record' means a record created, generated, sent, communicated, received or stored by electronic means.
>
> (i) 'Electronic signature' means an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

7.86 He concluded that where a party makes an oral statement in legal proceedings before a judge, and 'assuming that the court reporter's equipment was consistent with

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

modern practice, it would appear that the electronic capture of Mieko's oral assent that this was the agreement would satisfy the Statute of Frauds. No more is needed to show that Mieko made or adopted the agreement'.[1] This line of reasoning is far from convincing,[2] and arguably stretches the meaning of electronic signature beyond the terms of the statute.[3]

1 38 Kan.App.2d 401 at 410.

2 This decision was distinguished by the Court of Appeals of Kansas in *Ronald L. Jones Charitable Trust v Sanders*, 284 P.3d 375 (2012), 2012 WL 3966557 and *In re Estate of McLeish*, 49 Kan.App.2d 246, 307 P.3d 221 (Kan.App. 2013).

3 The same could be argued if a will is recorded on tape, and not written down, as in the case of *In the Matter of the Estate of Reed v Buckley*, 672 P.2d 829 (Wyo. 1983); in *Franklin County Cooperative v MFC Services (A.A.L.)*, 441 So.2d 1376 (Miss. 1983) it was determined by the Supreme Court of Mississippi that the statement 'OK, we will take care of it' made over the telephone had the capacity of proving intent to enter a contract when the words are subsequently written down in a memorandum.

7.87 The final claim to support the thesis that both parties entered into a binding agreement in court is more convincing: that an oral settlement placed on the record and acknowledged by the parties in open court should be sufficient to satisfy the requirement of the Statute of Frauds, especially because the law in Kansas allowed for oral separation agreements in divorce proceedings, and such agreements can be incorporated into the decree of divorce if approved by the judge.

7.88 Where one party to a conversation records what is said without the knowledge of the other party or parties, it does not follow that promises made, including a statement that might be construed as an electronic signature, will be valid. In the case of *Sawyer v Mills*,[1] heard at appeal before the Supreme Court of Kentucky, Barbara Sawyer and her husband recorded a conversation with Mr Mills in which he made promises to make certain payments. Among other things, it was determined that any contract formed during this conversation was not enforceable under the provision of the Statute of Frauds. Further, the court considered that the agreement by Mr Mills did not constitute an electronic signature just because it was identifiable and was identified at trial as being his. In explaining this in giving the opinion of the court, Nobel J said, at 8:

> There must be intent to attach or logically associate the electronic signature to the agreement, that is, an intent to execute the contract. That was impossible here, because the medium on which the alleged agreement and electronic signature were recorded (the audio tape) was used surreptitiously. Mills did not know he was being recorded when he went to the Sawyers' art studio. Thus, Mills's identifiable voice on the tape, even if construed as an electronic signature, was procured without Mills's knowledge or intent, and would be tantamount to a forgery which cannot be used to demonstrate a valid contract.

1 Ky., 295 S.W.3d 79.

7.89 Although the comments made by Mr Mills were capable of being construed as an electronic signature, the text of the statute envisages more than a mere spoken assent that is recorded in secret. The statute requires the electronic equivalent of a signature, that is, an electronic sound, symbol or process that demonstrates an intention to enter the agreement. Furthermore, the parties put the agreement into writing. Mr Mills refused to sign the written contract. This refusal to sign by Mr Mills demonstrated that he did not intend to execute or adopt anything he said in the conversation.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

The 'I accept' and 'wrap' methods of indicating intent

Click wrap

7.90 Clicking the 'I accept' or 'I agree' icon (also known as 'click wrap') to confirm the intention to enter a contract when buying goods or services electronically is now a very popular method of demonstrating intent. In the USA, the phrase 'wrap' has become common. The action of clicking an icon is capable of providing evidence of the process that is executed or adopted by the person clicking on the icon – that is, the user is required to undertake a positive activity.[1] This is certainly implied in the Canadian case of *Rudder v Microsoft Corp*,[2] and has been widely accepted in the USA.[3]

1 Although technically literate people are capable of installing software and bypassing the need to click on the 'I agree' icon, for which see *Aral v Earthlink, Inc.*, 134 Cal.App.4th 544 (2005), 36 Cal.Rptr.3d 229 (Cal. Ct. App. 2005) (determined by members of the Court of Appeal, Second District, Division, California, to be a contract of adhesion); where there is a succession of changes to the terms uploaded on to a website, it is incumbent on the issuer of such terms to ensure they retain evidence to prove when a person clicked to acknowledge that the new terms were received, as in the Maryland case of *Harold H. Huggins Realty, Inc., v FNC, INC.*, 575 F.Supp.2d 696; in *Rogers v Dell Computer Corporation*, 127 P.3d 560 (Okla. 2005), Dell failed to provide evidence to demonstrate where the contract was formed.

2 (1999) 2 CPR (4th) 474, 47 CCLT (2d) 168 (Ont Sup Ct), FSR (1996) 367. See also *Kanitz v Rogers Cable Inc.* (2002), 58 OR (3d) 299 (Sup Ct) and Barry Sookman, 'Browsewraps, fair dealing and Blacklock's Reporter v Canada: a critical commentary' (2017) 23(3) CTLR 55.

3 The following selected books and articles consider the US position: Nancy C. Kim, *Wrap Contracts: Foundations and Ramifications* (New York: Oxford University Press 2013); Simon Blount, *Electronic Contracts* (2nd edn, LexisNexis Butterworths Australia 2015); Rachel C. Anderson, 'Enforcement of contractual terms in clickwrap agreements: courts refusing to enforce forum selection and binding arbitration clauses'(2007) 3 Shidler J L Com & Tech 11; Robert Lee Dickens, 'Finding common ground in the world of electronic contracts: the consistency of legal reasoning in clickwrap cases' (2007) 11 Marq Intell Prop L Rev 379; Juliet M. Moringiello and William L. Reynolds, 'From Lord Coke to internet privacy: the past, present, and future of the law of electronic contracting' (2013) 72 Md L Rev 452; Erin Canino, 'The electronic "sign-in-wrap" contract: issues of notice and assent, the average internet user standard, and unconscionability' (2016) 50 UC Davis L Rev 535; Mark E. Budnitz, 'Touching, tapping, and talking: the formation of contracts in cyberspace' (2019) 43 Nova L Rev 235; Caterina Gardiner, 'Principles of internet contracting: illuminating the shadows' (2019) 48(4) CLWR 208 for a review of US and Irish cases.

7.91 For a 'click wrap' contract to be enforceable, it is necessary that the party to whom the contract is directed is notified that a contract exists, and that it is intended to apply to them. In the 9th circuit case of *Knutson v Sirius XM Radio, Inc.*,[1] Mr Knutson, in purchasing a motor vehicle from Toyota, was not aware that a trial subscription to Sirius XM satellite radio that accompanied the purchase of the vehicle also meant that Sirius intended him to be bound by the terms of a contract that he was not aware existed.

1 771 F.3d 559, 14 Cal. Daily Op. Serv. 12,769, 2014 Daily Journal D.A.R. 15,058.

7.92 In England and Wales, the Law Commission has suggested that this form of signature is the technological equivalent of a manuscript signature using a cross.[1] It is suggested that this analysis is sound. This analysis is also in keeping with the decisions made by judges over the past 200 years regarding the form that a manuscript signature may take.[2] In English law, the validity of the signature depends on the function it performs, not necessarily the form a signature takes. Even if the act of clicking on an

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

icon to order goods or services is deemed to be less secure than that provided by a manuscript signature, it does not follow that the reliability of the signature will affect its validity. Should a dispute occur between a buyer and a seller where one of the issues relates to the pressing of the icon, and the parties fail to resolve the matter, they will have to contemplate taking legal action. Before the matter reaches court, both parties will have to pay particular attention to the quantity and quality of the evidence available to them. In all probability, the reliability of the signature will depend on the ability of one or both of the parties to adduce sufficient forensic evidence of a high enough quality to demonstrate that either the icon was clicked or it was not. Even if the relying party can prove that the icon was clicked, it will not follow that the purported buyer clicked it. The nexus between the action of clicking the icon and the identity of the person who purported to order the items may be difficult to resolve, bearing in mind the security risks associated with using the Internet.

1 Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions Advice from the Law Commission* (2001), 3.37; see also 3.36 and 3.38.

2 For a historical consideration of the case law from every common law country relating to manuscript signatures, facsimile transmission and telegram up to 1990 (including an exhaustive treatment of the US) – invaluable in understanding electronic signatures and the various forms electronic signatures can take, and helpful in understanding how judges in common law jurisdictions adapted the meaning of a signature as technologies developed and people used them in ways that were not anticipated – see Stephen Mason, *The Signature: The Judicial Development of the Concept from the Thirteenth Century to the Age of the Facsimile Transmission* (Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London) (to be published in 2022).

7.93 Proof is central to the question. In the US case of *Kerr v Dillard Stores Services, Inc.*,[1] the issue was whether an employee had clicked the 'I accept' icon in respect of an arbitration agreement. In this instance, the employer required employees to consent to arbitration by executing the arbitration agreement by way of an intranet computer system. For months, the employee had made it clear that she did not wish to sign the arbitration agreement, and refused to do so. Evidence was given to demonstrate how easy it was for a supervisor to reset an employee's password: indeed, this is just what a supervisor did in front of the plaintiff when the plaintiff had failed to log on to find out when she was next on duty. On the same day that the supervisor logged on to change the plaintiff's password, the computer system sent an internal email to the plaintiff, indicating that the agreement had been 'signed'. The employee was adamant that she had not executed the agreement, and Vratil J concluded that it was unlikely that the plaintiff would not have spontaneously reversed her decision in front of the supervisor, and that the supervisor could have clicked on the 'I accept' icon as the plaintiff watched. The judge set out the problem:

> The problem with Dillard's position is that it did not have adequate procedures to maintain the security of intranet passwords, to restrict authorized access to the screen which permitted electronic execution of the arbitration agreement, to determine whether electronic signatures were genuine or to determine who opened individual emails. While the record establishes that Champlin and plaintiff were at the kiosk on April 28, it does not show that they were there at precisely 3:26:20 p.m. Therefore, it is not inconceivable Champlin or a supervisor logged on to plaintiff's account and executed the agreement. The Court recognizes that defendants' burden of proof is not absolute certainty, but merely a preponderance of the evidence. At the same time, Dillard's has not demonstrated the efficacy of its security procedures with regard to electronic

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> signatures. Therefore, its version of events is no more likely true than plaintiff's. For these reasons, this case basically turns on the burden of proof. Dillard's has the burden of proof and its evidence that plaintiff executed the arbitration agreement is not persuasive. On this record, the Court cannot find that it is more likely than not true that plaintiff executed the electronic agreement to arbitrate.[2]

1 2009 WL 385863, 105 Fair Empl.Prac.Cas. (BNA) 1298, 92 Empl. Prac. Dec. P 43,483.
2 2009 WL 385863 at 5.

7.94 This case illustrates how important proof is in the context of digital evidence.

7.95 In passing, Professor Preston notes that 'wrap' contracts are now considered to be enforceable without further inquiry, and the trend among judges in the US demonstrates a 'circularity of judicial review: one court finds a new kind of contract enforceable, and other courts then assume enforceability because "everyone is doing it" without performing a thorough analysis of the earlier opinions and distinguishing the facts',[1] and cites Matheson CJ in the case of *Hancock v American Telephone & Telegraph Company, Inc.*,[2] where the judge states, at 1255, that 'Clickwrap agreements are increasingly common and "have routinely been upheld" '. New terms to describe the methods devised to enforce contract terms on websites include 'sign-in-wraps' and 'scrollwrap'.[3]

1 Cheryl B. Preston, ' "Please note: you have waived everything": can notice redeem online contracts?' (2015) 64 American University Law Review 535,543, including the further citations noted in the article; see also Jeffrey H. Dasteela, 'Consumer click arbitration: a review of online consumer arbitration agreements' (2017) 9 YB On Arb & Mediation 1 .
2 701 F.3d 1248 (10th Cir. 2012).
3 New York: *Berkson v Gogo, LLC*, 97 F.Supp.3d 359 (2015).

7.96 In the Queensland case of *Harding v Brisbane City Council*,[1] the applicant used an online facility to appeal against a planning application. The person submitting the request was required to include details of a form of 'identification' as part of the submission process. Mr Harding typed in the number of his driving licence, but he made an error, and one of the numbers he typed in was incorrect. His application was rejected. At the appeal, the judge was required to determine, among other things, whether the input of an incorrect number merited the rejection of the submission. It did not. Robin QC DCJ held at [18] that:

> I think a common sense approach should be taken by which erroneous reproduction of more than a couple of digits (in the absence of special circumstances, such as the same number (exclusively) repeated – which may indicate some hardware or software malfunction) might be seen as creating some concern as to the signature, having regard to s 14(a) & (b) of the [Electronic Transactions (Queensland) Act 2001]; on a commonsense approach in the present context, one wrong digit does not create any real concern.

1 [2008] QPEC 75 (16 October 2008).

7.97 This discrepancy did not vitiate the submission as a properly made one. Interesting as the observation made by Robin QC DCJ is, that is the numbers identifying the driving licence constituted a 'signature', the judge was not correct. The signature comprised the act of clicking the 'accept' icon, and not the submission of the numbers identifying the driving licence.[1] The numbers identifying the driving licence acted as

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

an additional item of evidence to demonstrate to the Council that the person making the submission was who they claimed to be, which is a different issue entirely.

1 The 'I accept' icon was accepted in *eBay International AG v Creative Festival Entertainment Pty Ltd* (ACN 098 183 281) [2006] FCA 1768.

Browse wrap

7.98 There is a category of electronic signatures commonly called 'browse wrap' agreements, although there is some controversy around how judges apply the distinction between 'click wrap' and 'browse wrap' in case law.[1] Judges have also had to deal with cases that look like 'browse wrap', but are 'click wrap',[2] and what can be described as hybrid cases,[3] as described in the case of *Fjeja v Facebook, Inc.*[4] by Holwell, J at 838:

> Facebook's Terms of Use are somewhat like a browsewrap agreement in that the terms are only visible via a hyperlink, but also somewhat like a clickwrap agreement in that the user must do something else – click 'Sign Up' – to assent to the hyperlinked terms. Yet, unlike some clickwrap agreements, the user can click to assent whether or not the user has been presented with the terms.

1 For the US, see: Monique C. M. Leahy, 'Litigation of internet "wrap" agreements' (2017) 150 Am Jur Trials 383; Cheryl B. Preston, 'How did we end up in a world where browsewraps are enforced even when they waive all consumer rights?' (2018) 45 Fla St U L Rev 1012; James Gibson, 'Boilerplate's false dichotomy' (2018) 106 Geo LJ 249; Kevin Conroy and John A. Shope, 'Look before you click: the enforceability of website and smartphone app terms and conditions' (2019) 63 B BJ 23. For the position in Canada, see Sookman, 'Browsewraps, fair dealing and Blacklock's Reporter v. Canada'; Theodore Milosevic, 'What makes a consumer? Mandatory arbitration clauses and free digital services in Canada' (2017) 75 UT Fac L Rev 9; see also Eliza Mik, 'Contracts governing the use of websites' 2016 Sing J Legal Stud 70. For the European Union, where clickwrap is acceptable in respect of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 12, 16.1.2001, 1–23, see *El Majdoub v CarsOnTheWeb.Deutschland GmbH* (C-322/14) EU:C:2015:3343, [2015] 1 WLR 3986, [2016] 1 All ER (Comm) 197, [2015] 5 WLUK 617, [2015] All ER (EC) 1073, [2015] CEC 1225, [2015] ILPr 32 and Andrew Dickinson and Johannes Ungerer, ' "Click wrapping" choice of court agreements in the Brussels I regime', L.M.C.L.Q. 2016, 1(Feb), 15–19.
2 California: *Savetsky v Pre-Paid Legal Services, Inc. d/b/a LegalShield*, 2015 WL 4593744 (previous hearing reported at 2015 WL 604767).
3 The Court of Appeals of Texas concluded the facts in *Hotels.com, L.P. v Canales*, 195 S.W.3d 147, 195 S.W.3d 147 (2006), which illustrated a similar hybrid approach. In this case, the terms did not apply to the main plaintiff because it entered a contract over the telephone, but the terms applied to those plaintiffs that had used the website.
4 841 F.Supp.2d 829 (2012).

7.99 In this case, the judge held that the user was bound by the terms and conditions, and said, at 839–840:

> The mechanics of the internet surely remain unfamiliar, even obtuse to many people. But it is not too much to expect that an internet user whose social networking was so prolific that losing Facebook access allegedly caused him mental anguish would understand that the hyperlinked phrase 'Terms of Use' is really a sign that says 'Click Here for Terms of Use'. So understood, at least for those to whom the internet is in an indispensable part of daily life, clicking the hyperlinked phrase is the 21st-century equivalent of turning over the cruise ticket. In both cases, the consumer is prompted to examine terms of sale that are located somewhere else. Whether or not the consumer bothers to look is irrelevant.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> ...
> Here, Fteja was informed of the consequences of his assenting click and he was shown, immediately below, where to click to understand those consequences. That was enough.

7.100 'Browse wrap' agreements are where one party aims to impose terms of use or sale on another party where a visitor demonstrates assent by using the website.[1] The potential customer is not required to indicate acceptance of any terms by any positive action, but the user must have had actual or constructive knowledge of the terms and conditions for them to be effective.[2] This form of electronic signature comprises the process of using the website, thereby indicating knowledge of the relevant terms, although for such terms to be effective, or for constructive notice to apply, they must be conspicuous, intend to apply and the party with the burden of proof must demonstrate how a visitor is made aware of the terms. A party might fail because they cannot demonstrate a number of issues of relevance, such as that the agreement actually existed on its website at the material time, that any agreement applied to the actual product in dispute, or that the defendants agreed to its terms.[3]

1 Further reading: Uri Benoliela and Shmuel I. Becher, 'The duty to read the unreadable' (2019) 60 BC L Rev 2255; William Hurley, 'Failure of notice to terms in online contract formation: a solution that informs consumers of their obligations and rights' (2019) 14 Liberty U L Rev 249; Tal Kastner and Ethan J. Leib, 'Contract creep' (2019) 107 Geo LJ 1277; Budnitz, 'Touching, tapping, and talking'.

2 Or the product, if in Illinois: *Schafer v AT & T Wireless Services, Inc.*, 2005 WL 850459 (S.D.Ill.).

3 Florida: *IT Strategies Group, Inc. v The Allday Consulting Group, L.L.C.*, 975 F.Supp.2d 1267 (2013) where the plaintiff failed to demonstrate that the defendants had actual or constructive knowledge of its online user agreement and that they had assented to the terms of that agreement.

'I accept'

7.101 The first instance decision in the case of *Bassano v Toft*[1] is an example where the use of the 'I accept' icon was upheld in England under the provisions of the Consumer Credit Act 1974. It was argued by counsel for Mrs Bassano that the loan agreement was not executed by her in a manner that complied with the Act. Popplewell J disagreed, indicating, at [43], that:

> s61 of the Act requires the agreement to be signed in the prescribed form, and the form prescribed at the time was that required by The Consumer Credit (Agreements) Regulations 2010 (SI 2010 No 1014). The only relevant prescription was in regulation 4(3)(a), which provides that the signature must be in a space indicated in the document for that purpose and dated. Regulation 4(5) recognises that a regulated agreement may be concluded electronically by regulation 4(5), and that the document may contain 'information about the process or means of providing, communicating or verifying the signature to be made by the debtor'. There was therefore nothing in the Consumer Credit Act 1974 to suggest that regulated agreements were capable of being signed by an electronic signature; and I can see no reasons of policy why a signature should not be capable of being affixed and communicated electronically to an agreement regulated by the Act, just as it can for other documents which are required to be signed.

1 [2014] EWHC 377 (QB), [2014] 2 WLUK 800, [2014] ECC 144, [2014] CTLC 1177, [2014] Bus LR D99, [2014] CLY 273.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.102 This type of conflicting evidence, coupled with a denial that the email communications were sent by the sender, occurred in Germany in the three cases of OLG Köln, 19 U 16/02, LG Konstanz, 2 O 141/01 A, and AG Erfurt, 28 C 2354/01.[1] The three individual defendants were asked to pay for items bought in Internet auctions. The winning bids were sent from email accounts where the user can write the email on the website of the provider of the address. Each of the defendants had access to the address by means of a password, but denied taking part in the bidding process. All three cases were dismissed, because the relying party failed to prove to the satisfaction of the courts that the defendants sent the declarations, which meant the plaintiff failed to prove that a contract had been concluded. By the same token, exactly the same problem may occur with the use of digital signatures. Whether a user denies clicking on an icon or using their private key to sign a document or message, the problem will be the same: proving that the sending party carried out the action. In this respect, the difference between a digital signature and clicking an icon is a narrow one.

1 Michael Knopp, Case Note, OLG Köln, Ur19 U 16/02; LG Konstanz, 2 O 141/01 A; AG Erfurt, 28 C 2354/01, (2005) 2 Digital Evidence and Electronic Signature Law Review 105; for a translation of Ur19 U 16/02, see Henriette Picot and Marlene Kast (2008) 5 Digital Evidence and Electronic Signature Law Review 108.

Personal Identification Number (PIN) and password

7.103 The PIN is possibly the oldest form of electronic signature,[1] and has become a very widely used form of authentication, especially to obtain access to a bank account through the use of an ATM (automated teller machine or automatic teller machine or automated banking machine or cash machine), or to confirm a transaction with a credit card or debit card.[2] Arguably, in the banking context, the PIN combines two functions. Before we consider these two functions, let us look at the requirements of the bank. The bank needs to satisfy itself that:

> 1. The card is legitimate (this is difficult to achieve, as the reports about fraud demonstrate), and
>
> 2. The card is in the possession of the customer to whom it was issued, or a person authorized by the customer to use the card.

1 In *United States of America v Miller*, 70 F.3d 1353 (D.C. Cir. 1995), Karen LeCraft Henderson J referred to the PIN at 1355 as acting 'as a sort of electronic signature authorizing an ATM to release available funds'.

2 The use of a PIN was explicitly recognized as a type of electronic signature by the Civil Chamber of the Supreme Court of Lithuania in its ruling in the case of *Ž.Š. v AB Lietuva taupomasis bankas*, civil case no. 3K-3-390/2002; for a case note, see S. Trofimovs (2008) 5 Digital Evidence and Electronic Signature Law Review 143, and for a translation, see Sergejs Trofimovs (2009) 6 Digital Evidence and Electronic Signature Law Review 255; for Austria, see case note, OGH Urteil vom 29.6.2000, 2 Ob 133/99v, Oberster Gerichtshof (Austrian Supreme Court) (2008) 5 Digital Evidence and Electronic Signature Law Review 141 and translation into English: OGH judgment of 29.06.2000, 2 Ob 133/99v – Liability for misuse of ATM cards, Oberste Gerichtshof (Supreme Court) (2009) 6 Digital Evidence and Electronic Signature Law Review 223.

7.104 If the bank satisfies itself that its computer systems are interacting with the card issued to the customer (which is not always the case), then the computer system requests the purported customer to undertake one further act to confirm they (or a person authorized by them) have physically inserted the card into the ATM, or the

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

point of sale terminal, by keying in the correct PIN. Generally, if the computer systems receive positive results from both interactions, then the bank will permit the person at the ATM or the point of sale terminal to undertake whatever activity they are permitted to do within the terms of the mandate.

> 1. The first function of a PIN
>
> The first function of the PIN acts as a means of authentication. The PIN purports to demonstrate that the person who keyed in the PIN knew the correct PIN (there are some forms of attack that do not need the correct PIN – any combination of numbers will act to deceive the card issuer that the correct PIN has been keyed in).
>
> 2. The second function of a PIN
>
> Once the computer systems of the bank are satisfied that the card is legitimate and the PIN is the correct PIN of the customer, then the person at the ATM or the point of sale terminal can undertake any activity on the account that is permitted within the mandate and within the limitations of the technology.

7.105 The PIN, even though it is offered to the machine before a transaction is effected, acts as a signature to verify a payment or other form of transaction. This means that the presentation of a card to an ATM, and the input of a PIN, is similar to a cheque that is written out by the account holder, signed and then presented to the cashier at the bank. The customer completes the action necessary to request a payment in advance of the payment being made by the cashier, and then signs the cheque in the presence of the cashier – all before receiving acknowledgment that a transaction has been authorized. This means the PIN is a form of electronic signature.

7.106 It might be considered that the action of clicking the 'I accept' icon or box, or typing in a PIN, is merely a means by which the person agrees to conclude the contract, but the act is not that of appending their electronic signature. This analysis might be right, but we must recall that the digital world is different to the physical world. Conceptually, some of the forms of electronic signature may not strictly be considered 'signatures' in the physical world. Nevertheless, it is a convenient shorthand to refer to some forms of agreeing to enter a contract as an 'electronic signature' – at least we can all understand the meaning behind these words, even if the form is not quite what we expect.

7.107 Invariably, a claim by the user that they did not authorize one or more transactions conducted on the account will require the relying party – that is, the bank, with the burden of proof – to prove the account holder authorized the transaction. The fact that a withdrawal or other form of transaction took place may not be in issue, and in any event the bank can adduce the evidence under the relevant business records or the Bankers' Books exemptions. The burden remains the same,[1] whatever the technology used.[2]

1 In Cormac Herley, P. C. van Oorschot and Andrew S. Patrick, 'Passwords: if we're so smart, why are we still using them?', in Roger Dingledine and Phillipe Golle (eds), *Financial Cryptography and Data Security, 13th International Conference, FC 2009, Accra Beach, Barbados, February 23–26, 2009* (Springer 2009), https://www.microsoft.com/en-us/research/publication/passwords-if-were-so-smart-why-are-we-still-using-them/?from=http%3A%2F%2Fresearch.microsoft.com%2Fpubs%2F80199%2Ffc09.pdf, the statement that 'users become responsible for all approved transactions where authorization relied on a correct PIN' is incorrect. Whatever the form of technology

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

that is used, the relying party has the burden of proof. The bank must prove that it had the mandate of the customer to undertake an action on the account, regardless of the nature of the technology. Although it was held in the South African case of *Diners Club SA (Pty) Ltd v Singh* 2004 (3) SA 630 (D) that a contract term by which the customer was liable, irrespective of who used the PIN, was not against public policy; compare this to the Japanese decision by the Supreme Court in *Taro Kono (an alias) v The Shinwa Bank, Ltd* 8 April 2003, MINSHU Vol. 57 No 4 at 337, Hanrei-Times No 1121 at 96, discussed with other Japanese authorities and the effect of the Depositor Protection Act 2005 by Hironao Kaneko, 'How bank depositors are protected in Japan' (2011) 8 Digital Evidence and Electronic Signatures Review 92. For a comparative analysis of the contractual tension between the liability of a bank and the liability of the customer generally, see Sandra Booysen, 'Consumer protection and the court's role in shaping the bank-customer contract' (2019) 135 (Jul) LQR 437.

2 Maryke Silalahi Nuth, 'Unauthorized use of bank cards with or without the PIN: a lost case for the customer?' (2012) 9 Digital Evidence and Electronic Signature Law Review 95; case translation: Norway, Journal number 04-016794TVI-TRON, *Bernt Petter Jørgensen v DnB NOR Bank ASA by the Chairman of the Board* (Trondheim District Court, 24 September 2004) (2012) 9 Digital Evidence and Electronic Signature Law Review 117; case translation: Republic of Turkey, case number: 2009/11485, judgment number: 2011/4033, by Av. Burcu Orhan Holmgren (2012) 9 Digital Evidence and Electronic Signature Law Review 124.

7.108 The central concern is usually whether it was the customer or somebody else who was responsible for withdrawals made from the customer's account using the correct PIN or password. Judges across the globe have had to address numerous problems that have arisen in connection with the use of the PIN in personal banking. Issues include:

> (1) Whether it was the customer or a third party without authority who used the PIN (the debate might be that the technology does not need the correct PIN)[1] – by way of example, cases that illustrate this issue are recorded in the USA,[2] Germany,[3] Nigeria,[4] Papua New Guinea,[5] and England and Wales.[6]
>
> (2) Responsibility for the PIN sent by the bank through the postal service falling into the wrong hands and leading to the unauthorized use of the PIN in banking transactions, causing loss to the customer.[7]
>
> (3) Transactions that occur with the authority of the user, but the user may dispute the amount they authorized, as in the Danish case of U.2000.1853V, where, at a restaurant with late-night opening hours, A authorized two Dankort card payments as he swiped his debit card through one of N's card terminals, entered his PIN and agreed the amount that appeared on the display. The court was satisfied that one of the payments was erroneously accepted in the sum of DKK 10,500 instead of DKK 105. N was therefore ordered to pay back the difference. The court accepted, as a starting point, that when the appellant entered his PIN and approved an amount in the sum of DKK 10,500, the appellant made a binding payment to the respondent. However, that action did not rule out that it could be proved that payment of a higher amount was made by mistake.[8]

1 Steven J. Murdoch, 'Reliability of chip & pin evidence in banking disputes' (2009) 6 Digital Evidence and Electronic Signature Law Review 98; Roger Porkess and Stephen Mason, 'Looking at debit and credit card fraud' (2012 Autumn) 34(3) Teaching Statistics 87 (also translated into German: Betrug mit Kundenkarten und Kreditkarten, Stochastik in der Schule (2014) 34(2), S. 15).

2 For a number of early cases in the US, see *Judd v Citibank*, N.Y.City Civ.Ct., 435 N.Y.S.2d 210; *Feldman v Citibank, N.A.; Pickman v Citibank, N.A.*, N.Y.City Civ.Ct., 443 N.Y.S.2d 43; *Ognibene v Citibank, N.A.*, N.Y.City Civ.Ct., 446 N.Y.S.2d 845; see also *State of New York, by Abrams v Citibank, N.A.*, 537 F.Supp. 1192 (1982); in *Porter v Citibank, N.A.*, 123 Misc.2d 28, 472 N.Y.S.2d 582 (N.Y.City Civ.Ct. 1984), where the customer used their card but no money was dispensed, employees of the bank testified that on average cash machines were out of balance once or twice a week.

3 5 October 2004, XI ZR 210/03, published BGHZ 160, 308–321 Bundesgerichtshof (Federal Court of Justice); for a translation and commentaries by Michael Eßer and Thomas Kritter, see (2009) 6 Digital

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Evidence and Electronic Signature Law Review 248; it has been demonstrated that any PIN can be used to obtain money from an ATM, with no need for the thief to have the correct PIN, for which see Steven J. Murdoch, Saar Drimer, Ross Anderson and Mike Bond, 'Chip and PIN is broken', 2010 IEEE Symposium on Security and Privacy, http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf (this was awarded the Best Practical Paper).

4 *Geoffrey Amano v United Bank for Africa (UBA) PLC*, Suit No: PHC/257/2011, reported in (2013) 3 SLP (Section on Legal Practice) Law Journal 114; *Benjamin Agi v Access Bank PLC* (2014) BNLR 23 discussed by Timothy Tion, 'Electronic evidence in Nigeria' (2014) 11 Digital Evidence and Electronic Signature Law Review 76; for an example of members of staff stealing from ATMs, see Timothy Tion, 'Another method of stealing cash from ATMs' (2017) 14 Digital Evidence and Electronic Signature Law Review 13.

5 *Roni v Kagure* [2004] PGDC 1, DC84 (1 January 2004).

6 *Job v Halifax PLC* (not reported) Case number 7BQ00307 (2009) 6 Digital Evidence and Electronic Signature Law Review 235; *Shojibur Rahman v Barclays Bank PLC*, commentary by Stephen Mason and Nicholas Bohm (2013) 10 Digital Evidence and Electronic Signature Law Review 169; *Shojibur Rahman v Barclays Bank PLC* (on appeal from the judgment of Her Honour District Judge Millard dated 24 October 2012), commentary by Stephen Mason and Nicholas Bohm (2013) 10 Digital Evidence and Electronic Signature Law Review 175.

7 Court of First Instance of Athens constituted by a single judge 5526/1999; for a translation into English, see Anastasia Fylla, Case note – Greece (2007) 4 Digital Evidence and Electronic Signature Law Review 89.

8 For a full report of this case, see (2007) 4 Digital Evidence and Electronic Signature Law Review 98.

7.109 Of interest is a decision that accepts the proposition that the unique number issued by a bank can be a signature. In the New Jersey case of *Spevack, Cameron & Boyd v National Community Bank of New Jersey*,[1] the unique account number assigned by a bank to a depositor was determined to be as complete a signature as the depositor's written or printed name. Bilder J (retired and temporarily assigned on recall) observed, at 1169, that a signature may take many forms, and there was no reason why a bank account number could not be one of them:

> In this computer age the use of numbers as a means of identification has become pervasive. Indeed, numbers are more readily recognized and handled than signatures. The 'signature' used by Homequity was its account number at Midlantic, the bank in which it deposited the check. That 'signature' accurately identified the payee and the funds were properly credited to the payee's account. In fact, had Homequity written a name without the account number, the bank would have had to look up the number that corresponded with the same. In keeping with the electronic age, it is the numbers which have the primary significance.

1 677 A.2d 1168 (N.J.Super.A.D. 1996), 291 N.J.Super. 577. Note the 1844 New York case of *Brown v The Butchers & Drovers' Bank*, 6 Hill 443, 41 Am.Dec. 755 where a person writing '1. 2. 8.' on the back of a bill of exchange as a substitute for his name served to endorse the bill.

7.110 The problems with the PIN and banking applications represent an ever-changing struggle between clever thieves who implement new strategies to steal and the banks in overcoming the threats as they are discovered.[1]

1 Mason and Reiniger, '"Trust" between machines?'; Stephen Mason, 'Electronic banking and how courts approach the evidence' (2013) 29 Computer Law and Security Review 144; Stephen Mason, 'Debit cards, ATMs and negligence of the bank and customer' (2012) 27 Butterworths Journal of International Banking and Financial Law 163; Stephen Mason, 'UK credit card fraud: the scale of the problem' (2012) 6 e-Finance & Payments Law & Policy 14.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.111 As to the use of passwords as a form of electronic signature, in England and Wales Companies House relies on a six-character alphanumeric 'Authentication Code' which it describes as the 'equivalent of a company officer's signature'.[1] The password, which can be changed by the user, will only be sent out by Companies House by post to the company's registered office. Likewise, electronic tax returns to HM Revenue & Customs go through a government gateway, which involves identity and security checks including a unique taxpayer reference number, a password and an activation code, thereby removing the need for a signature.[2]

1 https://www.gov.uk/guidance/company-authentication-codes-for-online-filing.
2 Confirmed in *Creative Eye Photography LLP Helipix LLP v The Commissioners for Her Majesty's Revenue & Customs* [2017] UKFTT 399 (TC), [2017] 5 WLUK 213 at [27], a decision of the First-tier Tribunal Tax Chamber.

7.112 In *Niche Generics Ltd v European Commission (T-701/14)*,[1] an application was made for an annulment of a decision by the Commission that a settlement agreement entered into by the applicant constituted a restriction on competition. An issue arose as to whether a defence had been filed by the Commission, it being a requirement in article 3(1) of the Rules of Procedure of the General Court of 2 May 1991, that '[t]he original of every pleading must be signed by the party's agent or lawyer'. However, the Rules also provided a mechanism by which certain criteria could be put in place to satisfy that requirement. A decision by the General Court on the lodging and service of procedural documents by means of e-Curia was made on 14 September 2011[2] in these terms in article 3:

> A procedural document lodged by means of e-Curia shall be deemed to be the original of that document for the purposes of the first subparagraph of Article 43(1) of the Rules of Procedure where the representative's user identification and password have been used to effect that lodgement. Such identification shall constitute the signature of the document concerned.

1 Also known as Perindopril, Re, Servier, Re EU:T:2018:921, [2018] 12 WLUK 705, [2019] 4 CMLR 15.
2 Decision of the General Court of 14 September 2011 on the lodging and service of procedural documents by means of e-Curia, OJ C 289, 1.10.2011, 9.

7.113 The argument as to any failure to file a defence was rejected. The procedural decision and overall decision of the General Court in *Niche Generics* demonstrates the fact that a user identification and password are capable of amounting to an electronic signature in that context. It is easy to see how that concept could be expanded in relation to passwords actually being a component of an electronic signature.

Typing a name into an electronic document

7.114 The use of electronic signatures predates any form of legislation, and in the latter decade of the twentieth century adjudicators found themselves applying well-established legal principles to new technologies when presented in the form of electronic signatures, just as judges in the nineteenth century were confronted with the increasing use of printing, typewriting and telegrams: all, it must be said, without the need for special legislation to be enacted. The early case law in which electronic signatures appeared demonstrated the flexibility of the common law,[1] although this

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

form of electronic signature is not uniformly accepted in all jurisdictions,[2] and some judges in common law jurisdictions have failed to demonstrate flexibility.[3]

1 The first example appears to be *Wilkens v Iowa Insurance Commissioner* 457 N.W.2d 1 (Iowa App. 1990), where an agent countersigned insurance policies by typing his name into the document on the computer; see also *Doherty v Registry of Motor Vehicles*, No 97/CV0050 (Suffolk, SS Massachusetts District Court, May 28, 1997), http://www.loundy.com/CASES/Doherty_v_RMV.html, where an email was signed by the typewritten name of the officer; electronic signatures are used routinely in traffic offences, for which see the Canadian cases of *R v Eged*, 2009 BCPC 180 (CanLII) and *City of London v Caza*, 2010 ONSC 1548 (CanLII) by way of example.

2 For instance, see the following case translations from Denmark: U.2001.252Ø (request for dissolution; Bankruptcy Court; signature; sufficiency of electronic signature with name typed on document) and U.2001.1980/1H (request for dissolution; Bankruptcy Court; requirement for manuscript signature; sufficiency of electronic signature with name typed on document) (2009) 6 Digital Evidence and Electronic Signature Law Review 232.

3 In the Australian case of *Philip Laming v TicketXpress Pty Ltd* PR941462 [2003] AIRC 1503 (3 December 2003), Hamilton, Deputy President of the Australian Industrial Relations Commission indicated, incorrectly, at [2] that 'Emails do not contain signatures, even electronic signatures, and the only readily identifiable marking may be the email address'.

7.115 Typing a name into a document such as an email is a valid method of signing a document,[1] as established in *Orton v Collins*,[2] where the word 'Putsmans' was deliberately typed in an email after the customary salutation 'Yours faithfully'. Mr Peter Prescott QC, sitting as a Deputy Judge, said, at [21]:

> I have no doubt that its purpose would be recognized throughout the profession. Anyone would think: 'Putsmans are signing off on this document'. It was intended to signify that document was being sent out with the authority of the defendants' legal representative.

1 For additional examples, see China: *Beijing Han-Hua-Kai-Jie Technology development Ltd. v Chen Hong* (2018) Zhe 0192 (2007) 4 Digital Evidence and Electronic Law Review 96 (employment); France: Case number 235784 from the Conseil d'Etat, Elections municipales de la Commune d'Entre-Deux-Monts dated 28 December 2001 (2004) 1 Digital Evidence and Electronic Law Review 81; Case number 00-46467 from the Cour de Cassation, chambre civile 2, Sté Chalets Boisson c/ M. X. dated 30 April 2003 (2004) 1 Digital Evidence and Electronic Law Review 82; Germany: OLG Köln, 19 U 16/02; LG Konstanz, 2 O 141/01 A; AG Erfurt, 28C 2354/01 (2005) 2 Digital Evidence and Electronic Law Review 105; Ur19 U 16/02, OLG Köln, 6 September 2002 (2008) 5 Digital Evidence and Electronic Law Review 108; 12 U 34/07, Court of Appeal Berlin (Kammergericht Berlin), 30 August 2007 (2008) 5 Digital Evidence and Electronic Law Review 110 (all contracts); Italy: Tribunale sez. V, Milano, 18/10/2016, n. 11402 (2019) 16 Digital Evidence and Electronic Law Review 90 (contract); Slovenia: I Up 505/2003, The Supreme Court of the Republic of Slovenia (2007) 4 Digital Evidence and Electronic Law Review 97 (procedure). For a name in a text message, see China: *Yang Chunning v Han Ying* (2005) hai min chu zi NO.4670, Beijing Hai Dian District People's Court (2008) 5 Digital Evidence and Electronic Law Review 103 and Denmark: U.2001.252Ø (2009) 6 Digital Evidence and Electronic Law Review 232; U.2001.1980/1H (2009) 6 Digital Evidence and Electronic Law Review 234.

2 [2007] EWHC 803 (Ch), [2007] 1 WLR 2953, [2007] 3 All ER 863, [2007] 4 WLUK 353, [2007] 2 EGLR 147, (2007) 151 SJLB 608, [2007] NPC 49, [2007] CLY 488; *Green (Liquidator of Stealth Construction Ltd) v Ireland* [2011] EWHC 1305 (Ch), [2011] 5 WLUK 588, [2012] 1 BCLC 297, [2011] BPIR 1173, [2011] CLY 1875 where it was accepted that typing a name into an email is sufficient for the purposes of s 2 Law of Property (Miscellaneous Provisions) Act 1989; *Lindsay v O'Loughnane* [2010] EWHC 529 (QB), [2010] 3 WLUK 515, [2012] BCC 153.

7.116 The main area of contention is to argue whether an email or series of emails constitutes the necessary evidence that an agreement has been reached.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Acts by a lawyer as agent

7.117 An agent, with the appropriate authority, remains capable of binding their principal digitally, just as in the physical world. That this applies to attorneys is illustrated in the Tennessee case of *Waddle v Elrod*,[1] where the Supreme Court determined that the emails exchanged between counsel with their name typed at the bottom of the email satisfied the signature requirement of the Statute of Frauds. The same principle applies in New Zealand.[2]

1 367 S.W.3d 217 (2012).
2 *Cox v Coughlan* [2014] NZHC 164 (14 February 2014).

Interest in real property

7.118 In *Faulks v Cameron*,[1] the Supreme Court of the Northern Territory in Australia applied the provisions of s 9 of the Electronic Transactions (Northern Territory) Act 2000 (NT) to the name typed at the bottom of the email. Acting Master Young concluded, at 64:

> I am satisfied that the printed signature on the defendant's emails identifies him and indicates his approval of the information communicated, that the method was as reliable as was appropriate and that the plaintiff consented to the method. I am satisfied that the agreement is 'signed' for the purposes of s45(2).

1 [2004] 32 Fam LR 417, [2004] NTSC 61; see also *Kavia Holdings Pty Limited v Suntrack Holdings Pty Limited* [2011] NSWSC 716.

Loan of money

7.119 In the New South Wales case of *Stuart v Hishon*,[1] Ms Hishon loaned money to Mr Stuart and subsequently initiated proceedings to recover A$28,216.17 plus interest, being the outstanding and unpaid balance of monies owing to her pursuant to the loan of A$83,760.87 made by Ms Hishon to him in July 1996. Prior to the litigation, a series of email correspondence occurred between the parties regarding the payment of the loan, and Mr Stuart ended each email with 'Tom'. Counsel for Mr Stuart argued that it was necessary to provide evidence to establish that Mr Stuart placed the printed name on his email intending it to be an acknowledgment of the debt, and that no such evidence existed. Harrison J did not accept this argument, stating, at [34], that 'Mr Stuart typed his name on the foot of the email. He signed it by doing so. It would be an almost lethal assault on common sense to take any other view.'

1 [2013] NSWSC 766.

7.120 In China, in the court of first instance case of *Yang Chunning v Han Ying*,[1] Mr Yang claimed that the defendant Miss Han asked to borrow RMB 11,000 from him. Yang agreed to lend the money to Miss Han, but she failed to return the money. As evidence, Mr Yang exhibited several text messages sent from Miss Han's mobile telephone about the loan. It was confirmed that the messages were transmitted from Miss Han's mobile telephone number. In this case, the judge supported the plaintiff's claim based on the evidence of the mobile telephone message between the parties. The court judged that these messages, as a form of electronic text according to the Electronic Signature Law,[2] could serve as evidence to support Mr Yang's claim.

1 (2005) hai min chu zi NO.4670, Beijing Hai Dian District People's Court; for a translation into English of this case, see (2008) 5 Digital Evidence and Electronic Signature Law Review 103.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

2 Electronic Signatures Law of the People's Republic of China of 2004 (amended by Electronic Signatures Law of the People's Republic of China of 2015 (Order No. 24 of the President of the People's Republic of China, promulgated on and effective since 4 April 2015).

7.121 In the Texas case of *Parks v Seybold*[1] before the Court of Appeals, the Gaming Management Corporation executed a note payable to Scott Seybold in the amount of US$10,000, plus 15 per cent interest. Clyde Parks wrote the note by hand, and he signed it in his capacity as vice-president of the corporation. The corporation ceased to exist, and Mr Seybold sought full payment on the note. The parties subsequently exchanged a number of emails, and the court agreed with the trial judge that the emails constituted writing, and the inclusion of the words 'Thank you, Clyde' above an automatic signature block served to demonstrate that Parks had signed the emails.

1 2015 WL 4481768; John G. Browning, 'No ink, no problems? A look at the validity of email signatures as contracts' (2017) 80 Tex BJ 772 ; George L. Blum, 'Use of e-mails to establish enforceable contracts' (2017) 32 ALR 7th Art 6.

Employment

7.122 In England and Wales, the first case of this nature occurred in the Industrial Tribunal case of *Hall v Cognos Limited.*[1] Cognos employed Mr Hall as a sales executive under the terms of the Standard Employment Agreement used by Cognos. He was provided with a motor car for business and personal use. Mr Hall was reimbursed for all reasonable expenses incurred for travel, accommodation and other costs in accordance with the relevant policy, which the chairman determined was incorporated into the contract. The policy stated that all expenses over six months old would not be paid. Mr Hall failed to submit any travel expenses between 1 December 1995 and 3 June 1996. By January 1997 Mr Hall wanted his expenses to be paid. A series of emails was exchanged on 15 January between Mr Hall, Sarah McGoun (of HR) and Keith Schroeder, Mr Hall's line manager. Mr Hall asked if he could submit a late expenses claim to Ms McGoun. Ms McGoun in turn referred Mr Hall to Keith Schroeder, and Mr Schroeder, in response to the question as to 'whether [the late submission] is OK with you?' replied, 'Yes, it is OK.' Mr Hall subsequently submitted his expenses, although he did not provide all the necessary forms immediately. He also inflated his claims. His employers refused to make any payment and dismissed him.

1 Industrial Tribunal Case No 1803325/97.

7.123 Counsel for Cognos argued that because an email was not in writing and signed, the exchange of emails did not have any effect on the terms of the employment agreement. Mr C. T. Grazin, the chairman sitting on his own, declined to accept this proposition, attractive as it appeared to him. He held that the emails were in writing and signed once they were printed out. Despite there being no reference or discussion to any relevant case law or the statutory definitions of 'writing' and 'document,' the chairman concluded at 5:

> I am satisfied than an email is 'in writing and signed by the parties' once it is printed out. The position might (it is not necessary to make any finding on this point) be different if the email was only retained temporarily on the computer's hard disk storage system. The documents that were, however, produced from the computer are clearly in writing and bear the signatures of both 'Sarah' and 'Keith'. The fact that those signatures are printed, rather than hand-written, is not in my view material. For those reasons, I reject Mr Pym's submission that the relevant

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

email messages are incapable, as a matter of law, of having any modifying effect on the specific contract between the parties.

7.124 A further argument put forward on behalf of Cognos was that Mr Schroeder did not have the authority to respond to Mr Hall's request, nor was he authorized to agree to it. This was rejected on the basis that, as Mr Hall's line manager, Mr Schroeder was vested with the appropriate authority to deal with such a request, and as a result, Mr Hall could rely on Mr Schroeder's response. This meant Mr Schroeder's response acted to bind Cognos. As a result, the exchange of emails between Mr Hall and his line manager acted to vary the policy, and Cognos was obliged to pay Mr Hall his reasonable expenses.

Contract

7.125 The members of the Court of Appeal Civil Division in *Nicholas Prestige Homes v Neal*[1] did not concern themselves with the question of the signature in emails in this particular case. It was concluded that a contract was formed with the exchange of emails regarding the commission on a sale of property. By implication, the names typed at the end of the email, 'Marc Taylor' and 'Sally', were construed as valid signatures.[2]

1 [2010] EWCA Civ 1552, [2010] WLUK 9, (2010) 107(48) LSG 14.

2 An exchange of emails constituted an agreement in *Bieber v Teathers Ltd (In Liquidation)* [2014] EWHC 4205 (Ch), [2014] 12 WLUK 408, [2015] CILL 3609, and as with *Nicholas Prestige Homes v Neal*, the nature of the signatures was not considered. In *Temple, Re* 2012 CarswellOnt 2817, 2012 ONSC 376, [2012] O.J. No. 856, 109 O.R. (3d) 374, 214 A.C.W.S. (3d) 609, 75 C.B.R. (5th) 312, Newbould J determined that a name on an email was a sufficient signature within the requirements of the Limitations Act, 2002, S.O. 2002, c. 24 (Ontario), but the judge did not indicate where the name was placed, whether it as at the end of the email or the name as part of the email address, in *Toronto Common Elements Condo. Corp. No. 2041 v Toronto Standard Condo. Corp. No. 2051*, 2015 ONSC 4245 (CanLII), Corbett J refused to accept an email was signed, but failed to indicate whether a name appeared in the body of the email, and if a name was included in the body of the email, where the name was placed, whether it as at the end of the email or if a name formed part of the email address. In *Lev v Serebrennikov* 2016 ONSC 2093 (CanLII), Pattillo J accepted an email was signed, but did not clarify where the name was placed, whether it as at the end of the email or the name as part of the email address, although by inference, the judge was probably referring to the name that formed part of the email address.

7.126 Whether a signature contained in an email constitutes a valid contract in Israel was considered by Noa Grossman J in *Computer Sky Edv v Prime Medical Company Ltd.*[1] It was held that a contract that was signed through email correspondence is valid. In essence, the reasoning of the decision was as follows: negotiations are carried out today through electronic communications; an offer, a request for an offer and the reception of an offer can all be performed via email correspondence; the correspondence as a whole is what creates the actual agreement; unlike a printed contract that incorporates the parties' will into one document, a contract reached by way of reciprocating electronic communications is a mosaic of all the parties' communications.

1 Tel Aviv Peace Court Civil Case 29488/04 (4 August 2005, unpublished decision).

7.127 Two rulings of the Lithuanian courts, in the Court of Appeal[1] and in the Supreme Court of Lithuania,[2] accepted email communications (typed by the person who appends their name at the end) as evidence in civil proceedings, although it is not certain whether names written in the emails will be accepted as a form of electronic signature.

1 10 April 2006, case no. 2A– 95/2006.

2 6 March 2006, case no. 3K-3-169/2006.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.128 In Scotland, the nature of the electronic signature was not specifically at issue in *Baillie Estates Ltd v Du Pont (UK) Ltd*,[1] where Hodge L concluded that an exchange of emails constituted a valid contract, notwithstanding the apparent informality of the content of the emails exchanged, because the exchange demonstrated an agreement to enter into a contract. By inference, it is possible to observe that the name typed at the bottom of each email constituted an electronic signature.

1 2009 GWD 25–399, [2009] ScotCS CSOH_95, [2009] CSOH 95.

7.129 A contract in South Africa can be varied by an exchange of emails that includes the name of the person sending the email where their name appears in the email, as in the case of *Spring Forest Trading v Wilberry*,[1] where the parties agreed to cancel a contract by exchange of emails. Cachalia JA said, at [28]:

> The typewritten names of the parties at the foot of the emails, which were used to identify the users, constitute 'data' that is logically associated with the data in the body of the emails, as envisaged in the definition of an 'electronic signature'. They therefore satisfy the requirement of a signature and had the effect of authenticating the information contained in the emails.

1 (725/13) [2014] ZASCA 178, 2015 (2) SA 118 (SCA) (21 November 2014).

7.130 This finding is also consistent with the approach taken by the courts in South Africa, as noted by the judge at [26]:

> The approach of the courts to signatures has therefore been pragmatic, not formalistic. They look to whether the method of the signature used fulfils the function of a signature – to authenticate the identity of the signatory – rather than insist on the form of the signature used.

Guarantees and debt

7.131 That email correspondence is used extensively for business has become a fact that judges now take for granted. An exchange of emails occurred in respect of a debt claimed in two amounts, one of A$33,884.02 and the other of A$2,859.14, in respect of two different companies in a case before the Federal Circuit Court of Australia in *Austral-Asia Freight Pty Ltd v Turner*.[1] Hartnett J concluded, at [30], that there was an objectively manifested intention to be legally bound, that it was conveyed in sufficient writing, and that the name typed at the end of the emails constituted a signature for the purposes of s 126 of the Instruments Act 1958 (Vic). In New Zealand, in the case of *Sanson v Parval Marketing Limited*,[2] upheld on appeal under *Gachot v Sanson*,[3] it was accepted that the first name of a person typed into an email is capable of forming part of the evidence to demonstrate the assignment of a guarantee.

1 [2013] FCCA 298 (2013), 2013 WL 2253153; Dane Weber, 'Tech neutrality in Australian signature law' (2015) 24 JL Inf & Sci 101.
2 [2008] NZHC 87 (11 February 2008).
3 [2009] NZCA (CA95/2008) 86; Barry Allen, 'The validity of informal guarantees' (2013) 13 Otago L Rev 57.

Public administration, the judiciary and the police

7.132 In *Badre v Court of Florence, Italy*,[1] an extradition order was made in enforcement of a European Arrest Warrant. The electronic signature on the certificate issued by the

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Serious Organised Crime Agency was challenged because, it was argued, it was not subscribed with a physical signature in ink, but with an electronic signature in the form of letters and a number: 'GW (200820)'. There was no other dispute about the content of the certificate. It was accepted that in all other respects the document produced was a proper certificate. The certificate was issued under the provisions of s 2(7) and (8) of the Extradition Act 2003. The purpose of the certificate is to assert the authority to issue an arrest warrant under the Act. Counsel for the appellant submitted that the provision of a proper certificate under s 2 of the Act is a precursor to the validity of the warrant and the subsequent jurisdiction of the court. When a certificate is issued, the requested person may be lawfully arrested. The powers of the court follow on from such an arrest. If the arrest cannot be shown to be lawful, the court has no jurisdiction. Mr Summers argued that a machine purported to issue the certificate in this case. McCombe LJ rejected this argument, indicating that it seemed clear that the designated authority provided the certificate. The official causing the certificate to be issued used their initials GW and an identifying code as a means of authentication. The electronic form of the signature on the certificate did not act to detract from the validity of it. The judge then went on to observe, at [16], that a manuscript signature would be preferable:

> It is perhaps unfortunate that the electronic age has produced more haste and less speed, because it has thrown up this technical argument where none existed before. It must surely be the easiest task in the world to produce a signature in ink, or at least the full name and designation of the individual certifying and perhaps an official stamp or rubric confirming that that individual does indeed certify the contents of the document to lend some additional force of authority to the certificate that is being produced. I would hope that SOCA would consider either reverting to the old practice of producing these certificates, properly signed by a real person, in the form that was actually used in an earlier warrant in this case (subsequently withdrawn); or at least better identifying the individual making the certification on the face of the document.

1 [2014] EWHC 614 (Admin), [2014] 3 WLUK 250, [2014] ACD 933.

7.133 An identical point was taken in *The Queen on the Application of Neculai Jugan v Deta Court of First Instance, Romania*,[1] where a certificate was issued pursuant to s 2(7) of the Extradition Act 2003. It was dated 28 May 2013, and below the date were the words 'Signed LT' in type, and underneath that '#101782'. The appellant contended that this was not a valid signature, which meant that an essential procedural requirement had not been made out. This argument was rejected on the basis that a witness gave written evidence confirming the signature and the authenticity of the certificate.

1 [2014] EWHC 460 (Admin), [2014] 2 WLUK 261.

7.134 Many police forces in the United Kingdom now use digital systems to implement and record decisions, as in the case from Scotland of *HM Advocate v Purves*,[1] as explained by Maciver S at [7]:

> I found from that evidence that the procedure within Lothian and Borders Police is that the applications from various officers for directed surveillance are dealt with by a secure online system which meets that Force's requirements in respect of security and accessibility. A password system is used which means that only selected and appropriate individuals can access the system and once authorization has been given by a detective superintendent the authorization cannot be altered. The applying officer makes his application by typing the grounds for his request in his online

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> application and that is read on screen by a detective superintendent or superior rank who, having considered the application, either grants or refuses authorization. If authorization is granted as in this case, the reasons for authorization are typed personally by the superintendent and thus entered into the secure system.

1 2009 GWD 30-479, [2009] HCJ 2, 2009 SLT 969, [2009] ScotHC HCJ_2, 2010 SCL 88.

7.135 In this instance, the solicitor advocate for the first accused argued that the authorization for directed surveillance granted by the police superintendent in terms of the Regulation of Investigatory Powers (Scotland) Act 2000 was not in writing until it was printed off, and it could not therefore be a valid authorization until that time, and that when it was printed off, it did not have the signature of the authorizing superintendent and was also defective on that account. The Sheriff rejected both arguments. As a matter of general principle, he dismissed the first argument at [11]:

> I found on a simple basis of commonsense and reality, that it must be accepted and understood that in every phase of life, society has moved forward, and specifically in this connection has moved on from only producing documents in pen and ink, and that the development is normal and acceptable. I did not find it an acceptable or reasonable argument that an online document which had not yet been printed off but which had been typed and was viewable on a screen was not to be regarded as being 'in writing'. I came to the view that such a document, having been prepared in this case by Detective Superintendent Doneghan personally by depressing the keys on his personal computer and by the use of a secure system, was in fact a written document and was preserved for future use within Lothian and Borders Police online system. I consider it to be a flawed argument to suggest that that document could not be regarded as a written document until it was actually printed off and could be held in the hand for reading purposes.

7.136 Regarding the issue of whether the authorization was signed, there is no requirement for the document to be signed under the provisions of the statute, so it follows that the authorization was valid.[1]

1 For an electronic facsimile in Scotland, see *Scrimgeour-Wedderburn v Procurator Fiscal, Kirkcaldy* [2019] HCJAC 57.

Statute of Frauds

7.137 Email is a particularly useful means of communicating and negotiating the terms of contracts. Aside from the question as to whether the content of an exchange of emails is sufficient to demonstrate the formation of a contract, one of the issues is whether the exchange of electronic communications was signed, and if so, whether the emails were sufficiently signed under the relevant Statute of Frauds, or whether the signatures in an exchange of emails between the parties clearly identified the parties. In Canada, an electronic signature in an email was held to constitute a signature under the Statute of Frauds 1677.[1] In England and Wales, Clarke J considered that a series of emails was capable of constituting writing under the Statute of Frauds in *Golden Ocean Group Limited v Salgaocar Mining Industries PVT Ltd*,[2] and said, at [103], that 'an email, the text of which begins "Paul/Peter", may be regarded as signed by Peter because by that form of wording Peter signifies that he is addressing Paul and authenticates the content of the whole of what follows'. On appeal before the Civil Division of the Court of Appeal,[3] Tomlinson LJ saw no reason why a series of emails ought to be excluded from the Statute of Frauds. He said, at [22]:

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> I can see no reason why the contract of guarantee so identified should not be regarded as an agreement in writing for the purposes of the Statute … I can see no objection in principle to reference to a sequence of negotiating emails or other documents of the sort which is commonplace in ship chartering and ship sale and purchase. Whether the pattern of contract negotiation and formation habitually adopted in other areas of commercial life presents difficulty in adoption of the same approach must await examination when the problem arises. Nothing I have said is intended to discourage the obviously sensible practice of incorporating a guarantee either in a readily identifiable self-standing document or otherwise providing for it as part of the terms of a formally executed document. The Statute must however, if possible, be construed in a manner which accommodates accepted contemporary business practice. The present case is not concerned with prescribing best or prudent practice. It is concerned with ensuring, so far as is possible, that the adoption of usual and accepted practice cannot be used as a vehicle for injustice by permitting parties to break promises which are supported by consideration and upon which reliance has been placed.

1 *Leoppky v Meston* 2008 ABQB 45 (CanLII).
2 [2011] EWHC 56 (Comm), [2011] 1 WLR 2575, [2011] 2 All ER (Comm) 95, [2011] 1 WLUK 356, [2011] 1 CLC 125, [2011] CILL 3022, [2011] CLY 3112.
3 *Golden Ocean Group Ltd v Salgaocar Mining Industries PVT Ltd* [2012] EWCA Civ 265, [2012] 1 WLR 3674, [2012] 3 All ER 842, [2012] 2 All ER (Comm) 978, [2012] 1 Lloyd's Rep 542, [2012] 3 WLUK 313, [2012] 1 CLC 479, [2012] CILL 3161, (2012) 162 NLJ 425, [2012] CLY 3047.

7.138 The court dismissed the arguments that the name 'Guy' at the end of the email was not a signature, and no more than a salutation, and one typed in a 'matey' or familiar fashion, or in the alternative, if it was a signature, it was only the signature of a communication and not appropriate or effective to authenticate a contract of guarantee. The court considered that the name was typed in a manner that indicated that it was intended to authenticate the document, and agreed that an electronic signature is sufficient and that a first name, initials or a nickname will suffice.

Wills

7.139 There are circumstances when a will has been considered for probate as a result of being written on a computer, and it is conceivable that a court may be required to consider the content of an email that is clearly testamentary in character – perhaps an email sent by a serviceman or woman while on active duty.[1]

1 Jeremy Malcolm, a lawyer in Australia, signed his will using digital signatures; see Angus Kidman, 'Australian makes digital will', ZDNet Australia, 20 January 2004, http://www.zdnet.com/article/australian-makes-digital-will/, (2004) 1 Digital Evidence and Electronic Signature Law Review 90; Michael Cameron Wood-Bodley, 'Wills, data messages, and the Electronic Communications and Transactions Act' (2004) 21 The South African Law Journal 526; Law Commission, *Making a Will* (Consultation Paper 231, 2017), ch 6 on electronic wills – the Law Commission has yet to finalize its recommendations at the time of writing.

7.140 An early example of a will prepared in digital form is the Quebec case of *Rioux v Coulombe*,[1] where the police found a note after the testator committed suicide on 4 May 1996 that led to the discovery of a diskette, with the following text written by hand on the label: 'Ceci est mon testament/Jacqueline Rioux/1er février 1996' ('This is my will/Jacqueline Rioux/1 February 1996'). A single electronic file was stored on the disk, comprising directions of a testamentary nature. There was no signature in the document. The file had been last saved on 16 April 1996 at 10:25 am. On the same

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

day, the testator wrote in her diary that she had made a will on her computer, bearing the date 1 February 1996. Michaud, greffier (master) of the Quebec Superior Court, decided that the text did not meet the requirements of article 726 of the Code civil du Québec requiring a holograph testament.[2] However, he found the electronic will to be valid under the dispensing power of Quebec. In so doing, he failed to address any of the evidential issues that arose out of the circumstances.[3] Such matters were covered in the South African case of *Macdonald v The Master*,[4] where the deceased committed suicide on or about 14 December 2000 and left in his own handwriting four notes dated 13 December 2000 on a bedside table next to the bed on which he was lying. One of the notes read as follows:

> I, Malcom Scott MacDonald, ID 5609065240106, do hereby declare that my last will and testament can be found on my PC at IBM under directory C:/WINDOWS/MYSTUFF/MYWILL/PERSONAL.

1 1996 CarswellQue 1226, 19 ETR (2d) 201, JE 97-263, EYB 1996–87749.

2 Brown J considered the meaning of the word 'holograph' in detail in the case of *In the Matter of the Estate of Reed v Buckley*, 672 P.2d 829 (Wyo. 1983) at 831–832, and reached the logical conclusion that a tape recording could not be considered to be a piece of writing. It follows that a will drafted using digital data cannot be a holographic will.

3 Nicholas Kasirer, 'From written record to memory in the law of wills' (1997–8) 29 Ottawa Law Review 39, suggested, at 44, that the Master was somewhat perfunctory in deciding that the diskette and the text recorded on it did not constitute a holographic will, missing the opportunity of testing the elasticity of the ordinary rules of form, and he went on to discuss the evidential problems that were not addressed (44–48).

4 2002 (5) SA 64; Michael Cameron Wood-Bodley, '*Macdonald v The Master*: computer files and the "rescue provision" of the Wills Act: notes' (2004 January) 21(1) South African Law Journal34; Sizwe Snail and Nicholas Hall, 'Electronic wills in South Africa' (2010) 7 Digital Evidence and Electronic Signature Law Review 67; see also Juliet Brook, 'Succession: to dispense or not to dispense? A comparison of dispensing powers and their judicial application' (2019) 1 PCB 9.

7.141 The deceased was employed as a senior IT specialist with IBM Global Services. The evidence before the court was that the personal computer allocated to the deceased was controlled by a password that only the deceased knew. Each employee with a personal computer at IBM was required to change their password every month, to record the password on a piece of paper, seal it in an envelope and hand it over to an employee whose job was to safeguard the passwords by keeping them in a locked facility. Only three senior members of staff had the right to request the password. Mr Dimmick, the Professional Development Manager, had a right to obtain the password. On 14 December 2000 he obtained access to the computer and printed the contents on to paper. The document purported to be the deceased's last will and testament. It was handed to his widow and the file was then deleted. The document had the following heading: LAST WILL AND TESTAMENT FROM MALCOLM SCOTT MACDONALD. The first paragraph read:

> I, the undersigned, Malcolm Scott Macdonald (ID 5609065240106), divorced, do hereby revoke all wills, codicils and other testamentary acts heretofore made by me and declare the following to be my last will and testament.

7.142 The document then appointed an executor and set out the disposition of the deceased's property, but it was neither dated nor signed by any witnesses or the deceased. The Master refused to accept the will, because it failed to comply with the provisions of the Wills Act 34 of 1964, s 2(1)(a), in that it is necessary for a will

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

to be in writing, signed and attested by two competent witnesses, and the testator must initial every page. Hattingh J set out the requirements necessary for the will to be accepted at 70 F–G:

> In order to be successful with their application under this section, the applicants must, on a balance of probabilities, establish:
>
> (a) the documents, annexures A and F were drafted by the deceased;
>
> (b) that the deceased had died since the drafting of the documents; and
>
> (c) the documents were intended by the deceased to be his will.

7.143 It was necessary to decide whether the requirements of s 2(3) had been satisfied. It reads:

> If a court is satisfied that a document or the amendment of a document drafted or executed by a person who has died since the drafting or execution thereof, was intended to be his will or an amendment of his will, the court shall order the Master to accept that document, or that document as amended, for the purpose of the Administration of Estates Act, 1965 (Act No. 66 of 1965), as a will, although it does not comply with all the formalities for the execution or amendment of wills referred to in subsection (1).

7.144 Hattingh J commented that the legislature introduced s 2(3) with the intention of eliminating injustice and inequity where a person failed to comply with the formalities set out in s 2(1). It was necessary to determine whether the deceased drafted the documents. Of the two approaches that could be adopted (the document must be drafted in the deceased's handwriting, or the document may be typed by the deceased or even dictated by the deceased), the judge adopted the liberal approach, commenting at 71A–B that:

> The retention of the formal requirements of s2(1) and the peremptory nature of s2(3) do not justify a strict interpretation of s2(3). Not only is this inconsistent with the very purpose of s2(3), namely to prevent the last wishes of a testator from being nullified by a non-compliance with technical formalities, but it also does not take cognizance of the realities of the technological world we live in.[1]

1 Hattingh J gave detailed reasons for trusting the digital data and the surrounding circumstances at 71G–J.

7.145 The second point, that the deceased had died since the drafting of the documents, was accepted, as was the third point, that the testator intended the draft will to be his last will and testament. Hattingh J usefully set out the factors at 72C–G that were of importance in reaching his decision:

> (a) the documents are a clear indication of the deceased's intention that they should be regarded as his will and testament;
>
> (b) the documents are not preliminary sketches or notes for discussion with an attorney or anybody else to draft a will, but his final wishes;
>
> (c) there is no element of suspicion of fraud attached to the documents and their reproduction;
>
> (d) there is no suspicion that there could have been any tampering with the computer or the documents;

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

(e) not only did the documents exist on the computer, but there was indeed clear reference by the testator to these specific documents in his notes;

(f) there was a clear indication by the deceased where this document could be found on his computer;

(g) only the deceased had access, by way of secret password, to put the documents on the computer;

(h) only the deceased could have typed the said documents;

(i) they could only be extracted upon the instructions of the deceased in his own handwriting and only with the deceased's own secret code.

7.146 In this case, Hattingh J concluded, at 72I–J, that s 2(3) called 'for an approach which promotes an extensive or flexible interpretation. This is also in accordance with the spirit of the technological age. ' Although the testator did not sign his name in the document, it could be argued that the password served a similar function.

7.147 In the Saskatchewan case of *Buckmeyer Estate (Re)*,[1] the executor proffered three documents for admission to probate: a will dated 5 May 2007, an email dated 23 August 2007 and an amendment to the will dated 27 August 2007. The will was properly proven. The issue to be determined was whether the email and the amendment were testamentary documents and whether s 37 of The Wills Act, 1996, S.S. 1996 c. W-14.1 applied. The email was from the deceased, John Buckmeyer, to the executor (johnbuckmeyer@hotmail.com to dave.gibson@sasktel.net). The subject was 'John's arrangements'. The email consisted of two pages. It was accepted that he wrote the email and that it contained his electronic signature. The content indicated that he was very sick and in his last days, and stated that he wanted to give the executor more information and express his wishes clearly before he died. The deceased listed his credit accounts, gave a direction with respect to his cremation, where his ashes were to be sent and directions with respect to funeral services. Ottenbreit J considered the provisions of the Electronic Information and Documents Act 2000, S.S. 2000 c. E-7.22 in respect of the electronic signature in the email. The judge, it is respectfully suggested, correctly indicated that the issue was whether the content of the email complied with the provisions of the Wills Act. The issue was whether the content of the email constituted a disposition intended to take effect on death, reflecting testamentary intention, as an essential element for a clause to be considered testamentary is the disposal of property. In this instance, Ottenbreit J decided that the purpose of the email was to provide additional information to the executor in carrying out his duties. It was not a testamentary document and therefore not admitted to probate.

1 2008 SKQB 260 (CanLII).

7.148 There have been a number of cases in Australia where wills have been made only in electronic form. Aside from deciding whether the electronic will is valid, the judges have also had to decide whether a will is signed where the deceased typed their name into the document. In the case of *In the will of Mark Edwin Trethewey*,[1] Beach J concluded that typing the name at the foot of the document was the equivalent of a signature in the circumstances of the case.[2]

1 [2002] VSC 83 (14 March 2002).

2 Other cases from Australia include: Queensland: *Mellino v Wnuk* [2013] QSC 336, where the deceased recorded his testament on to a DVD before taking his own life; *Re Yu* [2013] QSC 322, where

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

shortly before the deceased took his own life he created a series of documents on his iPhone, typing his name at the end of the document in a place where on a paper document a signature would appear, followed by the date, and a repetition of his address; *Re Nichol; Nichol v Nichol* [2017] QSC 220, where the deceased created a text message stating a testamentary intention on his mobile telephone without sending it shortly before he took his own life, signing it 'MRN190162Q', which matched the deceased's initials and date of birth, 19 January 1962; but see *Mahlo v Hehir* [2011] QSC 243, where McMurdo J concluded that he was not satisfied that Dr Mahlo intended that an electronic document should form her will, because she knew that in writing a new will, she had to do more than type or modify a document upon her computer. She understood that she also had to sign it; New South Wales: *Alan Yazbek v Ghosn Yazbek* [2012] NSWSC 594, where a Microsoft Word document, Will.doc, was completed by the deceased on 14 July 2009 and was found in his laptop computer after his death; *Re Estate of Wai Fun Chan, Deceased* [2015] NSWSC 1107, where the deceased made a will by video; *The Estate of Roger Christopher Currie, late of Balmain* [2015] NSWSC 1098, where a will written by the deceased in a computer file, ending 'Signed by the writer Roger Christopher Currie on this day Wednesday, 1 April 2009', was granted probate; South Australia, In the *Estate of Wilden (Deceased)* [2015] SASC 9, where the deceased left two items of a testamentary nature, a DVD containing a video recording of the deceased and a typed document signed by the deceased but not witnessed. For a useful discussion of the case law in the USA, see David Horton, 'Tomorrow's inheritance: the frontiers of estate planning formalism' (2017) 58 BC. Rev 539 and David Horton, 'Wills without signatures' (2019) 99 BUL Rev 1623. In 2007, the Borgarting lagmannsrett (Court of Appeal for the region near Oslo) in Norway was required to determine whether an electronic copy of a testament that was lost could be admitted into probate in the case of LB-2006-27667, for which see Jon Bing, translation and commentary (2008) 5 Digital Evidence and Electronic Signature Law Review 134.

Constitution of a legal entity

7.149 In *Islamic Council of South Australia Inc v Australian Federation of Islamic Councils Inc*,[1] Brereton J observed at [22] that the constitution of the organization did not explicitly require that a request be signed, but went on to observe that 'if it were necessary that it be formally signed, the word "Ramzi" was subscribed to the email with the intent of authenticating the communications, and constitutes a signature notwithstanding that it appears in typewritten and not handwritten form'.

1 [2009] NSWSC 211.

Amending boilerplate contractual terms

7.150 The findings in the above cases, especially those cases that revolve around the exchange of emails, are significant. Even if the Industrial Tribunal decision of *Hall v Cognos Limited* from England and Wales is not binding on any court, it remains a good decision. This is partly because the form of the document is irrelevant. First, the effect the case law should have on the advice that a lawyer gives their clients is highly pertinent, whether dealing with commercial contracts, employment contracts or any other form of relationship that it is possible to create or vary in writing. Consider, by way of example, a standard clause added to most contracts in the following terms:

> The contract shall not be altered unless done so in writing and signed by both parties.

7.151 If the words 'in writing and signed' remain as a standard element in such a clause, it will leave open the probability that contracts, no matter how long they have taken to negotiate, or their apparent length, are susceptible to being varied by an exchange of emails, perhaps between two fairly junior employees, or a person posing as an employee using the company email address.[1] This may well occur because most

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

organizations have now lost control of their means of communication, because all, or virtually all, employees in some sectors have the ability to communicate with the outside world by means of email and other forms of technology, contrary to the position before the introduction of such facilities. This problem will be mitigated to a certain extent in contracts that provide a list of nominated personnel within each organization who have the authority to agree alterations and variations. In such circumstances, if a junior employee agrees an alteration without reference to those who are authorized to agree such changes, any dispute will centre on what, if any, authority was vested in the junior employee, and whether their actions acted to bind the organization. From the point of view of the organization, it is imperative to ensure that its employees are made aware of the effect that a promise can have if made by exchange of email. To mitigate this problem, it may be wise to establish whether the parties are content for a contract to be altered by exchange of emails, and if not, to include an amended version of the standard clause, such as:

> The contract shall not be altered unless done so in writing on paper and signed with the manuscript signature of both parties.

1 As occurred in *CSX Transportation, Inc. v Recovery Express, Inc.*, 415 F.Supp.2d 6 (D.Mass. 2006).

7.152 The *Hall v Cognos Limited* case illustrates the ease by which a contract can be varied, as does *C&S Associates UK Ltd v Enterprise Insurance Company Plc*,[1] the Ohio case of *In re National Century Financial Enterprises, Inc., Amedisys, Inc., v JP Morgan Chase Manhattan Bank, as Trustees*[2] and the New York case of *Stevens v Publicis, S.A.*[3] A further point centres on whether the use of email is appropriate and reasonable in the circumstances. Whether the use of email is a reasonable means of communication between two parties, or any number of parties, will depend on a range of factors, as indicated by Marrero DJ in *Bazak International Corp. v Tarrant Apparel Group*,[4] where he commented, at 387–388:

> Nonetheless, whether email is an appropriate and reasonably expected form of communication between the two particular parties before the court is a question of fact. Here, the issue's resolution requires a factual inquiry into trade usage and course of dealing … Neither party directly addresses whether email is an appropriate method of communication in the re-sale trade generally or in Tarrant and Bazak's particular relationship. Yet later email correspondence from Tarrant to Bazak (the 'GMAC email') provides evidence in light of which a reasonable jury could find that the parties did accept email as an appropriate form of communication.

1 [2015] EWHC 3757 (Comm), [2015] 12 WLUK 703.
2 310 B.R. 580 (Bkrtcy.S.D.Ohio 2004).
3 50 A.D.3d 253, 854 N.T.S.2d 690, 2008 N.Y. Slip Op. 02880.
4 378 F.Supp.2d 37758 (S.D.N.Y. 2015).

7.153 This view corresponds with that expounded in *Campbell v General Dynamics Government Systems Corporation*,[1] although this issue was never debated with other forms of communication, such as the use of telegrams or telex.[2]

1 321 F.Supp.2d 142 (D.Mass. 2004), affirmed 407 F.3d 546 (1st Cir. 2005).
2 The position is reinforced in the case of *Basis Technology Corporation v Amazon.com, Inc.*, 71 Mass. App.Ct. 29, 878 N.E.2d 952 (Mass.App.Ct. 2008).

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

The name in an email address

7.154 The name in an email address is capable of identifying a person. This is particularly so where an email address in an organization, whether public or private, is allocated by setting out the name of the person followed by the domain name of the organization. There are other variations that can be used, such as when an email address describes the office or function of the person, rather than their name. However, even this, if allocated to a single person, can also function to identify an individual. The link between the prefix of the email address and the person responsible for sending the email can be problematic: for instance, the sender may be able to choose the first part, and may decide to adopt letters or numbers or a combination of letters and numbers with a view to obfuscating their identity. Further, the sender might hide the true email address. If it was not obvious who the sender was, and if correspondence ensues and a dispute occurs, it will be a matter of establishing what, if any, evidence there is pertaining to the source of the relevant emails as a preliminary point. It has been held in a number of jurisdictions that the name in an email address, or the combination of the name and the domain name in an email address can be a form of electronic signature.

Limitation Act 1969 (NSW)

7.155 The case of *McGuren v Simpson*[1] raised the issue as to whether correspondence by email was capable of constituting an acknowledgement that was in writing and signed for the purposes of the Limitation Act 1969 (NSW). Mr Simpson and Ms McGuren were in a relationship between 1992 and 2000. Mr Simpson received a cheque for A$23,000 when he was in prison in November 1993 in respect of a claim for damages for personal injuries he suffered in a motor vehicle accident. He endorsed the cheque in favour of Ms McGuren's sister to enable her to bank the cheque in her account on behalf of Ms McGuren (Ms McGuren did not want to pay the cheque into her own account as it would have affected the state benefits she was receiving at the time). Mr Simpson claimed that the defendant used the money almost entirely for her own purposes and he sought recovery of the money from Ms McGuren. Ms McGuren asserted that she used the money in accordance with his instructions and with his approval. Mr Simpson's main item of evidence was in the form of an email sent to him by Ms McGuren. It read in part:

> Date: Wed, 29 Sep 1999 14 16.20+1000
>
> To: "Rob – yahoo"<Robert-john-simpson@yahoo.com.au>
>
> From: "McGuren, Kim" Kim.Mcguran@air.gov.au
>
> I am going to try and book a cab for 6pm at childcare does that suit you?
>
> It probably won't turn up but I may as well book it. So, what do you want to do: split up, – go to counselling or – just blame each other for every thing since everything is obviously the other persons fault, for the rest of our lives? Yes, I spent the money and I shouldn't have and yes, you have been violent and you shouldn't have so what now??

1 [2004] NSWSC 35.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.156 Master Harrison dealt with an appeal from a Local Court Magistrate, and the main issue to determine was whether Mr Simpson's cause of action was statute barred under s 14 of the Limitation Act 1969 (NSW). The time limit is extended under the provisions of s 54 where the person against whom the cause of action lies confirms the cause of action by acknowledging it to the person who holds the action, providing the acknowledgment is in writing and signed by the maker. Mr Simpson's case was that Ms McGuren acknowledged the cause of action in the email she sent when she wrote the words 'Yes, I spent the money and I shouldn't have'. The Magistrate had previously determined that the email was an electronic communication within the meaning of s 9(1) of the Electronic Transaction Act 2000 (NSW). However, the Act was not in force at the time the email was sent, which meant the provisions of the Act did not apply to the email, hence the Magistrate's decision was incorrect. Master Harrison dealt with the problem in the context of the common law. First, he concluded that the email constituted a written document. In so doing, he noted the expansive approach taken in other jurisdictions [at 20], and decided to construe the Act to take into account the changes in technology [at 21], a view taken by judges in England and Wales and the USA in the nineteenth century: 'It is my view that … section 54 of the Act ought to be read to accommodate technological change and that, accordingly, the email sent by the plaintiff constitutes a written document'. Second, he agreed with the decision of the Magistrate, that the email address was a signature for the purpose of s 54(4) of the Limitation Act 1969 (NSW), at [22]:

> As Ms McGuren's name appears in the email and she expressly acknowledges in the email as an authenticated expression of a prior agreement, the email is recognisable as a note of a concluded agreement. Accordingly, the Magistrate was correct at law to conclude that Ms McGuren signed the email and that the requirements of s 54(4) of the Act were met. It was open to the Magistrate to find that Ms McGuren acknowledged the claim and she has admitted her legal liability to pay Mr Simpson that which he seeks to recover.

Statute of Frauds

7.157 The question arose in the English case of *J Pereira Fernandes SA v Mehta*[1] whether the name forming part of an email address could be construed as a signature. J Pereira Fernandes SA is a Portuguese company that supplied bedding products in July 2002 to Bedcare (UK) Limited,[2] a company of which Mr Mehta was a director. Bedcare failed to pay for the products it had received, and was wound up on a Petition by J Pereira Fernandes SA by an Order made on 7 March 2005. The cause of the appeal before His Honour Judge Pelling QC, sitting as a judge of the Chancery Division, related to the presentation of a winding up petition by J Pereira Fernandes SA on 12 January 2005. On 20 February 2005 an email was sent from the email address 'Nelmehta@aol.com' to Ian Simpson & Co, solicitors acting for J Pereira Fernandes SA.[3] Mr Mehta's name was not typed at the end of the email. On 9 November 2005, District Judge Harrison gave summary judgment to J Pereira Fernandes SA in the sum of £24,985.53 and ordered Mr Mehta to pay the costs of the claim, which were summarily assessed in the sum of £1,080.00. Mr Mehta was subsequently given permission to appeal by Holman J on 20 February 2006. The email contained the following text:

> I would be grateful if you could kindly consider the following.
>
> If the hearing of the Petition can be adjourned for a period of 7 days subject to the following:

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> a. A Personal Guarantee to be given in the amount of £25,000 in favour of your client – together with a list of my personal assets provided to you by my solicitor
>
> b. A repayment schedule to be redrawn over a period of six months with a payment of £5,000.00 drawn from my personal funds to be made before the adjourned hearing
>
> I am also prepared to give a company undertaking not to sell market or dispose of any company assets without prior consent from your client pending the signing of the Personal Guarantee.

1 [2006] EWHC 813 (Ch), [2006] 1 WLR 1543, [2006] 2 All ER 891, [2006] 1 All ER (Comm) 885, [2006] 2 Lloyd's Rep 244, [2006] 4 WLUK 182, [2006] Info. TLR 203, Times, 16 May 2006, [2006] CLY 774, also known as *Metha v J Pereira Fernandes SA*.
2 A search on the website of Companies House for Bedcare (UK) Limited does not reveal any results, and there are no results for a person by the name of Nilesh Mehta associated with a legal entity known as Bedcare (UK) Limited.
3 In the reports, it is said that Mr Mehta caused one of his members of staff to send the email. The email was sent on Tuesday 20 February 2005 at 20:30. It was subsequently confirmed in May 2006 to Ian Simpson & Co by the Insolvency Service in Manchester that no employee or salary records were recorded as being delivered up for Bedcare (UK) Limited (information provided by Ian Simpson & Co to the author).

7.158 The email address that appeared on this particular email also appeared on other emails sent to Ian Simpson & Co by Mr Mehta, which included his name typed at the end of the email. There were two matters of relevance to consider: whether the email could be considered a sufficient note or memorandum, and if so, whether it was signed by the party charged, that is, or on behalf of Mr Mehta. The email was a rare example of a document that is brought into the purview of s 4 of the Statute of Frauds 1677.[1] This is because s 4 now only applies to contracts of guarantee, and the content of this email provided a guarantee, in that Mr Mehta offered to personally cover debts owed by the company. Section 4 reads:

> Noe action shall be brought … whereby to charge the defendant upon any speciall promise to answere for the debt default or miscarriages of another person … unlesse the agreement upon which such action shall be brought or some memorandum or note thereof shall be in writeing and signed by the partie to be charged therewith or some other person thereunto by him lawfully authorised.[2]

1 For a history of the Statute, see W. S. Holdsworth, *A History of English Law Volume VI* (Methuen & Co 1924), 379–97, who considered that the Statute was out of date when he wrote this text, at 396: 'the prevailing feeling both in the legal and the commercial world is, and has for a long time been, that these clauses have outlived their usefulness, and are quite out of place amid the changed legal and commercial conditions of to-day.'; E. Rabel, 'The Statute of Frauds and comparative legal history' (1947) 63 Law Quarterly Review 174, in which he concluded, at 187, 'The case against the Statute of Frauds has been proved time and again by outstanding authorities, even before the Sixth Interim Report of the English Law Revision Committee of 1937 solemnly pronounced sentence for repeal. An examination of the historical background on which the Statute arose can but support the views expressed by the Revision Committee and the conclusion that the Statute essentially belongs to distant times, far removed from the conditions of modern life'; Lord Wright, *Legal Essays and Addresses* (Cambridge University Press 1939), 226; for a discussion of the purpose and additional sources of criticism, see Graham S. McBain, 'Legislative comment abolishing the Statute of Frauds 1677 section 4' (2010) 5 Journal of Business Law 420, who concluded, at 433: 'When dealing with ancient legislation it is easy to develop a visceral fear akin to that of Vitalstatistix in the Asterix cartoons. He has only one fear: he is afraid that the sky may fall on his head tomorrow. However, as he always says, tomorrow never comes. If s.4 is repealed, one would assert that the legal sky will not fall: the number of oral guarantees given will not increase,

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

nor the amount of litigation concerning them. And there is no reason to believe that, in the case of oral guarantees giving rise to litigation, the English judiciary will fail to be vigilant in detecting perjury.'

2 *Halsbury's Statutes of England and Wales Volume 11(1)* (4th edn, 2010 reissue), 7; Chronological Table of the Statutes Part 1 (HMSO).

7.159 Harrison DJ, in giving summary judgment, considered that the email did amount to a note or memorandum of guarantee, although he did not explicitly comment on whether the names in the email address could amount to a signature. Judge Pelling QC agreed with Harrison DJ on this point, and also held the email to be a note or memorandum that brought it within s 4 of the statute. He commented on the purpose of the statute as follows at [16]:

> The purpose of the statute of frauds is to protect people from being held liable on informal communications because they may be made without sufficient consideration or expressed ambiguously or because such a communication might be fraudulently alleged against the party to be charged. That being so, the logic underlying the authorities I have referred to would appear to be that where (as in this case) there is an offer in writing made by the party to be bound which contains the essential terms of what is offered *and* the party to be bound accepts that his offer has been accepted unconditionally, albeit orally, there is a sufficient note or memorandum to satisfy s 4.

7.160 The second question to consider was whether the email had been signed. Solicitors for J Pereira Fernandes SA already had a number of emails from Mr Mehta in which he included his name typed at the bottom of the text. In this respect, the evidence of a number of communications from the same address demonstrated that they were authentic. Mr Mehta did not dispute that the email was sent.

7.161 The evidence upon which a decision could be made in *Fernandes* was more substantial than the evidence that Prakash J (as she then was) dealt with in *SM Integrated Transware Ltd v Schenker Singapore (Pte) Ltd*.[1] In this instance, Judge Pelling QC took the view that the email address was similar to an automatically generated name and facsimile number of the sender of a facsimile transmission, although his comments, at [19], noted that a human being had to type the data into the software:

> As is well known to anyone who uses email on a regular basis, what is relied upon is not inserted by the sender of the email in any active sense. It is inserted automatically. My knowledge of the technicalities of email is not sufficiently detailed to enable me to know whether it is inserted by the ISP with whom the sender or the recipient has his email account. However, I accept Mr Aslett's submission that as a matter of obvious inference, if it is inserted by the latter it can only be from information supplied by the former. Mr Mehta suggested that the address was inserted by his employee. I do not see how this could be so and certainly Mr Mehta was not able to give me a coherent explanation of how that might be so. It is possible that Mr Mehta's employee was authorised to use Mr Mehta's e mail account remotely but, even if that is so, I do not see how that can impact on any of the issues I have to resolve since it is not in dispute that the email was sent on the instructions of Mr Mehta and the method by which the sender address came to be inserted would not be affected even if that was the position.

1 [2005] 2 SLR 651, [2005] SGHC 58.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.162 That such information is considered in judgments to be 'automatic' illustrates a misunderstanding. A human being has to put the information into the machine. The facsimile number of the sender is put into the machine by a person, as is the name in an email address or the 'signature block' of an email.

7.163 Counsel for J Pereira Fernandes SA submitted that the intent to sign was not relevant, and mentioned *Elpis Maritime Co. Ltd. v Marti Chartering Co. Inc.*,[1] which had different facts to the case in point, and also emphasized the decision in *Evans v Hoare*,[2] where the name and address were relied upon to serve as a signature. However, the judge pointed out that in *Evans v Hoare*, Cave J considered, at 597, that the place of the signature was not relevant: 'Whether the name occurs in the body of the memorandum, or at the beginning, or at the end, if it is intended for a signature there is a memorandum of the agreement within the meaning of the statute.' Judge Pelling QC then went on to indicate that the name of the party to be bound must be intended as a signature. In reaching this conclusion, the judge did not refer to the comments made by Cave J (at 597–598, (reference omitted)) after the text he quoted, which are highly significant:

> In the present case it is true that the name of the defendants occurs in the agreement; but it is suggested on behalf of the defendants that it was only put in to shew who the persons were to whom the letter was addressed. The answer is that there is the name, and it was inserted by the defendants' agent in a contract which was undoubtedly intended by the defendants to be binding on the plaintiff; and, therefore, the fact that it is only in the form of an address is immaterial. A case was referred to in the argument, *Schneider v Norris*, in which a printed bill-head was held to amount to a signature within the meaning of the statute. That is a stronger case than the present. The printed heading there was not put into the document for the purpose of constituting a memorandum of the contract; but it was so used with the assent of the party sought to be charged, and it therefore was held to have the effect of a signature. This shews that it is unimportant how the name came to be inserted in the document.

1 [1992] 1 AC 21, [1991] 3 WLR 330, [1991] 3 All ER 758, [1991] 2 Lloyd's Rep 311, [1991] 7 WLUK 297, (1991) 141 NLJ 1109, (1991) 135 SJLB 100, [1992] CLY 3931.
2 [1892] 1 QB 593, (1892) 66 LTRep NS 345.

7.164 The judge considered that the approach he took was supported by the decision in *Caton v Caton*.[1] The facts in this case might be compared to the decision in the case decided by the Master of the Rolls, *De Biel v Thomson*,[2] and subsequently affirmed by the Lord Chancellor and reaffirmed upon further appeal, *Hammersley v De Biel, an infant, by Blake*,[3] where an extremely vague promise, the evidence of which was very tenuous, was upheld under the Statute of Frauds.

1 (1867) LR 2 HL 127.
2 3 Beav. 469.
3 [1845] 12 Clark & Finnelly 45, 8 ER 1312.

7.165 Earlier cases on the physical position of the signature also emphasizes the need to consider the intent behind the signature, as commented on by the Lord Chief Baron in *Stokes v Moore*.[1] In *Ogilvie v Foljambe*,[2] a letter written by the plaintiff relating to the sale of a lease situated in Grosvenor Place began 'Mr Ogilvie has the pleasure to acquaint Mr Foljambe …' In this instance, Sir William Grant MR held the name governed all that followed in the letter. In *Holmes v Mackrell*,[3] a promissory note written in the

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

hand of the defendant with his name written on top, but not signed at the end, was held to be a sufficient signature for the document. In his judgment at 796, Crowder J intimated why this issue was of some importance:

> In the case of a note written in the third person, the name at the commencement serves to authenticate the document just as well as a formal signature at the foot of it. If, then, the signature is sufficient, what does the defendant say here? In effect he says, – 'I have given two promissory notes for 510*l*., and I am now liable upon them'. That is a plain and deliberate and unconditional acknowledgment of a debt, and it is clear from the case of *Tanner v Smart*, 6 B. & C. 603, 9 D. R. 549, and the authorities which have followed it, that, where there is an absolute and unconditional acknowledgment of an existing debt, a promise to pay is to be inferred. It seems to me that the acknowledgment here is one from which a promise to pay must necessarily be inferred.

1 (1786) 1 Cox 219, 29 ER 1137.
2 (1817) 3 Mer 53, 36 ER 21.
3 (1858) 3 CB (NS) 789, 140 ER 953.

7.166 It appears that judges, when dealing with cases where a promise was made that affected an innocent party, and the person making the promise subsequently sought to avoid being held to their promise by arguing a technical point that the promise was not signed, thus making it unenforceable, were generally not willing to allow the person making the promise to succeed on such a technicality. Two of the most notable English cases, *Lobb and Knight v Stanley*[1] and *Tourret v Cripps*,[2] neither of which was cited or discussed in *Fernandes*, illustrates that similar situations had arisen in the past, and lawyers and judges have previously been required to deal with similar factual situations as in *Fernandes*. In *Lobb*, Stanley, a certified bankrupt, gave a written promise signed by him after his bankruptcy. Three undated letters were produced, one of which read 'Mr Stanley begs to inform Mr Lobb …' It was considered sufficient that he began the text with his name, and his name governed the promise that followed.[3] In *Tourret v Cripps*,[4] Mr R. L. Cripps wrote in his own hand on a sheet of memorandum paper an offer to lease parts of 14 and 15 Mortimer Street, Cavendish Square. The memorandum was not signed by him, but contained, at its head, the words 'From Richd. L Cripps' and his address. Tourret, who initiated an action against Cripps for specific performance, accepted the offer. His printed name served as a signature to hold him to the promise he made.

1 (1844) 5 QB 574, 114 ER 1366.
2 (1879) 48 L J Ch 567, 27 WR 706.
3 This case was specifically mentioned by Phipson, where a 'signature under the Statute of Frauds may be by surname only' (S. L. Phipson, *The Law of Evidence* (6th edn, Sweet and Maxwell 1921), 516).
4 (1879) 48 L J Ch 567, 27 WR 706. These cases were reviewed by Buckley J in *Hucklesby v Hook* 82 LT 117.

7.167 Judge Pelling QC considered the automatic insertion of an email address at [28] and [29] (original emphasis):

> However, that is not the issue in this case. Here the issue is whether the automatic insertion of a person's email address after the document has been transmitted by either the sending and/or receiving ISP constitutes a signature for the purposes of s 4.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> 29. In my judgment the inclusion of an email address in such circumstances is a clear example of the inclusion of a name which is incidental in the sense identified by Lord Westbury in the absence of evidence of a contrary intention. Its appearance divorced from the main body of the text of the message emphasizes this to be so. Absent evidence to the contrary, in my view it is not possible to hold that the automatic insertion of an e mail address is, to use Cave J's language, '*intended for a signature*'. To conclude that the automatic insertion of an email address in the circumstances I have described constituted a signature for the purposes of s 4 would I think undermine or potentially undermine what I understand to be the Act's purpose, would be contrary to the underlying principle to be derived from the cases to which I have referred and would have widespread and wholly unintended legal and commercial effects. In those circumstances, I conclude that the e mail referred to at [3] above did not bear a signature sufficient to satisfy the requirements of s 4.

7.168 In this particular instance, the judge made observations about the technicalities of email in the absence of expert evidence, as did Lyberopoulos J, the president of the court in the Greek case 1327/2001 – Payment Order.[1] It seems that the judge assumed that the ISP adds the email address to the document.[2] He then concluded, in the absence of any relevant technical evidence, that the email address could not, therefore, be intended as a signature. It is suggested that this approach is arguable. It is possible to distinguish the decision by Hall VC in *Tourret v Cripps*[3] on the basis that Cripps wrote the content by hand. That decision must be correct, taking into account the handwritten text, the printed words 'From Richd. L Cripps', and the address printed on the paper. Hall VC might have speculated as to the purpose of having stationery printed, and whether each time a letter or note is sent, the use of the information printed on the letter was sufficient evidence to demonstrate an intent to sign. In this instance, as in other cases, the judge looked to the entire document for evidence to indicate intent, and taking into account the message written on the letter, together with the name printed on the top of the stationery, Hall VC considered that this was sufficient to hold the man to his promise. However, to distinguish *Tourret* from *Fernandes* in this way is far from satisfactory. This is because the facts in *Tourret* comprised a mix of text written by hand with pre-printed text. With networked communications, such a mix is impossible. The very nature of networked communications means that content must be typed – or cut and pasted – so to argue that the decision in *Tourret* is significantly different because of the addition of text written by hand cannot be right.

1 English translation by Michael G. Rachavelias, Case Translation – Greece (2006) 3 Digital Evidence and Electronic Signature Law Review 104; Georgia Skouma, Case Note (2004) 1 Digital Evidence and Electronic Signature Law Review 83.

2 In *Golden Ocean Group Limited v Salgaocar Mining Industries PVT Ltd* [2011] EWHC 56 (Comm), Mr Justice Christopher Clarke indicated, at [103], that 'There is authority that the insertion of a person's email address by an internet service provider after the document has been transmitted is, absent evidence to the contrary, incidental'.

3 (1879) 48 L J Ch 567, 27 WR 706. These cases were reviewed by Buckley J in *Hucklesby v Hook* 82 LT 117.

7.169 Also, Judge Pelling QC did not consider the email as a complete document. The problem with his analysis is that the information contained in the 'From', 'To', 'Sent' and 'Subject' part of the email cannot be disconnected from the body. The information is neither separate when presented visually on a screen, nor when printed out on paper. In addition, the source code (usually hidden) is also an integral part of the email, and

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

this set of metadata is of considerable evidential value, as argued by the applicant in the pleadings in the case of Tribunale Mondovì, 7 giugno 2004, n. 375 (decr.), *Giur. It. 2005, 1026*.[1] Further, should the method used to cause an email address to be attached to a particular email be of relevance, then other factors ought to be considered, including the mechanism by which the application software brings the disparate objects together to permit the user to view the email on screen, because each object will be in a different storage location on the computer.

1 For a translation of the pleadings, see Gian Paulo Coppola, Case Note (2007) 4 Digital Evidence and Electronic Signature Law Review 86.

7.170 A similar issue relating to email correspondence confronted Phelan J in the Canadian case of *Dursol-Fabrik Otto Durst GmbH & Co. c. Dursol North America Inc.*,[1] decided after the decision by Judge Pelling QC, in proceedings for contempt of court where the defendant and his company were the subject of a number of orders prohibiting the marketing and selling of goods. One of the issues to determine was whether the defendant, Robert Scott, used email correspondence to market and sell products. In his evidence, he claimed he was ignorant of two email addresses in issue and how the signature that appeared at the end of emails worked. The evidence indicated he sent out emails that identified him in his corporate capacity. In this case, the court heard appropriate technical evidence as well as the evidence from the defendant. The judge did not believe the defendant because his evidence was both contradictory and inconsistent. In reaching his decision, the judge made some interesting and highly pertinent remarks at 56 about the use of email and the practical aspects of using email that bear repeating:

> Even if one accepted Scott's explanation, which I do not, he was a business man who used computers constantly to transact business. He took no steps to deal with his address and signature. In today's world such ignorance, or, more importantly, the refusal to secure the technical assistance to deal with these types of matters, is not acceptable. Scott exhibited recklessness and a complete disregard for the obligations he had under this Court's Orders.

1 2006 FC 1115.

7.171 The technical evidence demonstrated that, contrary to the defendant's assertions, he could see the default signature he set up, thus contradicting his claim that he was not aware his signature appeared at the end of the email. Further, it was also established that the defendant had a number of different email addresses, and had the option of using whichever address he chose when sending and responding to correspondence. The judge rejected the contention that the defendant's claimed lack of knowledge of email addresses and signatures was a mitigating factor in disobeying a court order.

7.172 One further point might be usefully considered, and that is the purpose of the email address, which is of the utmost significance. The address acts to ensure the communication reaches the person it is addressed to; otherwise, an email address, even if different by one letter, number or dot, is unforgiving. It will not reach its destination, unlike a letter sent by way of post, where a human being can extract information from the envelope and use their knowledge to effect delivery of an envelope incorrectly addressed. It is also suggested that the 'From' address is also used with the intent to

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

identify the sender (it being the function of the 'reply-to' address to indicate where, by default, a reply will be sent). If it follows that the 'From' line of an email acts to designate the sender, then the act of signature is the irrevocable dispatch of the email. Additional technical evidence may be adduced to demonstrate a connection to the person who sent, or caused to be sent, a document in electronic form, taking into account all of the data associated with the document, including the metadata, client software and any other technical information that may not be obvious on the face of the document as presented on the screen to a recipient without further exploration of the technical attributes of the software. In this respect, it is difficult to see how the email address can be considered to have merely appeared or is incidental: it is a crucial element of the document.[1]

1 On the face of it, the email address, if correct, appears to contain all the information required to deliver it to the intended recipient. However, that is not always the case, as illustrated by Tim McCormack in 'Electronic delivery' (2018) 15 Digital Evidence and Electronic Signature Law Review 70, where he considers this precise problem in *Edgbaston Golf Club Ltd v Revenue and Customs (VAT – REPAYMENTS: Vat – repayments)* [2018] UKFTT 189 (TC), [2018] 4 WLUK 30, [2018] STI 834.

7.173 It is the action of clicking the 'send' icon, or causing an agent to click the 'send' icon, that is the act of authentication. This view accords with the comments offered in the Law Commission Report,[1] where it is suggested that the clicking of an icon probably constitutes the technological equivalent of signing with mark, and is therefore a signature. Further, the action of clicking the 'send' icon tends to be the irrevocable dispatch of the communication (although if the person is quick enough, they may, depending on the software, stop the software from sending the email), and can be similar to, or the equivalent of, the act of writing a manuscript signature or affixing a stamp to a document. In this respect, the information contained in the email address serves the same function as the use of headed notepaper in *Tourret v Cripps*. Cripps took a sheet of headed notepaper and wrote a promise on the paper. In *J Pereira Fernandes SA v Mehta*, Mehta either himself or through an agent, caused an email to be written (or the contents cut and pasted) that contained a promise. Instead of taking out a physical piece of notepaper and writing on it, he or his agent used a machine, namely a computer. The information contained in the email address served the same purpose as the name and address on the notepaper used by Cripps. Conceptually, there is no difference between the two: the cases are merely separated by time and the technology – that is, Mehta did not add any content by writing by hand. Prakash J gave her reasons for accepting the name in an email address based upon the same principle in *SM Integrated Transware Ltd v Schenker Singapore (Pte) Ltd*[2] at 92:

> There is no doubt that at the time he sent them out, he intended the recipients of the various messages to know that they had come from him. Despite that, he did not find it necessary to identify himself as the sender by appending his name at the end of any of the emails whether the messages were sent to his colleagues or to third parties like Mr Heng. I can only infer that his omission to type in his name was due to his knowledge that his name appeared at the head of every message next to his email address so clearly that there could be no doubt that he was intended to be identified as the sender of such message.

1 Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions Advice from the Law Commission* (2001), 3.37–3.38.
2 [2005] 2 SLR 651, [2005] SGHC 58.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.174 In analysing this case, Professor Ter Kah Lang indicated that the judge only addressed the identification function of the email address, not the intent to authenticate. Had the judge considered authentication, Professor Ter Kah Lang suggests that the conclusion might have been different.[1] Simon Blount also agrees with this analysis. However, he suggests that if Tan was saying that he did not need to sign his emails because he knew his name was already part of the email address, the decision may be correct, although in such case the author then intends to be bound by every word sent in the email.[2]

1 Ter Kah Leng, 'Have you signed your electronic contract?' (2011) 27 Computer Law & Security Review 75, 77.
2 Simon Blount, *Electronic Contracts* (2nd edn, LexisNexis Butterworths 2015), 35.

7.175 In *J Pereira Fernandes SA v Mehta*, Judge Pelling QC mentioned the Electronic Communications Act 2000, but no consideration was given to the provisions of s 7,[1] or whether s 7 applied to the facts of this case. Arguably, an email address is brought within the ambit of the Act as a form of electronic signature. First, the question is whether the email address can be considered a signature for the purposes of the Act, and the provisions of s 7(2)(a) have to be considered. As discussed above, an email will not arrive at its destination without a correct address, and if a person sending an email wishes the person receiving the email to reply, they must also use an accurate 'reply-to' email address, otherwise the recipient will not be able to respond. It is suggested above that there is a purpose for including a name or other form of description (such as the use of a title in lieu of a name) in the address of an email: to identify the sender. Also, technically, an email includes the various addresses in the email. Without an address, there would be no purpose in sending or receiving email correspondence. If the email address is not logically incorporated into the body of the text to be sent, the content will not be sent or received. To relate the email address to the provisions of s 7(2), it is necessary to consider the elements of an electronic signature:

> 'So much of anything in electronic form': This is such a wide-ranging provision that the address associated with an email must come with the term, just as the hidden metadata must also come within the term. Without the email address, the email could not be sent and received.
>
> 'Incorporation or logical association for the purpose of establishing authenticity or integrity': The thing in electronic form must be incorporated or logically associated with the communication or data for the purpose of being used to establish the authenticity or the integrity of the communication or data, or both. For the thing to be an electronic signature, it must be affixed to the data for a purpose: that is, to authenticate the communication or data or provide for the identity of the communication or data.

1 The judge stated, at [30], that it was his understanding that the Electronic Communications Act 2000 was enacted to give effect to Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 187/1, 17.7.2000). The aim of the Act was to implement the provisions of the now repealed Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, 12, as set out in Note 19 of the Explanatory Notes to the Act.

7.176 An email address clearly comes within the requirements of this provision: it is in electronic form, and the name in the email address is included for the purpose of establishing the authenticity of the content. If the name were a nickname or

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

pseudonym, rather than a proper name or part of a proper name, the same conclusion would apply, based on the previous decisions at common law. If it is accepted that the email address, or the name of the person in an email address, can be considered an electronic signature, it can be admitted into evidence under the provisions of s 7(1).[1]

1 Judge Pelling QC expressed the view, at [30], that typing a name into the main body of an email can constitute an electronic signature, which is correct.

7.177 Finally, the Law Commission considered the nature of the evidence required to demonstrate the intent to authenticate. An objective test was proposed:

> 3.29 Because signatures affect many areas of personal and commercial life, it is essential that the courts develop a straight-forward approach. We believe this should be by way of a purely objective test: namely, would the conduct of the signatory indicate an authenticating intention to a reasonable person? This approach is consistent with the authorities, flexible and would, over time, produce the greatest certainty.[1]

1 Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions Advice from the Law Commission*.

7.178 It is suggested that this test cannot be right, because an objective test would need to be based on an analysis of the surrounding circumstances, including the technology, and the average person using the technology probably varies widely in terms of their technical understanding and ability, partly because the technology changes so rapidly. It was suggested that a subjective test is more appropriate.[1] This is the view taken by Flemming DJP in the South African case of *Chisnall and Chisnall v Sturgeon and Sturgeon*,[2] where he held that the signing of a contract for the sale of an erf (a legal term for a plot of land in Namibia, South Africa) was achieved by a mark or marks with the function of making the document an act of the signer, and of signifying assent to the content of the document. He indicated, at 645F, that 'An enquiry concerning assent must, of course, not be into what the signatory subjectively planned but what his acts signify to the other party'. This is what the English authorities have also held up to this point. A subjective test will allow a judge to consider both the surrounding circumstances and what was in the mind of the sender at the moment they are deemed to sign. If the facts of *J Pereira Fernandes SA v Mehta* are considered in this light, the conclusion must be that the email in question was signed. The surrounding circumstances in this case, as in *SM Integrated Transware Ltd v Schenker Singapore (Pte) Ltd*, were as follows:

> (1) The email was from Mr Mehta.
>
> (2) Mr Mehta knew that his email address would appear in the email, which went to show that it came from him; it also enabled the recipient to respond; as a result, the email address was his unique mark.
>
> (3) There was a course of correspondence between the parties by email.
>
> (4) The email contained a promise made by Mr Mehta or under his authority.
>
> (5) Mr Mehta admitted the email was sent, which indicated that he adopted the content of the email.

1 The subjective test is proposed by Mr Pépin Aslett, counsel for J Pereira Fernandes SA, Nicholas Bohm and the author.
2 1993 (2) SA 642 (W).

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.179 In this case, Prakash J had a great deal of evidence to demonstrate that the name in the email address could be construed as an electronic signature.

7.180 In summary, it is suggested that the requirement for a signature is not dependent and should not be limited by technology, and this is borne out by the case law from the past.[1] Lawyers and judges have been required to consider how new technologies affect the underlying legal principles. The decisions reached in the past remain relevant: the conclusion was, and remains, that any form of mark, whatever the technology used, has the capacity to demonstrate intent, and this should be no different when considering electronic signatures. Taking this into account, the decision by Judge Pelling QC is open to question. In addition, the judge suggested, in reaching his decision, that to conclude otherwise would lead to 'widespread and wholly unintended legal and commercial effects'. Arguably, this decision has led to the opposite: there is now uncertainty, especially among lay people who cannot be expected to understand that this decision refers only to s 4 of the Statute of Frauds, and only to guarantees. This decision is incompatible with the previous decisions on identical facts, albeit in applying the legal principles to different technologies, and sends a signal out that implies that a person may no longer be held to their promise for the lack of typing their name into the body of an email.[2] Notwithstanding this observation, this decision is generally accepted as being correct, sometimes with no discussion,[3] and sometimes with some discussion but without covering much of the case law discussed above.[4] Professor Ter Kah Lang set out the issue: that there is a fundamental distinction between identifying the sender by means of the pre-printed letterhead, and the intent of the signatory to adopt the name as authenticating the document.[5] Miller J commented on this point in *Welsch v Gatchell*[6] at [75], although arguments could abound if one party specifies that a particular type of electronic signature is required:

> An electronic signature will not prove adequate unless the Court is satisfied that its insertion was intended to signify adoption of the electronic note or memorandum of which it forms part or with which it is otherwise associated. That suggests that it would be prudent for those who wish to rely on an electronic writing and signature to warn the party to be charged that the writing is a contract that will bind that party when he or she attaches an electronic signature to it, and to specify what form of electronic signature is required.

1 In *Mercury Tax Group Ltd, R (on the application of) v HM Commissioners of Revenue & Customs* [2008] EWHC 2721 (Admin), [2009] STC 743, [2008] 11 WLUK 303, [2009] Lloyd's Rep FC 135, [2009] BTC 3, [2008] STI 2670, [2009] CLY 3928 the signature pages of a trust deed, an option agreement and a sale/purchase agreement were signed some time before the final versions were complete, and were then attached, without the consent of those who signed the pages, to final versions that were different to the draft versions; see also Emma Walton, 'Guidance on the execution of documents at "virtual" signings following the *Mercury* case' (2009) 24 Butterworths Journal of International Banking and Financial Law 327.

2 Judges in both the High Court and Court of Appeal (Civil Division) took a different view where it appears there was no signature in the case of *Decouvreur v Jordan* [1987] 1 WLUK 115, Times, 25 May 1987, [1987] CLY 1842; an appeal was dismissed before a court comprising Fox and Nourse LJJ and Sir Denys Buckley, where judgment for the plaintiff had been given by Mr Justice Farquharson in the sum of £15,000 on a claim against the second defendant under a contract of guarantee. The report states that 'Any writing by which the guarantor of a debt could be identified in a memorandum of the guarantee and which showed an intention to adopt the guarantee sufficed as a signature for the purposes of the Statute of Frauds 1677'. See Clive Freedman and Jake Hardy, 'J Pereira Fernandes SA v Mehta: a 21st-century email meets a 17th century statute' (2007) 21 Computer Law & Security Report 77.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

3 Brazell, *Electronic Signatures and Identities Law and Regulation*, 2-017; The Hon Mrs Justice Geraldine Andrews and Richard Millett, *Law of Guarantees* (7th edn, Sweet & Maxwell 2015), 82; MacQueen and Garland, 'Signatures in Scots law'.
4 Leng, 'Have you signed your electronic contract?'; Blount, *Electronic Contracts*.
5 Leng, 'Have you signed your electronic contract?', 79.
6 [2007] NZHC 1898, [2009] 1 NZLR 241, (2007) 8 NZCPR 708, (2007) 5 NZ ConvC 194,549 (21 June 2007).

7.181 Whether the name typed into an email can satisfy the provisions of s 4 of the Statute of Frauds is open to debate. What is disappointing is the lack of consideration of the decisions by senior judges from the nineteenth century when faced with identical facts in slightly different formats. The common law is supposed to be based on precedent, yet pertinent decisions by senior judges have either been missed or ignored in this debate.

Legal fees arrangement

7.182 In Israel, Hagai Brenner J determined, in a claim for legal fees in the case of *Atias v Salfan Ltd*,[1] that there was no basis for the defendant's claim that a legal fees agreement between her and the plaintiff was not signed. The plaintiff sent an email to the defendant in which he summarized their joint understanding of the legal fees. The defendant confirmed that understanding in a reply message, and used an expression that literally translates as 'No problem'. A legal fees agreement is not required to be in writing (although this is recommended) and the email correspondence between the two parties was determined to be sufficient proof of the existence of the agreement. In the absence of any other information, such as whether the defendant also signed her name in the reply email, it may be inferred that Hagai Brenner J reached the decision based on the email address of the defendant.

1 Tel Aviv Peace Court Civil Case 24210/06 (5 July 2006, unpublished decision).

Civil Law Act

7.183 In Singapore, whether the name in an email address could be an electronic signature was raised in the case *SM Integrated Transware* of *Ltd v Schenker Singapore (Pte) Ltd*.[1] In this instance, Prakash J determined that it was possible for an email address to be a form of electronic signature for the purposes of s 6(d) of the Civil Law Act (Cap 43, 1994 Rev Ed). In this case, SM Integrated entered into negotiations to provide warehousing space and logistics services to Schenker. Schenker intended to enter a contract with a third party to handle dangerous goods, which in turn meant Schenker needed more storage facilities than it actually had. SM Integrated and Schenker prepared a draft agreement by way of meetings and the exchange of email correspondence, the content of which included reference to the transaction and the terms of the draft agreement. The agreement was never signed. Schenker subsequently failed to enter a contract with the third party, and because it no longer required the additional storage space, it declined to sign the draft agreement. SM Integrated initiated an action for damages suffered as a result of the alleged repudiation of the proposed lease, claiming that a combination of the draft agreement and the correspondence by email relating to the terms of the agreement demonstrated that an agreement had been formed. Schenker took the view that there was no contract because the negotiations failed to produce a final agreement, but even if a valid contract existed, it did not satisfy

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

the requirements of the Electronic Transactions Act 1998 (Cap 88 of 1999), in that it was neither in writing nor signed.

1 [2005] 2 SLR 651, [2005] SGHC 58; Ter Kah Leng, 'Concluding leases by email' (2005) 21 Computer Law & Security Report 423; Bryan Tan, 'SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd [(2005)] SGHC 58' (2005) 2 Digital Evidence and Electronic Signature Law Review 112; Daniel Seng, 'The Singapore Electronic Transactions Act and the Hong Kong Electronic Transactions Ordinance' (2008) 5 Digital Evidence and Electronic Signature Law Review 7.

7.184 The arguments put forward by Schenker were not accepted. In her reasons for judgment, Prakash J gave careful consideration to the issue of whether or not the correspondence by email that passed between the parties was capable of satisfying the Statute of Frauds requirements of s 6(d) of the Civil Law Act (Cap 43, 1994 Rev Ed).

7.185 Counsel for Schenker argued that the signature and writing requirements regarding this particular type of contract were not capable of being satisfied electronically because of the provisions of s 4(1)(d) of the Electronic Transactions Act 1998 (as it was then), which stated that the Act does not apply to 'any contract for the sale or other disposition of immovable property, or any interest in such property'. This argument was also rejected.

7.186 In reaching a decision on this matter, it was reasonable to consider the position at common law and by construing the provisions of s 6(d) Civil Law Act 1994, not by 'blindly relying on s4(1)(d) of the ETA'.[1] It was also held that the communications exchanged by email were in writing.[2] Apart from the legal basis of the decision that the emails were in writing, Prakash J, at [81], took a realistic and sound approach by making it clear that, despite the claim that the emails did not constitute writing, the facts did not correspond to such a contention.

1 [2005] 2 SLR 651, paragraph 76.
2 [2005] 2 SLR 651, paragraphs 77–85.

7.187 Arguments that email and other documents created in digital form do not constitute 'writing' are disingenuous. The law is often derided for not responding to the development of new technologies, yet the comments made by judges in the nineteenth century indicated they were perfectly willing and able to apply legal principles to new forms of technology. It is widely recognized that digital data is the mainstay of many businesses and governments across the world, and to suggest that evidence from such sources is not admissible because it is not a 'writing' is bordering on the preposterous.

7.188 Mr Tan did not append his name at the bottom of the email, so the only evidence of a signature comprised the content of the heading: 'From "Tan Tian Tye"<tian-tye.tan@schenker.com>.' The name in the email address was considered a signature, and in reaching this conclusion, Prakash J referred to the Massachusetts case of *Shattuck v Klotzbach*,[1] and the seventh circuit case of *Cloud Corporation v Hasbro, Inc.*[2] In her judgment, Prakash J provided a clear exposition of the underlying principles that were established in the English and American courts in the nineteenth century:

> 91. I am satisfied that the common law does not require handwritten signatures for the purpose of satisfying the signature requirements of s 6(d) of the CLA. A typewritten or printed form is sufficient. In my view, no real distinction can be drawn between a typewritten form and a signature that has been typed onto an email and forwarded with the email to the intended recipient of that message.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> 92. One minor difficulty in this case is that Mr Tan did not append his name at the bottom of any of his email messages. All his email messages, however, including the message dated 4 February 2003 and sent to Ms Yong, had, near the start thereof, a line reading '**From**: "Tan Tian Tye" <tian-tye.tan @schenker.com>'. Mr Tan confirmed in court that he had sent out those messages. There is no doubt that at the time he sent them out, he intended the recipients of the various messages to know that they had come from him. Despite that, he did not find it necessary to identify himself as the sender by appending his name at the end of any of the emails whether the messages were sent to his colleagues or to third parties like Mr Heng. I can only infer that his omission to type in his name was due to his knowledge that his name appeared at the head of every message next to his email address so clearly that there could be no doubt that he was intended to be identified as the sender of such message. Therefore, I hold that the signature requirement of s6(d) is satisfied by the inscription of Mr Tan's name next to his email address at the top of the email of 4 February 2003.
>
> 93. I recognize that one person's email facility can, in some cases, be accessed by a third party who can then send out messages which purport to be authentic messages from the owner of that email address. If that happened, the owner of the address would be entitled to dispute the authenticity of the messages purportedly sent by him. That is not the case here. Further, such dispute would be as to the person who initiated the message and would not be decided on the basis of whether the message bore a signature.

1 14 Mass. L. Rptr 360, 2001 WL 1839720 (Mass. Super.).
2 314 F.3d 289 (7th Cir. 2002).

7.189 In the same year, Lai Kew Chai J referred to the decision of Judith Prakash J in the bankruptcy proceedings of *Wee Soon Kim Anthony v Lim Chor Pee*.[1] Although the judge did not have to consider the email correspondence in this case, having determined that the exchange did not form a valid agreement because there was no meeting of the minds, nevertheless he commented, at [39], that he considered the exchange of email correspondence was likely to satisfy the written record and signature requirements of s 111 of the Legal Profession Act (Cap 161, 2001 Rev Ed).[2]

1 [2005] 4 SLR 367, [2005] SGHC 159.
2 Note also *Singh Chiranjeev v Joseph Mathew* [2008] SGHC 222, [2009] 2 SLR 73.

7.190 It can be safely concluded that whether an email address is capable of constituting a form of electronic signature will depend on the facts of each case.[1]

1 For other examples regarding a name in an email address: Greece – 32/2011, translation and commentary by Michael G. Rachavelias (2014) 11 Digital Evidence and Electronic Signature Law Review 174 (assignment; validity; status of electronic document; email address; evidential weight); Payment Order 5845/2013, translation by Michael G. Rachavelias (2014) 11 Digital Evidence and Electronic Signature Law Review 177 (debt; electronic document; email; email address; burden of proof; forgery); Court Decision No. 1963/2004 (2005) 2 Digital Evidence and Electronic Signature Law Review 107 (notification procedure); Italy, Tribunale Mondovì, 7 giugno 2004, n. 375 (decr.), Giur. It. 2005, 1026 (2007) 4 Digital Evidence and Electronic Signature Law Review 86 (email acknowledging debt).

A manuscript signature that has been scanned

7.191 A variation of the biodynamic version of a manuscript signature is where a manuscript signature is scanned[1] from the paper carrier and transformed into digital

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

form, which makes it very easy to use by the recipient for the purposes of forgery. The files containing the representation of the signature can then be attached to a document. This version of a signature is used widely in commerce, especially when marketing materials are sent through the postal system and addressed to hundreds of thousands, if not millions, of addresses. It could be argued that when sending a document by facsimile transmission the recipient of the document has in their possession this version of the manuscript signature: the entire document is scanned and transmitted, together with the content. Arguably, this is the form of signature that was discussed in the case of *Re a debtor (No 2021 of 1995), Ex p, Inland Revenue Commissioners v The debtor; Re a debtor (No 2022 of 1995), Ex, Inland Revenue Commissioners v The debtor*[2] where a completed form of proxy was sent by facsimile transmission. Although the report does not clearly state the proxy form, as transmitted, contained the manuscript signature of the relevant official from the Commissioners of Inland Revenue, it can be inferred that a manuscript signature had been appended to the original form of proxy that was sent by facsimile transmission. Laddie J offered an opinion in relation to this point at 351f–g:

> For example, it is possible to instruct a printing machine to print a signature by electronic signal sent over a network or via a modem. Similarly, it is now possible with standard personal computer equipment and readily available popular word processing software to compose, say, a letter on a computer screen, incorporate within it the author's signature which has been scanned into the computer and is stored in electronic form, and to send the whole document including the signature by fax modem to a remote fax. The fax received at the remote station may well be the only hard copy of the document. It seems to me that such a document has been 'signed' by the author.

1 By way of example, scanned signatures were relied upon in the following cases in England and Wales (this list is not exhaustive): *National Bank Trust v Yurov* [2020] EWHC 100 (Comm), [2020] 1 WLUK 148; *TFS Stores Ltd v The Designer Retail Outlet Centres (Mansfield) General Partner Ltd* [2019] EWHC 1363 (Ch), [2019] Bus LR 1970, [2019] 6 WLUK 10, [2020] 1 P & CR 6, [2019] L & TR 26, [2019] CLY 1697; *Rotam Agrochemical Company Ltd v GAT Microencapsulation GMBH* [2018] EWHC 2765 (Comm), [2018] 10 WLUK 406; *FSHC Group Holdings Ltd v Barclays Bank Plc* [2018] EWHC 1558 (Ch), [2018] 6 WLUK 448; *Chartwell Estate Agents Ltd v Fergies Properties SA* [2014] EWHC 1567 (QB), [2014] 5 WLUK 471.

2 [1996] 2 All ER 345, [1995] 11 WLUK 290, [1996] BCC 189, [1996] 1 BCLC 538, [1996] BPIR 398, [1996] CLY 3469.

7.192 This observation must be correct. Providing the sending party intended the recipient to accept such a signature as a method of authentication and to act upon the content of the document transmitted, the method used to transmit the signature remains merely a method by which the document or message is communicated. The means of communication used should not affect the legal consequences that follow the delivery and subsequent receipt of the document.[1]

1 For a discussion of cases involving scanned images of manuscript signatures in Belgium, see Johan Vandendriessche, 'An overview of some recent case law in Belgium in relation to electronic signature' (2010) 7 Digital Evidence and Electronic Signature Law Review 90.

Mortgage redemption

7.193 In 2006 a registration judge in Denmark refused to cancel a mortgage because the signatures on the documentation were not manuscript signatures. The Danish

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Western High Court upheld this decision in case U.2006.1341V. The facts were that a mortgage bank N delivered a mortgage for the purpose of cancellation. The scanned signatures of A and B were affixed to the cancellation endorsement. By a notice circulated to all judicial districts, N had authorized A and B to jointly endorse the mortgage by means of scanned manuscript signatures. The endorsements were added or attached to the original mortgage. The registration judge refused to cancel the mortgage because the signatures were not added by means of a manuscript signature in accordance with s 9(1) of the Danish Registration of Property Act. The Danish Western High Court upheld this decision, and took the view that under s 261(2) of the Danish Administration of Justice Act, the endorsement must be signed, and in accordance with established case law, pleadings must be available in their original form, and photocopies or facsimiles are therefore not sufficient. In addition, the registry took the view that, on grounds of due process, manuscript signatures are still required on documents to be registered (or cancelled), and that any change of this state of the law should, if necessary, be clarified by the legislature in the same way as the provisions on digital signatures.[1]

1 For a case report, see (2007) 4 Digital Evidence and Electronic Signature Law Review 99.

Writing

7.194 In a case before the German Federal Supreme Court (Bundesgerichtshof), file number XI ZB 40/06, NJW 2006, 3784 regarding §130 Zivilprozessordnung (ZPO) (the German code of civil procedure), it was held that a scanned manuscript signature is not sufficient to be qualified as 'in writing' under §130(6) ZPO if the signature is printed on a document and then sent by facsimile transmission. This ruling appears to prevent the admission into evidence of a document twice removed from the source. First, the signature is scanned and then printed on the document, then the document is sent on by means of facsimile transmission. As an item of evidence, such a document might be highly suspect in the absence of a clear acknowledgment by the person whose signature it is that they were entirely responsible for the entire process or they authorized another person to produce the document and transmit it, and they adopted the content of the document as their own.

Employment

7.195 In France, the case of Cour de Cassation, soc., 17 mai 2006, 04-46706[1] also considered the legal effect of a scanned signature. In this instance, an employee of the Association of La Réunion Marine Park was dismissed on 27 January 2002. A claim for unfair dismissal was issued. The only relevant issue for present purposes was that the dismissal letter had not been signed, but took the form of a letter bearing a signature that had been scanned. On 25 May 2004 the Court of Appeal of Saint-Denis de la Réunion held that a scanned manuscript signature did not constitute an electronic signature, as defined by article 1316–4 of the French Civil Code, but nevertheless considered that the dismissal letter had been validly signed. Upon appeal to the Cour de Cassation, the supreme French civil court, the employee argued that the Court of Appeal should have decided that the dismissal letter was not admissible, as the Court of Appeal had found the signature had been rendered into digital form earlier. On this point, the Cour de Cassation held that the fact that the signature had been put into digital form on the dismissal letter might affect the formal process of the dismissal procedure, but did not

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

in itself deprive the dismissal of substantive justifiable grounds. The Cour de Cassation appeared to leave open the question of whether or not the electronic signature did affect the dismissal procedure. In this instance, the Cour de Cassation held that there were justifiable substantive grounds for the dismissal.

1 The decision in French is available at http://www.legifrance.gouv.fr/.

Biodynamic version of a manuscript signature

7.196 There are products available that permit a person to produce a biodynamic version of their manuscript signature.[1] For instance, some delivery companies use hand-held devices that require the recipient of an item of post or parcel to sign on a screen acknowledging receipt of the mail, and some banks use similar methods to provide a signature when using a debit or credit card.

1 Such a system was relied upon in *Sell Your Car With Us Ltd v Sareen* [2019] EWHC 2332 (Ch), [2019] 9 WLUK 397, [2019] BCC 1211, [2020] 1 CL 112; see also *Fitzpatrick v AIG Europe* (unreported) 1 July 2015, Jenkinson DJ, where the judge considered an electronic signature made with a proprietary product on a witness statement to be valid, for which see Gordon Exall, 'Electronic signature of witness statements: is it valid? A first instance decision', https://www.civillitigationbrief.com/2015/07/02/electronic-signature-of-witness-statements-is-it-valid-a-first-instance-decision/.

7.197 Another method of obtaining a digital version of a manuscript signature is where a person can write their manuscript signature by using a special pen and pad. The signature is reproduced on the computer screen, and a series of measurements record the behaviour of the person as they perform the action. The measurements include the speed, rhythm, pattern, habit, stroke sequence and dynamics that are unique to the individual at the time they write their signature.[1] The subsequent electronic file can then be attached to any document in electronic form to provide a measurement of a signature represented in graphic form on the screen. While it appears that this concept might be usefully applied in the electronic environment, the drawbacks are as significant as for any other form of generating electronic signatures, including linking the evidence in a coherent fashion to prove a person signed a particular document,[2] and problems relating to the protection of personal data.[3]

1 Such a device seems to be used by the Queensland Police Services, for which see *Bismark v Queensland Police Service District Court of Queensland* [2014] QDC 152 2014, WL 8104519 in which such a device is used by the appellant.

2 The nature of the evidence was discussed by Chin DJ in *Labajo v Best Buy Stores, L.P.*, 478 F.Supp.2d 523 (S.D.N.Y. 2007) at 530, although this report was in respect of a motion for judgment on the pleadings and before discovery, so the defendants would have had the opportunity of obtaining more coherent evidence for the trial; Fangjun Luan, Shiliang Ma, Kaidong Cheng and Xianfeng Dong, 'On-line handwritten signature verification algorithm based on time sequence' (2005) 1 International Journal of Information and Systems Sciences 229; Ricardo P. Gonçalves, Alexandre B. Augusto and Manuel E. Correia, 'Time/space based biometric handwritten signature verification', *10th Iberian Conference on Information Systems and Technologies (CISTI), 2015* (IEEE 2015), 743–748.

3 Anderson, *Security Engineering*, 15.9 for an indication about what can go wrong with biometric systems, and Jan Grijpink, 'Biometrics and privacy' (2001) 17 Computer Law and Security Report 154.

Electoral register

7.198 In Australia, the Electoral Commissioner rejected the biodynamic version of a manuscript signature (biodynamic signature) in the case of *Getup Ltd v Electoral*

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Commissioner[1] prior to the Australian election in August 2010. Ms Trevitt used her biodynamic signature to enrol as a voter over the Internet before the election took place. Lawyers for the Commissioner wrote to Ms Trevitt, indicating 'that the electronic signature on the claim form was not sufficient'.[2] Her attempt to register her vote was rejected. The main point at issue was whether the form of signature used was appropriate, in accordance with the provisions of s 10(1)(b) of the Electronic Transactions Act 1999 (Cth). Perram J considered s 10(1)(a) and (b), and whether this Act applied to the Commonwealth Electoral Act 1918 (Cth).

1 [2010] FCA 869 (13 August 2010).
2 [2010] FCA 869 (13 August 2010) at [8].

7.199 Ms Trevitt affixed her electronic signature to the form with a biodynamic signature. It was argued by counsel for the Commissioner that it was for the Commissioner to form an opinion about the reliability of the method in accordance with the purpose. The judge did not agree with this argument. He set out his reasoning at 14–15:

> The provision does not mention anyone forming an opinion. In particular, because s 10(1)(b) is pitched at a very high level of generality it understandably eschews identifying any of the parties to the communication at all. Even assuming the provision should be read as requiring someone to hold an opinion it is silent as to whether it is to be held by the sender or the recipient or both. Further, as Mr Kirk, who appeared with Ms Rao for the applicants, pointed out, the breadth of the requirement that the issue be considered in light of all of the relevant circumstances bespoke the possibility that not all of the circumstances might be known to the participants to the communication. Such a view of the provision counted against it being read as requiring the formation of an opinion by one or other of the persons involved in its application.
>
> 15. I do not see a way around those concerns. To accede to the notion that s 10(1)(b) required the Commissioner to form an opinion would involve, so it seems to me, an intolerably strained construction of its plain words. Further, it would be a construction which necessarily identified the recipient as the person whose opinion mattered. That reading of s 10(1)(b) might have very serious consequences in a range of cases yet to come and about which nothing can be known. In those circumstances, I do not read s 10(1)(b) in a manner for which the Commissioner contends. This has the consequence that the provision sets a standard which, in this instance, is to be ascertained and applied by the Court.

7.200 Perram J then considered the nature of the evidence, the possibility of forgery and the fact that the Commissioner accepted other forms of signature (whether they were sent by facsimile transmission and scanned versions of manuscript signatures), and concluded, at 17 that:

> In that circumstance, I cannot accept the slightly pixelated nature of Ms Trevitt's signature rendered it unreliable for the Commissioner's purposes, not at least while he continues to accept faxed or emailed claim forms.

7.201 This particular point, the abstract reliability test, refers to article 9(3) of the United Nations Convention on the Use of Electronic Communications in International Contracts. If not understood, the abstract reliability test could increase the risks of invalidity after the event, where the form of signature had never posed problems of authentication previously.[1]

1 The provision of the abstract reliability test merits further observations, for which see John D. Gregory, 'Must e-signatures be reliable?' (2013) 10 Digital Evidence and Electronic Signature Law Review 67.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Contract formation

7.202 At issue in the US case of *American Family Life Assurance Company of Columbus v Biles*[1] was whether the signature of the late David Biles was a forgery. The method used by Mr Biles to apply his signature to a life insurance policy was by way of a proprietary biodynamic version of his manuscript signature, using a pad and computer. Of interest was the approach taken by the two document examiners in the case. Robert G. Foley gave evidence for the plaintiff,[2] and William J. Flynn gave evidence for the defendant.[3] Mr Foley compared the photocopies presented to him by the plaintiff of the images of two signatures affixed to the document. Mr Flynn, in contrast, examined the data files used to create the images representing the electronic signature. One of the reasons for the hearings was an application to strike out the affidavit of Robert G. Foley on the basis that his examination was not appropriate, given that he ought to have examined the data files. Lee DJ ordered a *Daubert*[4] hearing to determine whether to agree to exclude Mr Foley's evidence.[5] At the subsequent hearing, the defendants sought to exclude the evidence of Mr Flynn. After hearing the evidence, the judge concluded that the challenge to Mr Foley's reliability was well taken, because his opinion was not based on the examination of the best evidence available.[6] The implication is that when electronic signatures of this nature are challenged, it is important to ensure the adjudicator is aware of the need for the examination of the digital data, and that a comparison of the images produced by the digital data alone is not appropriate.[7]

1 2011 WL 4014463 (S.D.Miss.) and 2011 WL 5325622 (S.D.Miss.).

2 *American Family Life Assurance Company of Columbus v Biles*, 2011 WL 5835356 (S.D.Miss.) (affidavit of Robert G. Foley); *American Family Life Assurance Company of Columbus v Biles*, 2011 WL 7909386 (S.D.Miss.) (supplemental affidavit of Robert G. Foley).

3 *American Family Life Assurance Company of Columbus v Biles*, 2011 WL 5835357 (S.D.Miss.) (affidavit of William J. Flynn).

4 *Daubert v Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).

5 *American Family Life Assurance Company of Columbus v Biles*, 2011 WL 4014463 2011 (S.D.Miss.).

6 *American Family Life Assurance Company of Columbus v Biles*, 2011 WL 5325622 (S.D.Miss.); *American Family Life Assurance Company of Columbus v Glenda C. Biles, Individually, Natural Mother of David Biles, Deceased, and Administratrix of Estate of David Biles, Deceased*, 714 F.3d 887 (5th Cir. 2013) (appeal on the enforcement of the arbitration agreement).

7 Heidi H. Harralson, 'Forensic document examination of electronically captured signatures' (2012) 9 Digital Evidence and Electronic Signature Law Review 67; for the failure to adduce relevant evidence of a signature, see a case from the Court of Appeals of North Carolina, *Meadlock v American Family Life Assurance Company of Columbus*, 221 N.C.App. 669, 729 S.E.2d 127 (Table), 2012 WL 2891079.

Digital signatures

Technical overview of digital signatures

7.203 Cryptography is the method of hiding the contents of a message, as used from ancient times to the present. Encryption (or enciphering) is the process by which a plaintext (or cleartext) message is disguised sufficiently to hide the substance of the content. As well as ordinary text, a plaintext message can be a stream of binary digits, a text file, a bitmap, a recording of sound in digital format, audio images of a video or film and any other information formed into digital bits. When a message has been encrypted, it is known as ciphertext or a cryptogram. The opposite procedure, that of turning the ciphertext back into plaintext, is called decryption (or deciphering).[1] In essence, contemporary cryptographic systems change one set of symbols that have

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

meaning (binary data) into a second set of symbols that have no meaning, by means of a mathematical process. Cryptography is usually required to undertake a number of functions, the most important of which is authenticity rather than secrecy. These functions are discussed below.

> (1) Authenticity: When sending or receiving information or placing an order, both parties need to have assurance of the origin of the message. The aim is to corroborate the identity of the software that sent the data. The identity of a person cannot be corroborated, because a person is not part of the communications process – the process only involves communications between software.
>
> (2) Integrity: It is helpful to demonstrate the integrity of the message, because it is important to know if the content of the message has been tampered with.
>
> (3) Honesty: To provide an assurance, to the extent that is technically possible, that demonstrates that the software emanates from a known source, such that the purported sender has been honest about the actions that have been caused to be undertaken. The purpose is an attempt to bind human users to specific actions in such a way that if they deny taking the action, they either demonstrate an intention to deceive, or they have been negligent in failing to secure the use of their private key adequately. This is called 'non-repudiation' in the security industry. There are different types of non-repudiation: non-repudiation of origin, which prevents the entity that sent the message or document from denying that they sent it, and non-repudiation of receipt, where an entity cannot deny they have received a message or document. Other types of non-repudiation include non-repudiation of creation, non-repudiation of delivery and non-repudiation of approval.[2]
>
> (4) Confidentiality: Another purpose is to provide for the confidentiality of a document. In the digital environment, cryptography is used as a substitute for a manuscript signature, and is often described as a digital signature. To understand how a document can be signed with a digital signature, it is necessary to be aware of how cryptography works, for which see the discussion below.

1 Encipher and decipher are terms used in the ISO 7498-2 standard.
2 Adams and Lloyd, *Understanding PKI Concepts*, 51.

Algorithms and keys

7.204 The plaintext of a message is encrypted and decrypted by the use of a cryptographic algorithm (also called a cipher). There tend to be two related functions, one for encryption and another for decryption. In most instances, the secrecy of the algorithm will not matter, because modern cryptography uses a key. However, it is possible to have what is called a restricted algorithm, because the security of the algorithm is based on ensuring the way it works is kept a secret. There are drawbacks to the use of restricted algorithms. If a user leaves the group that shares the algorithm, or should the secret be revealed for any reason, then the algorithm must be changed. Further, there is no quality control or standardization, which means these algorithms can be easy to break. By using a key, a strong algorithm does not need to be secret and can be used by millions of users. As a result, there is no need to constantly develop new algorithms. A key can comprise a number of values. This range of values is called a keyspace. A key can be used to encrypt and decrypt a message, or there can be two separate keys, one to encrypt a message and another for decrypting the message. To complete the picture, a cryptosystem comprises an algorithm, all possible messages, all possible cryptograms and all possible keys.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Control of the key

7.205 To decrypt the ciphertext, the recipient needs to know both the decryption algorithm and the decryption key. The way a key is controlled, managed and distributed is crucial. This is why the principle laid down by Auguste Kerckhoffs von Niuewenhof remains a fundamental rule of cryptanalysis: the security of a cryptosystem must depend on keeping the key secret.[1] This issue is discussed more fully when considering the weaknesses relating to cryptosystems.

1 Auguste Kerckhoffs, 'La Cryptographie militaire' (1983) 9 Journal des Sciences Militaires 5, although this principle applied to a time when all systems were symmetric.

Disguising the message

7.206 There are two types of mathematical families that permit a message to be disguised: symmetric cryptographic systems and asymmetric cryptographic systems.

Conventional or symmetric cryptographic systems

7.207 As the name infers, the encryption key can be computed from the decryption key, and the decryption key can be computed from the encryption key. In practice, these two keys are often identical when used in symmetric systems. The symmetric system is also referred to as secret-key algorithms, single-key algorithms, one-key algorithms or shared key ciphers. Two people can use the same system to send and receive encrypted messages to each other and both the sender and the receiver must agree on the key before they can communicate. This system can have very long keys, which means a message can be very secure. The effectiveness of this system depends on the key, and is suitable for closed user groups where there is a strong element of mutual trust between the users, such as banks, the military and intelligence agencies. However, a disadvantage is that the key must be kept secure and secret. Two people must have the key to communicate. If encrypted messages are to pass between large numbers of people, a large number of keys will have to be distributed. The security of the system depends on those people with access to the keys ensuring they are kept secure and secret. Also, from the point of view of managing the keys, it is important for pairs of users to have different keys to reduce the risks of compromise when large numbers of people share a key.

7.208 Some symmetric algorithms work on the plaintext, one digit at a time. These are called stream ciphers. Others work in groups of digits on the plaintext. The groups of digits are called blocks, and the algorithms are called block algorithms or block ciphers. How an algorithm and the cipher work is important, because of their strengths and weaknesses. If an algorithm or cipher is easy to attack, then an application should not use it, and if losses occur because of the failure of either, then a successful legal action may be possible because it could be argued that the system was designed and possibly implemented negligently.

7.209 Sending a message that has been encrypted provides for the security of the content only. It does not attribute the message to the source from which the message was sent. It is possible for an interceptor to intercept the message and send a substitute message in place of the original message. If a forger sends the message, the

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

recipient will not be aware that the sender of the message has used the key improperly. Authentication seeks to corroborate the integrity of the message and authenticity of the sender. There are two types of authentication.

> (1) One-way authentication is where one party is authenticated to another party, such as a person using an ATM when they wish to withdraw cash or make a deposit. The user identifies themselves by using their PIN, and the card is authenticated cryptographically.
>
> (2) Two-way authentication, where both parties to a message seek to verify the attribution of data that purports to identify each other or the message or both, such as virtual private networks.

7.210 The process of authentication also uses a secret key. This is called the message authentication code or data authentication code. This mechanism can provide authentication without the need for secrecy. In symmetric cryptographic systems, the aim is for the originator and the legitimate recipient to be the only two entities that can create or check the message authentication code. Here is an example of how the message authentication code can work:[1]

> Alice sends a message in plaintext to Bob. The software on the computer that Alice uses encrypts the message by using a block algorithm or cipher. All of the ciphertext blocks are then discarded with the exception of the last block. The last block is the message authentication code. (Note: if Alice wants to provide for both the integrity and the privacy of the message, the message can also be encrypted again.)
>
> Bob receives the message. The software on his computer computes what the message authentication code should have been. If Eve intercepted and altered the message, Bob will realise this, because the incorrect plaintext is re-encrypted, producing an incorrect message authentication code. If the plaintext has been altered, the ciphertext blocks will be different, especially the last ciphertext block. If the plaintext has not been altered, the re-encrypted plaintext will not have changed, and Bob can be sure that Alice has sent the plaintext message.

1 Alice, Bob, Carol, Dave and interloper Eve are used widely in cryptology. See 'The Alice and Bob after dinner speech' given at the Zürich Seminar, April 1984 by John Gordon by invitation of Professor John Massey, http://web.mit.edu/jemorris/humor/alice-and-bob.

7.211 However, this does not prevent Eve from listening in to Alice when she sends the message to Bob. Eve can then record every message, together with the message authentication code. Alternatively, she can delete the message sent by Alice, repeat old messages or change the order in which the messages are sent. Thus the message authentication code needs to include a scheme by which each message is numbered sequentially.

Asymmetric cryptographic systems (Public key)

7.212 Using a symmetric cryptographic system with large numbers of users is difficult. Keys cannot be distributed over the open communications network, so they have to be distributed in other ways. When a member leaves the group, all the other members have to redistribute new keys. Thus, assuming a separate key is used for each pair in a group, and if there are 10 people as members of the group, 45 different keys

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

will be required. The development of the asymmetric cryptographic system, or public key,[1] helps to resolve this problem. With this system, keys only have one purpose: one key to encrypt and one key to decrypt. Given a large enough key, the decryption key cannot be calculated from the encryption key within a useful length of time (perhaps several centuries). The algorithms used in the system are commonly called 'public key' because the encryption key is usually made public. Anybody can use the encryption key to encrypt a plaintext message, but only the person with the decryption key that corresponds to the encryption key can decrypt the message. The encryption key is called the public key or public encryption key, and the decryption key is called the private key, secret key or private decryption key. The system can work in two ways, as indicated below.

1 The concept of public key cryptography was invented twice during the twentieth century. First, by James H. Ellis, Clifford Cocks and Malcolm J. Williamson at British Intelligence GCHQ, whose work remained classified until December 1997. Second, two researchers at Stanford University, Whitfield Diffie and Martin Hellman, proposed the concept in 1976. Development of the principles can also be attributed to Ralph C. Merkle, Ronald L. Rivest, Adi Shamir and Leonard A. Adleman.

7.213 An individual creates and controls their own public key The user can generate a pair of keys using what is called a trapdoor one-way function, containing the mathematical equivalent of a secret trapdoor. For the purposes of understanding the concept, this algorithm is easy to compute in one direction and difficult to compute in the opposite direction, unless you know the secret.[1] Sending a message using public key cryptography can be described as follows:

> Alice and Bob decide to exchange messages that are encrypted.
>
> Alice generates her own public and private keys using the software on her computer. Although she keeps the private key secret, she gives Bob her public key.
>
> Bob writes his message and encrypts it using Alice's public key. He sends it to Alice.
>
> Alice decrypts Bob's message using her private key.

1 It has yet to be proven that a mathematical function can have a one-way function, for which see Fred Piper, Simon Blake-Wilson and John Mitchell, *Digital Signatures: Security & Controls* (Information Systems Audit and Control Foundation 1999), 16.

7.214 This method of encrypting and decrypting messages means that private keys do not have to be distributed. The private key should always be under the direct control of the owner. If the private key was distributed, there is no way of asserting a signature is yours, because you could always claim the other person who received your key executed the signature.

7.215 In addition, it is possible for Alice to place her public key in a public database. The protocol then looks like this:

> Bob goes to the database and obtains Alice's public key.
>
> Bob writes Alice a message and uses her public key to encrypt the message. Bob then sends the message to her.
>
> Alice decrypts the message using her private key upon receipt.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.216 There can be problems in relation to the methods by which an individual creates and controls their own keys, as in *Maughan v Wilmot*,[1] where the husband created his own digital signature to attach to emails.

1 [2016] EWHC 29 (Fam), [2016] 1 WLR 2200, [2016] 1 WLUK 90, [2016] 2 FLR 1349, [2016] Fam Law 307, [2016] CLY 316.

7.217 Authenticating a signature using public key cryptography The underlying rationale of public key cryptography is that a message can be attributed to a particular entity. First, Alice can use a key generation algorithm to generate a key pair: a private signing key and the public signature verification key, or she can use her existing key pair. She then publishes her public key on a database. Thereafter, the example continues:

> Alice writes a message and wants to send it to Bob with her digital signature. The software on her computer computes a digital signature from her private key and the content of the message.
>
> Alice sends her message and the digital signature to Bob. The signature may be, but does not need to be, separate from the message.[1] The signature operates in the same way as a message authentication code.
>
> Upon receipt of the message, Bob uses Alice's public key to verify that the corresponding private key signed the message.

1 This can be important, for which see Nicholas Bohm, 'Watch what you sign!' (2006) 3 Digital Evidence and Electronic Signature Law Review, 45.

7.218 However, given this scenario, it is generally noted in the technical literature that Bob cannot be sure that the public key in the database is that of Alice. This means this mechanism does not resolve the issue of identifying the sender of the message. A person could generate their own public and private keys, post the public key on a database and claim it belongs to Alice. Bob might think he is sending messages to Alice, but in fact his message might be posted to an interceptor. In addition, the interceptor could use their own private key to send messages to Bob, which he would assume came from Alice. There is a further problem with this method of adding a signature to a message, which in turn is inherent in any system that uses cryptography in the electronic environment to create a signature. The signature is not computed by Alice, but by the software on her computer. Thus there is no direct evidence to show Alice appended the signature to the message. This is, naturally, an identical problem with all forms of electronic signature and communication over networked communications – for instance, the same point can be made about the origin of an email. The recipient cannot be certain that an email comes from the purported source, yet the vast majority of emails that are sent and received are trusted. This is because the correspondents either know each other in the physical world, or even if they have not met, then they become familiar with each other in the virtual world by way of an exchange of correspondence and other signs, such as looking at websites and asking others who are trusted to indicate whether the person they have yet to meet is indeed the person they claim to be.

Public key infrastructure

7.219 The concept of the public key infrastructure (PKI) tries to resolve this problem by linking a public key to a named individual or legal entity.[1] The notion behind a public

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

key infrastructure is to have organizations called trusted intermediaries, trusted third parties, trust service providers or certification authorities that act to certify the connection between a person and their public key. In theory, the trusted third party guarantees the authenticity of the public key by issuing an individual identity certificate (usually abbreviated to 'certificate'), which binds a name string to a public key. This in turn seeks to create a link between the provision of a key and the identity of the natural person or legal entity to which the key has been issued. It should be emphasized that, when using a public key infrastructure, users should aim to continue to generate their own key pairs. Where a third party generates the key pair on behalf of a user, the degree of security exercised over the key pair is reduced.

1 For the flaws in PKI, see Carl Ellison, 'Improvements on conventional PKI wisdom', *Proceedings of the 1st Annual PKI Research Workshop* (NIST 2002), https://users.ece.cmu.edu/~adrian/731-sp04/readings/ellison-PKI-wisdom.pdf.

7.220 The certification authority issues an individual identity certificate, which includes the following characteristics: data identifying the certification authority, data identifying the subscriber that includes the subscriber's public key, and that it is signed with the Certification Authority's private key. The individual identity certificate may also contain other information, such as the level of inquiry carried out before issuing the certificate.

7.221 To acquire such a certificate, Alice will provide the certification authority with a copy of her public key and proof of her identity. The degree of proof of identity will differ, depending on the level of liability Alice wants to cover. When Alice sends a message to Bob, she also sends him a copy of her certificate. Alternatively, when she publishes her verification key, she publishes the certificate. The software on Bob's computer will decrypt the message according to the key he has been given. It will then be for Bob in most circumstances to undertake his own due diligence, perhaps by checking the certificate revocation list to ensure the public key has not been revoked or has expired, or sending an email to Alice (or contacting her by telephone) to confirm that she sent the communication. If Bob does not act to verify the information contained in the certificate, but contacts Alice directly, his due diligence will not involve the organization that issues the certificate.

Difficulties with public key infrastructure

7.222 The rationale behind the public key infrastructure is this: when a certification authority issues a certificate, it bases the issuance of the certificate on its Certificate Practice Statement and terms of trade. A contractual relationship is formed between the certification authority and the customer who buys the certificate. While the certificate purports to verify the identity of an individual person or legal entity, it is the merchant or person receiving the certificate who relies on the content of the certificate. The logic is as follows:[1]

> (1) The individual or entity provides the certification authority with sufficient evidence acceptable to the certification authority or registration authority to demonstrate that they are who they say they are. Depending on the level of the certificate obtained, this information could be the name, address and the number of a driving licence. For certificates that will support high value transactions, the

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

person or entity seeking a certificate may be required to provide more robust evidence, including physically appearing before a notary public.

(2) The certification authority provides the user with a certificate.

(3) The individual or entity is then given a keyholder's name.

(4) The keyholder is the person or entity that obtained the certificate.

(5) This is all the recipient needs to know.

1 Carl Ellison and Bruce Schneier, 'Ten risks of PKI: what you're not being told about public key infrastructure' (2000) 16 Computer Security Journal 1; for two responses to this article, see Ben Laurie, 'Seven and a half non-risks of PKI: what you shouldn't be told about public key infrastructure', https://groups.google.com/forum/#!topic/jyu.ohjelmointi.coderpunks/PtWHnFue9Zk and Aram Pérez, 'Response to "Ten risks of PKI" ', https://sites.google.com/site/aramperez/home/10-risks-of-pki; 'PKI Assessment Guidelines', C.4.2 'Attribution presumptions in digital signature statutes'.

7.223 There are a number of flaws with this logic. For instance, John Smith of York may wish to enter a contract with a company who is not aware of his identity. The company cannot distinguish, when it looks at the certificate, how many John Smiths live in York and whether this particular John Smith is the person identified with the certificate. Unless the certificate provides the company with a unique identifier for this particular John Smith (which they may or may not provide), and the company wishes to confirm John Smith's identity, it must consider other ways of doing so. The certification authority generally does not share a secret with the person to whom it issues a certificate, although there must be a method by which the certification authority can verify the identity of the person to whom it issues a certificate. Some certification authorities use the information collected by a credit bureau to verify the identity of the applicant. This means the identification verification process can be based on the accuracy of the data collected by the credit bureau – bearing in mind the focus of a credit bureau is on creditworthiness – and their effectiveness in keeping the information up to date and secret. Another issue is whether the recipient of the electronic signature trusts the originator's certification authority. If a certification authority were to undertake to positively identify a subscribing party, the information that might be needed to satisfy the recipient may be so extensive that few individuals or legal entities would consider subscribing for such a certificate.[1] In conclusion, a certification authority provides a very narrow promise when issuing a certifying certificate. It does not appear that certification authorities seek first to establish the identity of a person and then go on to verify that identity. It is important to understand that verification is not the same as identification.[2]

1 For a useful discussion, see Carl Ellison, 'Improvements on conventional PKI wisdom', *Proceedings of the 1st Annual PKI Research Workshop* (NIST 2002), 165–75, https://users.ece.cmu.edu/~adrian/731-sp04/readings/ellison-PKI-wisdom.pdf; Nicholas Bohm and Stephen Mason, 'Identity and its verification' (2010) 26 Computer Law & Security Review 43.

2 Jan Grijpink and Corien Prins, 'Digital anonymity on the internet' (2001) 17 Computer Law and Security Report 379, 381(a).

7.224 The purported advantage to the relying party of using the 'standard model' public key infrastructure digital signature is not that the signature provides greater security, but arises from persuading the subscribing party that because it is apparently more secure, the user takes responsibility for every use of the private key, whoever does so. It must be emphasized, however, that the greater security of the mechanism does not, in fact, offer the subscribing party any protection against attacks, such as the theft of the key or the failure of software such that the software signs something other than what is presented on the screen. The industry implies that the system has

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

a 'non-repudiation' property, and it is this property that justifies the imposition of a non-repudiation term on the subscribing party. This cannot be right, because if the system genuinely possessed a non-repudiation property, it would not be necessary to impose such a term. Given that digital signatures in a public key infrastructure do not possess such a property, and the inability to create false digital signatures is based on complex theoretic assumptions,[1] the acceptance of such a term invariably involves an acceptance of risk by the user. However, the nature and extent of the risk is not made clear, and it is highly improbable that ordinary users will have the knowledge, skills and resources to manage such a risk.[2]

1 Birgit Pfitzmann, 'Fail-stop signatures: principles and applications', in *Proceedings of the Eighth World Conference on Computer Security, Audit and Control* (Elsevier 1991), 125–134; Birgit Pfitzmann, *Digital Signature Schemes: General Framework and Fail-Stop Signatures* (Springer 1996).

2 Audun Jøsang and Bander AlFayyadh, 'Robust WYSIWYS: a method for ensuring that what you see is what you sign', in Ljiljana Brankovic and Mirka Miller (eds), *Proceedings of the Sixth Australasian Conference on Information security – Volume 81* (Australian Computer Society 2008), 53–58; Bohm, 'Watch what you sign!'; Don Davis, 'Compliance defects in public-key cryptography', *Proceedings of the Sixth USENIX UNIX Security Symposium* (San Jose, CA, 1996).

Authenticating the sender

7.225 There are various methods of obtaining sufficient evidence to demonstrate, with a degree of probability, that an electronic signature came from the person it purports to have been sent by. The aim is to gather sufficient evidence to be assured that the person sending the signature is the person they claim. Attempts are made, using various mechanisms, to obtain information from a combination of the following:[1]

Proof by knowledge: what the person knows.

Proof by possession: what the person owns.

Proof by characteristics: what the person is.

1 For an analysis of the strengths and weaknesses of each, see Richard E. Smith, *Authentication from Passwords to Public Keys* (Addison-Wesley 2002), 1.6.

7.226 When combined, the techniques relating to authentication can provide a higher level of authentication than a single method. In many instances, the method by which a person seeks to authenticate themselves is through a combination of hardware and software. A software component can retrieve and verify passwords. A token, such as a smart card, can be placed in a slot in a computer or in a separate 'reader'. However, both methods are vulnerable to attacks.[1] Identification can also be achieved by using a biometric measurement.

1 Saar Drimer, Steven J. Murdoch and Ross Anderson, 'Optimised to fail: card readers for online banking', in Roger Dingledine and Phillipe Golle (eds), *Financial Cryptography and Data Security, 13th International Conference, FC 2009, Accra Beach, Barbados, February 23–26, 2009* (Springer 2009), 184–200; Bohm and Mason, 'Identity and its verification'.

The ideal attributes of a signature in electronic form

7.227 Whether a signature is in manuscript or electronic form, the purpose for affixing the signature will not alter. However, when a signature is in electronic form, more considerations will apply. While it is abundantly clear that a manuscript signature can be forged, or can be transferred from one piece of paper to another,[1] or that documents

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

can be altered after they have been signed, digital signatures can help to resist attacks of these kinds. The requirements of a digital signature are set out below:

> (1) The signature must be authentic. In this respect the method ought, ideally, to provide for the authentication of the origin of the data and the integrity of the message.
>
> (2) Ideally, there ought to be a technical method in place that prevents the person appending the signature to the document from claiming later that they did not sign it. This is virtually impossible to achieve in the electronic environment. Care must be taken to distinguish between the degree of probability that a system can be designed to prevent a person from making such a claim, and any suggestion of a presumption that purports to bind the user to a signature that is verified.[2]
>
> (3) The signature should not be capable of being forged, in that the private key is secure.
>
> (4) Where a signature is added to a message that comprises a legal act, the signature and its link to the relevant document should remain verifiable for as long as it is of legal importance.
>
> (5) The signature cannot be reused.
>
> (6) The document that has been signed cannot be altered without rendering the signature unverifiable.[3]

1 For examples where the cutting and pasting of manuscript signatures have been upheld in the USA, see Iowa: *Ferguson v Stilwill*, 224 N.W.2d 11, where the signature of the Illinois Secretary of State, cut from an instrument and attached to a certificate of conviction, was sufficient in the absence of evidence to show the act of pasting was not authorized (1974); Maine: *Richardson v Bachelder*, 19 Me. 82, 1841 WL 932 (Me.), 1 App. 82, where an attorney affixed the signature of the magistrate, which was physically on a slip of paper, to the writ, and the writ was held to be properly issued, the magistrate having recognized and adopted it.

2 For an analysis of the means by which a computer can be affected by malicious software, see Daniel Bilar, 'Known knowns, known unknowns and unknown unknowns: anti-virus issues, malicious software and internet attacks for non-technical audiences' (2009) 6 Digital Evidence and Electronic Signature Law Review 123.

3 Bruce Schneier, *Applied Cryptography* (2nd edn, Wiley 1996), 2.6.

7.228 In the digital environment, it is considered technically possible to achieve all of these attributes – in theory[1] – but it must be emphasized that the connection between the human and the machine cannot be bridged, and the technology is fallible.[2] Practical problems, which are discussed below, continue to exist with the implementation of a digital signature. However, the essential functions set out above can, largely, be met by the application of cryptography to the formation of a digital signature. As with manuscript signatures, there are always risks attached to the use of any form of electronic signature, and the user, whether a sending party or a receiving party, should make themselves aware of the risks before using any form of electronic signature for high value transactions.

1 Javier Lopez, Rolf Oppliger and Günther Pernu, 'Why have public key infrastructures failed so far?' (2005) 15 Internet Research 544.

2 Adam L. Young and Moti Yung, *Malicious Cryptography: Exposing Cryptovirology* (Wiley 2004).

7.229 There is one further meaning that an electronic signature cannot, without education and training, provide. This is the addition of what is termed 'social meaning', or what can also be described as the 'significance of the act'. A ceremony is attached to the signing of a document, and when a person affixes their manuscript signature to a document, the importance of the act is reinforced by the physical nature of the act, because 'People

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

intuitively understand that they are legally responsible for the documents to which they attach their autographs'.[1] The function of attaching an electronic signature to a document or message is not understood in the same way as the use of manuscript signatures, partly because the signature can be applied to the document without any action by the individual to whom the signature is attributed, or even without their knowledge.[2]

1 Jos Dumortier, Patrick Van Eecke and Ilse Anné, *The Legal Aspects of Digital Signatures* (Interdisciplinary Centre for Law & Information Technology, Katholieke Universiteit Leuven, 1998), 77.
2 Eileen Y. Chou, 'Paperless and soulless: e-signatures diminish the signer's presence and decrease acceptance' (2015) 6 Social Psychological and Personality Science 343.

Methods of authentication

Authentication using secret codes

7.230 Secret codes or passwords have been used for some time, especially in banking. The code usually consists of a combination of digits or characters or both. The principle is based on ensuring the code is unique and only known to the user and the issuer. There is a shared secret between the two parties. The user identifies themselves by using the code, and if the code is correct, the issuer assumes the person entering a transaction is the person to whom the code is assigned.[1] Secret codes tend to be most appropriate when used in a closed community, as opposed to the open structure of the Internet, because a secret code cannot guarantee the identity of the person using the code. However, it should be noted that the evidence of a shared secret will not necessarily be sufficient to satisfy the relying party that an authorized user used the code. Evidence of the procedures and systems used by the relying party will not be sufficient to prove to a third party, such as a court, that it was the user that added the code. It is posited that a secret code cannot be considered strictly as a signature, because the code tends only to be used for the single characteristic of authenticating the user,[2] but two courts have decided otherwise, with respect correctly, given the facts.[3]

1 See United States District Court, Southern District of New York: *Banco del Austro, S.A., v Wells Fargo Bank, N.A.*, 215 F.Supp.3d 302, 90 UCC Rep.Serv.2d 1292; Salvatore Scanio, 'Interbank liability for fraudulent transfers via SWIFT: Banco del Austro, S.A. v. Wells Fargo. Bank, N.A.', (2017) 36(12) Banking & Fin Services Pol'y Rep 8; on the 2016 hack of the computers at Bangladesh Bank, the central bank of the country of Bangladesh, see Julie Anderson Hill, 'SWIFT bank heists and Article 4A' (2018) 22 J Consumer & Com L 25, and Geoff White and Jean H. Lee, 'The Lazarus heist: How North Korea almost pulled off a billion-dollar hack' (this is the story of the hack taken from 'The Lazarus Heist', a series of 11 programmes on BBC News World Service, broadcast in April 2021), https://www.bbc.co.uk/news/stories-57520169.
2 Anderson, *Security Engineering*, 10.4 for a study of the problems relating to ATMs; Dumortier and others, *The Legal Aspects of Digital Signatures*, 60–63.
3 *Standard Bank London Ltd v Bank of Tokyo Ltd* [1995] 2 Lloyd's Rep 169, [1995] 3 WLUK 182, [1995] CLC 496, [1998] Mason's CLR Rep 126, Times, 15 April 1995, [1995] CLY 397 and *Industrial & Commercial Bank Ltd v Banco Ambrosiano Veneto SpA* [2003] 1 SLR 221, where a message using an authentication code sent through the SWIFT (Society for Worldwide Interbank Financial Telecommunication) system had the legal effect of binding the sender bank according to its contents, and where a recipient bank undertook further checks on credit standing or other aspects, this did not detract from this proposition.

Authentication using biometric measurements

7.231 Using a biometric measurement is the method by which it is possible to authenticate an individual through the measurement of physical characteristics.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

A biometric measurement has the ability to identify a person because the image is reduced to digital form. Such a measurement represents a unique characteristic of that individual, but it cannot be a secret. Human characteristics comprise a number of attributes, some of which lend themselves to being measured:

> (1) Appearance, such as height, weight, colour of skin, hair and eyes, visible physical markings, gender, facial hair, wearing of spectacles.
>
> (2) Social behavioural traits, including voice recognition, style of speech, visible handicaps.
>
> (3) Natural physiography, such as iris patterns, retinal scan, fingerprint or thumbprint verification, capillary patterns in earlobes, two or three dimensional facial recognition, vein check and hand geometry, DNA patterns.
>
> (4) Bio-dynamics, such as signature verification and the dynamics when using the keys on a keyboard.[1]

1 Anderson, *Security Engineering*, ch. 15.

7.232 There are significant difficulties with the use of biometric measurements, including the range of tolerances to reduce false negatives and increase false positives, or vice versa. The manufacturer of the device usually sets the tolerances, and a great many devices do not work as claimed.[1]

1 Anderson, *Security Engineering*, ch. 15.

Fingerprints

7.233 Most fingerprint systems use optical or capacitive sensors for capturing the details of a fingerprint, such as branching and end points of the ridges. An optical sensor detects differences in reflection, while capacitive sensors detect differences in capacitance. Other systems use thermal sensors and ultrasound sensors. The process can be described thus: the image of the fingerprint is captured, features are then extracted from the image, and they are stored as templates on a database. Some systems encrypt templates and only manage the compressed images. Although widely used, there are problems associated with fingerprint scanners. Such systems can be undermined in a number of ways:

> (1) A person can be forced to press their finger against a scanner by a criminal.[1]
>
> (2) An impostor can use their own fingerprint and challenge the false rejection rate and false acceptance rate. Fingerprints tend to be categorized as 'loops', 'whorls' and 'arches', among other descriptions. If the impostor knows the category of the registered fingerprint and has a pattern similar to that of the registered one, there is a possibility that the scanner may not reject the false fingerprint.
>
> (3) A person may have their finger cut off, so a criminal can use the severed finger to defeat the scanning device.[2] This can be avoided where a device also gauges the temperature of the finger.
>
> (4) The use of an artificial clone of the original fingerprint, where a fingerprint is copied by making a mould of the registered fingerprint. Such copies are cheap to replicate and seem to be effective against many fingerprint devices.[3]
>
> (5) Other attacks will work, depending on the nature of the fingerprint system, such as making a noise or flashing a light against the scanner. Other techniques that can cause the scanner to stop working within the tolerances to the environment include heating up, cooling down, changing the humidity, and hitting or causing the scanner to vibrate.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

1 The police in Norway now have the power to force a finger or thumb on to a screen to unlock it, for which see Ingvild Bruce, 'Forced biometric authentication – on a recent amendment in the Norwegian Code of Criminal Procedure' (2017) 14 Digital Evidence and Electronic Signature Law Review 26.
2 See the example of Mr Kumaran, who had the tip of his index finger chopped off by thieves because the security system installed in his S-Class Mercedes Benz utilized the measurements of both the index fingers and thumbs of the owner. The immobilizer system caused the engine in the vehicle to cut out after a few minutes unless the owner pressed their finger or thumb on to the sensor: Jonathan Kent, 'Malaysia car thieves steal finger', BBC News Kuala Lumpur, 31 March 2005, http://news.bbc.co.uk/1/hi/world/asia-pacific/4396831.stm).
3 Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada and Satoshi Hoshino, 'Impact of artificial "gummy" fingers on fingerprint systems', Paper prepared for Proceedings of SPIE Vol 4677 Optical Security and Counterfeit Deterrence Techniques IV, 24–25 January 2002, http://cryptome.org/gummy.htm; note the comments on tests run by others as a result of this research in Anderson, *Security Engineering*, 15.5; see also David Chek Ling Ngo, Andrew Beng Jin Teoh and Jiankun Hu (eds), *Biometric Security* (Cambridge Scholars Publishing 2015). It is becoming possible to use machine learning to create false fingerprints: Philip Bontrager, Aditi Roy, Julian Togelius, Nasir Memon and Arun Ross, 'DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution' in *Proceedings of IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)* (Los Angeles, USA,October 2018), https://arxiv.org/pdf/1705.07386.pdf.

7.234 Regardless of how easy it may be to defeat fingerprint reading systems, they seem to be most effective when used as a deterrence factor, especially in reducing false claims by people on state benefits.[1]

1 Anderson, *Security Engineering*, 15.9.

7.235 In summary, it is possible to use a measurement of a biometric characteristic to authenticate an individual, but the use of such a measurement can only be effective in a closed system. There are many problems associated with the use of biometric measurements in an open system that have yet to be resolved.

Types of infrastructure for asymmetric cryptographic systems

7.236 There are a number of methods that provide for the signing of electronic documents by means of a digital signature. The discussion in this chapter will focus on the issues relating to the provision of key pairs that are provided and maintained by commercial organizations. However, it is to be noted that key pairs generated and used by individuals using any form of digital signature will also be subject to many of the issues discussed below.

7.237 The type of structure will affect the nature and extent of the legal liability that participants are exposed to. This in turn will determine how participants manage their legal liability. The two categories are:

> (1) A closed environment, where there is only one domain for all communications. This domain can be located in a single place for a single enterprise, or comprise a collection of enterprises, each of which operates under the same set of technical and operational procedures. One example may be a multinational company that operates in several jurisdictions and maintains an intra-company domain across the world. Another example may be a group of end users (both sending and receiving parties) that enter a network with one or more certification authorities by which liability is allocated according to agreed contractual terms between the parties. IdenTrust and Bolero are examples of such networks.[1]

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> (2) An open environment, where a sender enters into an agreement with a certification authority to provide a certificate for a verification key, and where the receiving parties are not known by either the sending party or certification authority in advance. The role of trusted third parties, also called certification authorities, is to provide certificates that link the identity of the owner to the public key.[2] These bodies can be public or private, licensed or unlicensed. Whether a certification authority is in the hands of a public or private body, and whether is it licensed or unlicensed, it must be trustworthy.

1 IdenTrust: http://www.identrust.com; Bolero: http://www.bolero.net.

2 Certification authorities issue certificates linked to a monetary value to limit liability on the certificate. When submitting documents to a court, it would hardly seem necessary to link the digital signature to the monetary value placed on the certificate, because the content of the document is the item of value, and the court does not rely on the monetary value of the certificate to accept documents electronically. This issue arose in the German case of FG Münster 11 K 990/05 F (Electronically signed statement of claim – On the interpretation of the term 'monetary limitation') before the Finance Court of Münster in Westphalia on 23 March 2006, which dismissed the claim because the corresponding signature certificate contained a monetary limitation of €100. This decision caused some consternation in Germany, for which see Martin Eßer, 'Case note – Germany' (2006) 3 Digital Evidence and Electronic Signature Law Review 111. The Federal Finance Court (Bundesfinanzhof) subsequently heard the appeal to this decision, and it was held that if such a signature contained a monetary restriction that restricts the kind of transactions it can be used for, the restriction does not impair the validity of the signature for the purposes of legal appeals: File number XI R 22/06; BB 2007, 92 (leading record only, otherwise not published); Martin Eßer, 'Case note Germany, 19 February 2009, IV R 97/06' (2009) 6 Digital Evidence and Electronic Signature Law Review 278.

Management of the key and certificate

7.238 The foundation of the public key infrastructure rests on asymmetric cryptography, with a public and private key pair. The public key is usually distributed in the form of a certificate, while the private key is a separate item with its own distinct structure that should be protected from being disclosed to unauthorized third parties when it is transported, used and stored. Once a person subscribes to a digital signature, a range of issues that are referred to as life-cycle management, among other terms, must be addressed. Regardless of the name given to the process, procedures and processes must be in place to create the certificate and key pair, verify the identity of the applicant, distribute the certificate and cancel the certificate at the end of its period of validity or before, should it be compromised. The quality of software, design of the network and management of the security system all affect the way the keys and certificate are managed and stored. This is important, because a digital signature is not computed by the user, but by software. The software on a computer will carry out the task on the instructions of a user, but the software is not in a position to identify whether the instructions come from a legitimate user or the signals from unauthorized malicious software that has successfully embedded itself in the user's computer.

Identifying an applicant

7.239 It should be recalled that an individual could generate their own public and private key pair, using software on their computer. The individual then provides the certification authority with evidence of their identity. The type of evidence and degree of proof will depend on the nature of the type of certifying certificate required. In any event, the identity of the person or entity must be bound to the public key. When

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

confirming the identity of a person or legal entity, a certification authority will tend to be expected to comply with the requirements from a recognized body.[1]

1 For an overview, see Piper and others, *Digital Signatures*, ch 5 and Adams and Lloyd, *Understanding PKI Concepts*, Part II.

7.240 The European Patent Office sets out the rules regarding electronic signatures and authentication in Decision of the President of the EPO dated 26 February 2009 concerning the electronic filing of documents.[1] In *ERICSSON/Electronic filing of appeals T1427/09*,[2] an electronic signature was affixed to the electronic filing of an appeal, but not in the correct name. This was an application for an appeal against the decision of the examining division, sent on 9 March 2009, refusing European patent application 01962282.8. The notice of appeal and the statement setting out the grounds of appeal in this case were filed electronically on 11 May 2009 and 17 June 2009 respectively. The notice of appeal dated 11 May 2009 included the name of Mr Friedrich Kühn, a European Patent Attorney. There was no manuscript signature. The electronic filing of this document was certified by a signature authentication showing that both the sender certificate and the signer certificate underlying the filing were issued to I. Elfving. Mr Kühn provided a manuscript signature to the statement setting out the grounds of appeal dated 17 June 2009. The electronic filing of this statement was certified by a signature authentication showing that both the sender certificate and the signer certificate underlying the filing were issued to R. Ahlund. The reference to a 'sender certificate' and a 'signer certificate' appears to indicate that a digital signature was affixed to the notice. In Decision of the President of the EPO dated 26 February 2009 concerning the electronic filing of documents,[3] article 8(2) provides that the authenticity of documents filed in appeal proceedings are to be confirmed by the use of an enhanced electronic signature of a person authorized to act in the proceedings in question. Neither I. Elfving nor R. Ahlund were authorized to act in the proceedings. As a result, the notice of appeal and the statement setting out the grounds of appeal were deemed not to be signed. The appellant was therefore invited to file signed copies of the documents within two months in accordance with Rule 50(3) of the European Patent Convention.

1 [2009] OJ EPO 182.
2 [2009] 11 WLUK 365, [2010] EPOR 22.
3 [2009] OJ EPO 182.

The certificate

7.241 When the certification authority has verified the identity of the individual or entity to their satisfaction, they will issue a certificate. This is a software record that affirms the connection of a public key to an identified person or corporate entity. It does not follow that a certification authority will undertake this task. There are a number of reasons for this. First, the cost of developing a suitable administrative infrastructure with the relevant expertise will be expensive. It may not, therefore, be possible to justify the cost in commercial terms. Second, there are a number of organizations that already have the relevant expertise, such as banks and credit reference agencies. While the database these organizations use may be imperfect, nevertheless it makes sound economic sense not to replicate a service that already exists. This usually means there is an added layer of contact where a certification authority issues a certificate. First, the registration authority will take steps to verify the identity of the person or legal

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

entity seeking a certificate. Upon confirmation of identity by the registration authority, the certification authority will then issue a certificate. Thus an additional layer of complexity is added to the mix surrounding the link between the person or legal entity seeking a certificate and the subsequent granting of the certificate.

7.242 The next point to ponder is the entity that generates the registration authority's key. Whoever generates the registration authority's key will also be involved in the contractual matrix. In all probability, a contractual relationship will exist between the certification authority and the registration authority, and the contract will provide for the liability and warranties between each entity. Where liability will fall in the event of a dispute will depend on the particular circumstances of the case.

The generation of the key pair belonging to the subscribing party

7.243 It is good practice for the subscribing party to generate their own key pair. Where the subscribing party generates a key pair, there is, theoretically, less of a risk of the private key being compromised. However, many subscribing parties will not have the software to generate their own key pair. This means a third party will be requested to generate a key pair on their behalf. There are two aspects to this that demonstrate a level of vulnerability that may be undesirable. The party generating the key pair will have to be trusted not to compromise the key, and the key pair will be vulnerable to attack or compromise when transported to the user.[1]

1 Adams and Lloyd, *Understanding PKI Concepts*, 92–94; Piper and Murphy, *Cryptography*, 109–110.

Validating the public key

7.244 Either the certification authority or the registration authority should carry out checks that the public key is actually that of the applicant, and that the applicant has the corresponding private key. The check is simple: it needs to be determined whether the subscriber can make a signature that can be verified by the public key. If carried out, such a check can protect both the subscribing party and the authority that undertakes the task, because it can ensure the subscribing party has submitted the correct key and the authority can demonstrate it undertook care to investigate and verify for itself that the public key was that of the applicant, thus making sure it did not certify an incorrect or invalid key.

Distributing certification authority keys

7.245 Individuals or entities wishing to use the public keys of different organizations or individuals may well have to visit each certificate authority to obtain the relevant public key. One mechanism is to have a hierarchy of certification authorities, where higher-level authorities certify low-level authorities. In this case, the prospective user needs to verify the highest level certificate first, usually called a root certification authority, then to check the trail and validity of every authority certificate that leads to the certificate the user wants to trust or use.[1] When a person buys a computer, there are a number of certificates already installed in their browsers. As a result, the user, without realizing it, 'trusts' whoever uploaded the software to the computer to include the appropriate authorities' certificates.[2] The certificates can be deleted and new ones added, if the user knows how to do this. If the user does not update their browser, the certificates will eventually expire and produce sometimes rather obscure error

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

messages when signatures are verified. In addition, unless the user is aware of the complexities of the hierarchy of certification authorities, it is possible for a malicious party to insert a fraudulent certificate into a chain of certificates, and appear to be trusted.[3]

1 Adams and Lloyd, *Understanding PKI Concepts*, 132–145 for a detailed discussion; Piper and others, *Digital Signatures*, 37–38.
2 Mason and Reiniger, ' "Trust" between machines?'
3 Niels Ferguson, Bruce Schneier and Tadayoshi Kohno, *Cryptography Engineering: Design Principles and Practical Applications* (Wiley 2010), 18.3.1 for an example of where a software fault had the capacity to undermine the security of an entire system; for further examples, especially of Secure Socket Layer (SSL) certificates, see http://wiki.cacert.org/Risk/History; *Carbanak APT: The Great Bank Robbery* (v 2.1, Kaspersky 2015), https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf.

Revocation of a certificate

7.246 The certificate is used to bind the name of a person or entity to their public key. However, just as with physical seals, there may be many reasons for revoking a certificate (or seal) before the expiry date. In the past, the owner of the seal would put notices up in such public places as churches and markets, warning people not to rely on the seal.[1] In the digital age, such notices are placed over the Internet. The reasons for revoking a certificate include, but are not limited to:

> (1) The user is aware that the private key corresponding to the certificate has been lost or compromised.
>
> (2) The certificate holder asks for the certificate to be revoked.
>
> (3) The certification authority revokes a certificate where the holder breaches a term of the agreement.
>
> (4) The certificate was issued in error.

1 As described by Wills J in *The Staple of England v The Governor and Company of the Bank of England* (1888) 21 QBD 160 at 167.

7.247 There are a range of technical solutions to providing public knowledge of certificates that have been revoked, but the most well known is the certificate revocation list.[1] A certification revocation list is a signed data structure that contains a list of those certificates that have been revoked. Where a list exists, there are a number of important issues that must be addressed:

> (1) The difference in time between the command to revoke the certificate and the last time the certificate was used.
>
> (2) The reliability of the revocation procedure; in other words, whether it can be relied upon to provide a definitive answer that can be trusted (in addition, the accuracy of the clocks that determine the time the revocation was actually uploaded to the certification revocation list – whether it was the certification authority time or the relying party time, and at whose risk – for instance the relying party deliberately sets their clock at a different time to confuse the evidence).
>
> (3) The number of revocation commands that the revocation system can handle at any one time.[2]

1 Adams and Lloyd, *Understanding PKI Concepts*, 107–126.
2 Niels Ferguson and others, *Cryptography Engineering*, 19.8.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.248 If a certification authority does not have a revocation list, the person seeking to determine whether to rely on a certificate needs to know how they can establish whether a key has been revoked or compromised.

Expiry of keys

7.249 Certificates have a fixed period of validity, in the same way that a royal seal matrix had, and they expire in due course. One technical question relates to how the life of the key is computed. Ellison and Schneier contend that the key has a 'theft lifetime' as a function of the vulnerability of the subsystem that stores the key. Other factors that should also be taken into account include the threat of physical and network exposure to attacks and how attractive the key is to an attacker.[1] In any event, there are three options available when a certificate expires: (1) no action is taken; (2) the certificate is renewed and the same public key is placed into a new certificate with a new period of validity, (3) a new pair of public and private keys are generated and a new certificate is generated to provide for a certificate update.[2]

1 Ellison and Schneier, 'Ten risks of PKI'.
2 Adams and Lloyd, *Understanding PKI Concepts*, 101–102.

The duties of a user

7.250 There are a number of points that people or organizations that use private keys should be aware of, as set out below.

(1) Management of private keys

The user must manage their private keys effectively and take measures that are appropriate to prevent the unauthorized use of the keys, and to protect them securely against any other form of attack, such as theft or misuse by a third party that gains access to the system by way of malicious software or other method. This duty is included in some electronic signature legislation.

(2) Storage of private keys after expiry

When deciding whether to use private keys, their use should be carefully monitored, because different types of algorithm are used for different purposes. Thus in the United Kingdom, consideration must be given to the possibility that a private key may be the subject of a s 49 notice under the Regulation of Investigatory Powers Act 2000, and to the safe storage of keys that have expired.

(3) Disposal of equipment with private keys

Particular care should be taken when disposing of the hardware that contains the private keys.

Internal management of a certification authority

7.251 The internal management of a certification authority, which the individual user may not be familiar with, can affect the trust to be placed in the certificates issued. Such issues include, but are not limited to, the following:

(1) The level and extent of the checks made on employees.

(2) How to verify the identity of the employees who control the keys.

(3) Policies on how keys are stored.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

(4) The mechanisms in place to verify that the relevant policies are followed.

(5) Whether the internal management of the certificate system is properly carried out.

(6) The level and extent of any insurance cover may also have a bearing on the suitability of different types of certificate issued.

Barriers to the use of the public key infrastructure

7.252 There are a variety of problems that affect those vendors that offer digital signature services. For instance:

(1) There is no standard in the industry relating to the provision of a directory service. A number of models exist and competing standards are under consideration, as well as the development of proprietary solutions.

(2) Vendors do not implement some functions, and when they are implemented, they may be implemented in a different manner to another vendor. This leads to problems with interoperability between the systems of different vendors.[1]

(3) The performance of the repository service where the certificate revocation lists are held may be a problem. At present there are a limited number of vendors that operate a public key infrastructure, and the numbers of people using those that are available are in the minority. Whether the systems in place are capable of expanding with greater use in the future is open to debate.

(4) The number of people that have any knowledge of public key cryptography is small. The numbers of personnel required are not limited to administrative personnel, but include people in senior positions who can develop the relevant policy documents, such as certification practice statements and interdomain interoperability agreements. The public key infrastructure strategy must also be considered and documented.[2]

1 Paweł Krawczyk, 'When the EU qualified electronic signature becomes an information services preventer' (2010) 7 Digital Evidence and Electronic Signature Law Review 7.

2 Adams and Lloyd, *Understanding PKI Concepts*, ch 25.

7.253 In addition, there are weaknesses that can affect the use of the signature, including the fact the data to be signed can be modified; a personal identity number can be obtained; the person affixing a signature might sign different data than intended; and an attacker can interfere with the software code as it is communicated between component parts. In essence, the signatory has to have trust in the writer of the software that it will work as intended.[1]

1 Adrian Spalka, Armin B. Cremers and Hanno Langweg, 'Trojan horse attacks on software for electronic signatures' (2002) 26 Informatica 191; Hanno Langweg, *Malware Attacks on Electronic Signatures Revisited* (2006), ftp://ftp.cryptopro.ru/pub/TrustedPass/110519/Theory/_hanno_research_gi06p.pdf; 'Attacks on PDF Signatures', https://www.pdf-insecurity.org/signature/signature.html; Fabian Ising and Vladislav Mladenov, *How to Break PDFs: Breaking PDF Encryption and PDF Signatures*, https://media.ccc.de/v/36c3-10832-how_to_break_pdfs; Christian Mainka, Vladislav Mladenov and Simon Rohlmann, 'Shadow attacks: hiding and replacing content in signed PDFs', Network and Distributed Systems Security (NDSS) Symposium 21–25 February 2021, (Virtual), https://www.ndss-symposium.org/wp-content/uploads/ndss2021_1B-4_24117_paper.pdf.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Risks associated with the use of digital signatures

Issuing a certificate to an impostor

7.254 A number of certification authorities have issued false SSL (Secure Socket Layer) certificates that support the security of websites.[1] The issuing of false certificates illustrates the weakness of how certificates are created and issued, and also how important the certificates are in relation to the operation of the Internet. It is not known whether false certificates have been issued that are associated with digital signatures that are used by people or legal entities. The 2001 example of VeriSign issuing two Class 3 Software Publisher certificates incorrectly has been cited in previous editions of *Electronic Signatures in Law* (now incorporated into this text) by way of example.[2] A more significant incident occurred in 2011, when DigiNotar B.V., a Dutch certificate authority owned by VASCO Data Security International, Inc, was placed into voluntary bankruptcy as a result of the discovery that the company had issued several hundred fraudulent certificates.[3] The company also issued certificates for the PKIoverheid program on behalf of the government in the Netherlands. A hacker obtained access to the DigiNotar computer systems and issued an unknown number of false certificates. On 2 September 2011, after being informed of the results of the investigation of the DigiNotar systems by Fox-IT, the Dutch government stopped trusting certificates issued by DigiNotar[4] and regained control over the company's intermediate certificate to manage an orderly transition, replacing untrusted certificates with new ones from another provider.[5] The fact that false certificates have been issued illustrates the weaknesses inherent in the trust placed in software code[6] – because it is software code that controls the entire edifice of everything digital – and it is imperative for lawyers to more fully understand the technical issues by adopting a realistically sceptical approach to understanding the nature of software.[7]

1 For the risks generally, see Piper and others, *Digital Signatures*, ch 4; Ferguson and others, *Cryptography Engineering*, ch 19; Doowon Kim, Bum Jun Kwon and Tudor Dumitras, 'Certified malware: measuring breaches of trust in the windows code-signing PKI', in *CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (Association for Computing Machinery 2017), 1435–1448, https://dl.acm.org/doi/10.1145/3133956.3133958. See the CAcert Wiki for a list of fraudulent certificates that have been issued (the aim of this website is to maintain a list of attacks with reasonably authoritative references): http://wiki.cacert.org/Risk/History.

2 The 'VeriSign security alert fraud detected in Authenticode signing certificates', 22 March 2000, is no longer available, nor is Gregory L. Guerin, 'Microsoft, VeriSign, and certification revocation'; the CERT Advisory is also no longer available; for the Microsoft Security Bulletin MS01-017, see https://docs.microsoft.com/en-us/security-updates/securitybulletins/2001/ms01-017; US Department of Energy Computer Incident Advisory Capability, L-062: Erroneous Verisign-Issued Digital Certificates for Microsoft; Ferdinand Gomes, 'Security Alert: Fraudulent Digital Certificates' (SANS Institute 2003), https://www.sans.org/reading-room/whitepapers/certificates/security-alert-fraudulent-digital-certificates-679.

3 The bankruptcy of DigiNotar B.V. is set out in Form 10-K submitted by VASCO Data Security International, Inc. to the US Securities and Exchange Commission on 10 March 2017, https://s24.q4cdn.com/314592314/files/doc_financials/2016/q4/VASCODataSecurityInternational_10K_20170310.pdf.

4 *Factsheet: Fraudulently Issued Security Certificate Discovered*, 5 September 2011, version 2.2 (no longer available); *Black Tulip Report of the Investigation into the DigiNotar Certificate Authority Breach* (Fox-IT BV, PR-110202, 13 August 2012, version 1.0), https://www.researchgate.net/publication/269333601_Black_Tulip_Report_of_the_investigation_into_the_DigiNotar_Certificate_Authority_breach.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

5 *Overheid zegt vertrouwen in de certificaten van Diginotar op, Nieuwsbericht* (3 September 2011) (no longer available).
6 Mason and Reiniger, ' "Trust" between machines?'
7 Note the comments by Nico van Eijk in 'The DigiNotar case: internet security is no abstract matter' (2013) 23 Computers & Law 21.

Certificate revocation list

7.255 There are two technical issues that affect the ability to download a suitably recent certificate revocation list: how the certification authority tells you where to obtain the relevant certificate revocation list, and whether your computer carries out the functions you require. There are many different ways to obtain a certificate revocation list, and because there is no standard within the industry, no one method is mandatory.[1] Regardless of the method used, the significant issues for every recipient, which they may not be aware of, are as follows:

> (1) The certificate revocation list should be digitally signed by the certificate authority using its root certificate to prevent a certificate revocation list from being forged.
>
> (2) The certificate revocation list is dated by the certification authority, which means that every certificate revocation list expires.
>
> (3) Every certificate revocation list has a higher sequence than the one issued previously, to prevent forgery.
>
> (4) The person wishing to check a particular certificate must know where to find a suitably recent certificate revocation list.
>
> (5) The certificate revocation list must be able to be obtained by a relying party.
>
> (6) The contents of the certificate revocation list must be authenticated.

1 Adams and Lloyd, *Understanding PKI Concepts*, 107–126.

7.256 Any duty that is to be imposed on a certification authority should take into account the complexity of these issues. If Microsoft designed the software to take a user to the address where the certificate revocation list existed only if the address was provided by the certification authority with the certificate, then establishing the responsibility for passing on this knowledge to a recipient will be a necessary prerequisite to any possible defence by a certification authority. In the VeriSign case, it did not issue Class 3 Software Publisher certificates with an address for the certificate revocation list. This appears to mean that, at the time of the incident, the user of the relevant Microsoft software was not able to retrieve the certificate revocation list of a given certifying certificate issued by VeriSign and Guerin concluded that Microsoft did not have software that had a working revocation infrastructure. Microsoft did not agree with this analysis, and published a rebuttal that is no longer available,[1] to which Guerin rebutted the points raised by Microsoft in his article, which is also no longer available. The report located on the US Department of Energy Computer Incident Advisory Capability website, referring to 'L-062: Erroneous Verisign-Issued Digital Certificates for Microsoft' no longer appears to be available. However, if a vendor of software such as Microsoft did not have a working revocation infrastructure in place in the past, then it could be argued that past certificates can hardly be said to be reliable. This means the evidential weight to be given to a certificate must be considered against these practical problems, otherwise the evidence may be so poor as to make the concept of

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

a certificate irrelevant. Arguably, a court should take such practical issues into account when deciding whether a duty of care should be imposed on a certification authority.

1 Microsoft published 'Response to inaccurate Crypto-Gram article on VeriSign certificates' at https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc751324(v=technet.10)?redirectedfrom=MSDN.

7.257 Depending on how it is used, a public key infrastructure has its uses.[1] However, it is very important to be clear about what a digital signature can and cannot do.

1 Ferguson and others, *Cryptography Engineering*, at 19.9, 'So what is a PKI good for?'. The authors conclude that 'there are few advantages to PKIs'.

What a digital signature is capable of doing

7.258 The uses to which cryptography can be put within a public key infrastructure include demonstrating the integrity of the message and providing for the confidentiality of a document, although using digital signatures within a public key infrastructure will not act to correct human behaviour.[1] A public key infrastructure is only capable of making a link between a public key and a claimed identity. A digital signature only authenticates that a certain private key was used to create the relevant digital signature.

1 Davis, 'Compliance defects in public-key cryptography', paragraph 1; Adams and Lloyd, *Understanding PKI Concepts*, ch 14 for a useful and more detailed discussion; Bernard Reynis and Ugo Bechini, 'European civil law notaries ready to launch international digital deeds' (2007) 4 Digital Evidence and Electronic Signature Law Review 14; Joan Decker, 'The e-notarization initiative, Pennsylvania, USA' (2008) 5 Digital Evidence and Electronic Signature Law Review 73; Timothy S. Reiniger, 'The proposed international e-identity assurance standard for electronic notarization' (2008) 5 Digital Evidence and Electronic Signature Law Review 78; this article is followed by the text of 'The draft International Electronic Notarization Assurance Standard' (2008) 5 Digital Evidence and Electronic Signature Law Review 81.

What no form of electronic signature is capable of doing

7.259 A digital signature can provide for the authenticity of information. It binds key pairs with names. The recipient of a message or document with which a digital signature is associated can confirm the binding of the verification key with the name of the person whose private key has been used. But the recipient cannot determine whether the sending party authorized the use of the digital signature: this is also true of any other form of electronic signature. The private key of a digital signature is protected by a password or passphrase. The most important point to be aware of is this: *the private key of a digital signature is only as good as the password that protects it*. This means that when the password is inserted into a computer to provide access to the private key of a digital signature, it proves any of the following:

> (1) The person to whom the private key was issued might have been the person that inserted this information into the software, and therefore the recipient can infer that the private key of the digital signature is capable of proving that the person to whom the private key was issued was physically at the keyboard at the time of the session; or
>
> (2) a person (perhaps the owner of the private key or her secretary) instructed the software to retain the password information in the computer memory, so that any person (*whether they were sitting in front of the computer or whether they*

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> *obtained control of the computer remotely)* who obtains access to the private key can use the password, which in turn does not prove that the person to whom the private key was issued is physically at the keyboard at the time of the session (the recipient of the correspondence is not to know whether it was the person whose key it was, or her secretary, or an impostor), although it can be concluded that the use of the password proved the computer stored this information; or
>
> (3) that a person (whether the owner of the key, their secretary or an imposter) who used the password actually knew the password.

7.260 The recipient relies on one small item to persuade them that the sender is the person whom they claim to be: the password that enables the sender to cause a computer to affix the private key of a digital signature to the document. In reality, reliance rests on the quality of the digital evidence[1] that ties a presumed identity to a presumed act, and in turn the integrity of the password, the software code and the security in place to protect the password and private key. The problems with passwords are so well known that Dan Geer merely stated the obvious in a talk at the UNC Charlotte Cyber Security Symposium in 2013: 'Everyone in this room knows how and why passwords are a problem.'[2]

1 Bearing in mind that computers and networks are not secure, for which see in the legal context, R. R. Jueneman and R. J. Robertson, Jr, 'Biometrics and digital signatures in electronic commerce' (2008) 38 Jurimetrics Journal 427; note also the further technical problems in P. Švéda and V. Matyáš Jr, 'Digital signatures and electronic documents: a cautionary tale revisited' (2004) 5 Upgrade 35.

2 Dan Geer, 'Tradeoffs in cyber security', a talk at the UNC Charlotte Cyber Security Symposium (2013), 9 October 2013, http://geer.tinho.net/geer.uncc.9x13.txt; see also Joseph Bonneau and Ekaterina Shutova, 'Linguistic properties of multi-word passphrases', in Jim Blythe (ed) *Financial Cryptography and Data Security Volume 7398* (Springer 2012), 1–12; Joseph Bonneau, Cormac Herley, Paul C. van Oorschot and Frank Stajano, *The Quest to Replace Passwords: a Framework for Comparative Evaluation of Web Authentication Schemes* (University of Cambridge Computer Laboratory Technical Report 817, 2012), https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf; Dan Goodwin, 'Anatomy of a hack: how crackers ransack passwords like "qeadzcwrsfxv1331" ', arstechnica, 21 May 2013, http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/; Andrey Belenko and Dmitry Sklyarov, ' "Secure password managers" and "military-grade encryption" on smartphones: oh, really?', (n.d.), http://www.elcomsoft.co.uk/WP/BH-EU-2012-WP.pdf.

7.261 It is generally recognized that the password is an exceedingly weak mechanism, as indicated by P. C. van Oorschot and Julie Thorpe:

> The ubiquitous use of textual passwords for user authentication has a well-known weakness: users tend to choose passwords with predictable characteristics, related to how easy they are to remember. This often means passwords which have 'meaning' to the user. Unfortunately, many of these 'higher probability' passwords fall into a tiny subset of the full password space. Although its boundaries vary depending on its exact definition and the probabilities involved, we refer to this smaller subset as the probable password space.
>
> Ideally, users would choose passwords equi-probably from a large subset of the overall password space, to increase the cost of a dictionary attack, i.e., a brute-force guessing attack involving candidate guesses from a prioritized list of 'likely passwords'. If a password scheme's probability distribution is non-uniform, its entropy is reduced. [1]

1 P. C. van Oorschot and Julie Thorpe, 'On the security of graphical password schemes', Technical Report TR-05-11, http://service.scs.carleton.ca/sites/default/files/tr/TR-05-11.pdf. There is a considerable amount of material on this topic, together with the associated subject of memory and the

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

human need to write down complex passwords (which could have a bearing on whether a human can be made liable for writing down passwords that the vendor or bank insists must be long and difficult to remember), for which see the following short list of more recent references, all of which in turn refer to other sources: Kirsi Helkala and Nils Kalstad Svendsen, 'The security and memorability of passwords generated by using an association element and a personal factor', in Peeter Laund (ed) *Information Security Technology for Applications, Lecture Notes in Computer Science, Volume 7161* (Springer 2012), 114–130; Joseph Bonneau, 'Guessing human-chosen secrets' (University of Cambridge Computer Laboratory Technical Report 819, 2012); Joseph Bonneau and Sören Preibusch, 'The password thicket: technical and market failures in human authentication on the web', *Ninth Workshop on the Economics of Information Security* (WEIS 2010), http://www.jbonneau.com/publications.html and http://preibusch.de/publications/password_market/; Wendy Moncur and Grégory Leplâtre, 'PINs, passwords and human memory' (2009) 6 Digital Evidence and Electronic Signature Law Review 116; Martin A. Conway and Emily A. Holmes, *Guidelines on Memory and the Law: Recommendations from the Scientific Study of Human Memory* (The British Psychological Society Research Board 2008, revised 2010), https://www.academia.edu/2326108/Guidelines_On_Memory_And_The_Law_Recommendations_From_The_Scientific_Study_Of_Human_Memory; Mark L. Howe and Lauren M. Knott, 'The fallibility of memory in judicial processes: lessons from the past and their modern consequences' (2015) 23(5) Memory 633, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4409058/; Herley and others, 'Passwords' (the authors report that transactions by way of a PIN reverse the burden of proof, but this is not correct).

7.262 The weaknesses are also explored by Petr Švéda and Václav Matyáš Jr.[1] The authors illustrate, at paragraph 3, that when a person has the private key of a digital signature on their computer, the user or owner 'cannot be sure that no further signature processes will be executed in the background when using his private key', and they make the point in paragraph 4 that 'It is very hard to build a system or an application that does not compromise its security. There are a lot of potential problems – e.g., it can be misused, one of the components can fail, as well as the signing application, keys stored on hard disk or in memory are vulnerable'. They go on to indicate, at 4.1:

> At the time of writing, we know of no technology that can make a hardware device fully resistant to penetration by a skilled and determined attacker from a powerful organization. A lot of experts believe that absolute protection will remain unattainable. So the total cost of breaking a hardware device has to be much more than the value of stored and protected information.

1 Švéda and Matyáš, 'Digital signatures and electronic documents'; Peter A. Loscocco, Stephen D. Smalley, Patrick A. Muckelbauer, Ruth C. Taylor, S. Jeff Turner and John F. Farrell, 'The inevitability of failure: the flawed assumption of security in modern computing environments', in *21st National Information Systems Security Conference: Building the Information Security Bridge to the 21st Century* (National Institute of Standards and Technology 1998), 303–314, https://babel.hathitrust.org/cgi/pt?id=coo.31924083977813&view=1up&seq=5 – the individual paper is available at https://www.cs.utah.edu/flux/fluke/html/inevit-abs.html; Dan Goodin, 'Once seen as bulletproof, 11 million+ Ashley Madison passwords already cracked', arstechnica, 10 September 2015, https://arstechnica.com/information-technology/2015/09/once-seen-as-bulletproof-11-million-ashley-madison-passwords-already-cracked/.

7.263 Smart cards are also vulnerable, as the authors point out at 4.2 (reference omitted):[1]

> A smart card is a simple and inexpensive security module. It consists of multiple components combined with a single chip that uses external power supply and clock. When a card is used as a personalized trusted device it generates a key pair locally, stores the private key locally, and only publishes the corresponding public key. The biggest problem with smart cards is that they lack a direct

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> communication channel to the user. None of current available smart cards has a really trustworthy user interface. The user is completely dependent on potentially untrusted devices to get some information about his transactions. For example if the personal computer to which the smart card has been connected is compromised, it might ask the smart card to sign a completely different message to that which the user sees.
>
> Many successful attacks have occurred because smart cards were exposed to more sophisticated attackers than designers anticipated ... The smart card without trustworthy user interface is a typical example of an architectural error. Many attacks are also possible due to protocol and application programming interface failures.

1 Klaus Schmeh, *Cryptography and Public Key Infrastructure on the Internet* (Wiley 2001), has a different view, although acknowledges attacks are possible (15.2.3).

7.264 In summary, it is necessary to ensure the person receiving data signed with the private key of a digital signature understands the difference between trusting the signature and trusting the owner of the signature.

The weakest link

7.265 Although this chapter has emphasized the reliance placed upon the activities of certification authorities and other participants in the public key infrastructure (registration authorities, directory services listing public keys, certification revocation list services, time stamping, to name but a few), comparatively little discussion has been given to the weakest link in the chain of a digital signature. If Bob wants Alice to use a digital signature to authenticate her messages, he has to persuade Alice that it is essential that when he receives a message or document from her, he can be completely assured, whether he decides to become a verifying party or not, that it was Alice, and only Alice, who caused the digital signature to be affixed to the document or message. He therefore has to persuade Alice that she must take good care of her private key, such that she accepts the risk of being held responsible for unauthorized use of it by others. If Alice asks, not without reason, 'What's in it for me?', there seems to be no answer. Whether Bob decides to undertake the sometimes gargantuan task of carrying out the verification procedure or not, if he cannot satisfy himself that Alice kept her private key absolutely safe, he cannot be sure that Alice affixed the digital signature to the message. So he will try to insist that Alice carries the blame anyway.

7.266 In any event, the recipient of a digital signature can be certain that:

> The person (whomsoever they might be) who keyed in the password that protects the private key of the digital signature, knew the password.

7.267 Or in the alternative, the recipient of a digital signature can be certain that:

> The person who caused the private key to be attached to an email or document called up the private key and clicked on the 'password' icon (they did not need to know the password) because the software was instructed to remember the password.

7.268 There seems to be an unquestioning reliance on the use of digital signatures that has no bearing on the risks associated with the use of the technology. This reliance is

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

also manifest in the assumption made that a digital signature proves the person whose signature it is, and was the person that caused the computer to affix the signature to the document, as in the Portuguese case of (Evora) Ac. RE 13-12-2005 (R.982/2005), in which an email was sent with a digital signature attached. In this instance, it was determined that the digital signature served to authenticate the document, and guaranteed the identity of the sender and the integrity of the message. While a digital signature is capable of identifying the sender, it cannot guarantee that the sender caused the digital signature to be affixed to the message. The most important point to be aware of is this: the private key of a digital signature is only as good as the password that protects it and any additional mechanism used to protect the private key, as Richard E. Smith has pointed out:

> Public key cryptography succeeds only as long as a private key's owner can keep it under control – always available when needed but never disclosed to anyone else. [1]

1 Richard E. Smith, *Authentication: From Passwords to Public Keys* (Addison-Wesley 2002), 431.

7.269 It will be argued by some that the private key to a digital signature can be secured by a combination of a password and the biometric measurement of a fingerprint, for instance. This 'solution' relies on the technology (secret) of the biometric scanner that is chosen to fulfil this role, and does not take into account the various methods by which the mechanism can be compromised.

7.270 A digital signature is not linked to the person creating it: the unique link is made with the private key, not the user. Nobody is capable of committing a private key to memory[1] because it is far too complicated, which is why passwords are used to protect the key. Below is an example of a private key in TXT format (2048 bits), by way of example:

> privateExponent:
>
> 5c:a2:77:1b:6a:45:0c:af:e4:aa:c3:91:b2:7e:ab:ea:ec:27:14:25:6a:2a:67:d8:ce:25:1a:e4:09:11:f2:31:10:b1:43:c9:dd:d7:a7:13:d7:14:21:91:c5:15:27:ff:cd:8d:64:d5:e5:3e:64:48:a2:95:ec:d9:3f:75:8e:22:d9:11:42:90:c3:e9:fb:de:3d:ba:69:d4:db:b5:eb:84:68:f1:92:ad:36:71:04:b4:4a:f6:03:2f:5f:6c:ac:b0:ed:30:5a:89:94:c8:82:ea:55:eb:62:e8:09:0b:d0:d2:40:b8:a7:2e:70:71:aa:59:58:14:21:ae:20:d6:16:84:d2:29:5c:9b:a7:56:50:3a:10:0b:c6:70:2b:97:dd:f8:fa:73:74:22:5f:d6:ce:0d:75:45:8a:61:5d:86:25:cb:ad:19:06:fe:8e:a4:f9:0d:35:2a:02:04:93:ec:df:0c:db:ca:f0:8c:ae:a7:54:c2:37:a1:11:7b:9f:40:54:a4:fd:31:a4:f9:ee:60:3c:8f:3b:0e:b1:e2:10:6d:f0:36:50:63:27:6e:cc:85:c1:5d:10:4a:36:23:5d:bf:c7:ee:9b:af:3f:e6:49:47:c6:9e:b8:00:b0:d9:d2:de:07:46:43:14:2f:de:7c:51:57:a5:8d:4b:13:04:54:25:3b:d5[2]

1 'Guidelines on memory and the law recommendations from the scientific study of human memory'; Howe and Knott, 'The fallibility of memory in judicial processes'.

2 This example is from Symeon (Simos) Xenitellis, 'The open-source PKI book: a guide to PKIs and open-source implementations' and quoted under GNU Free Documentation License, Version 1.3, 3 November 2008, published by the Free Software Foundation: http://ospkibook.sourceforge.net/docs/OSPKI-2.4.7/OSPKI-html/sample-key-components.htm. For an example of a private key in PEM format, see http://ospkibook.sourceforge.net/docs/OSPKI-2.4.7/OSPKI-html/sample-priv-key.htm. I am grateful to Arnis Paršovs and Alan Liddle for explaining that it is only necessary to memorize this part.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.271 This means that private keys are retained on a computer, disk or smart card. It is not possible to create an electronic signature that can be uniquely linked to the signatory, and it remains the case that passwords have to be relied upon to secure the private key of a digital signature.

The burden of managing the private key

7.272 The user of a digital signature is expected to keep their private key secure. Failure to do so will mean a mischievous member of staff or a malicious third party can append a digital signature to a document or message for nefarious purposes. The management of the private key acts to underpin the efficacy of a digital signature. Some of the issues to which a recipient must give consideration include those set out below.

Bypassing passwords

7.273 Depending on the nature of the application software on any given computer or system, where a user has set their security setting to 'High' they will have to enter their password every time they wish to enter their private key to affix the private key of a digital signature to a document or message. Where the security setting is set to the default, 'Low', the messages will be automatically signed without any further intervention by the user. Given this scenario, any person with access to a computer or device containing a digital signature in a powered-up state will be able to send messages or documents with a digital signature affixed.

7.274 A busy person might find it inconvenient to enter their password every time they wish to use their private key to affix a digital signature to a document or message. An alternative is for the user to retain their private key in memory during the login session. If a user keeps the private key in memory, this exposes the key to being stolen. Examples include leaving the computer unattended, thus permitting a third party to take sufficient action to steal the key. Alternatively, if the private key is on a laptop computer and the laptop computer is stolen, it may be possible for the thief to obtain access to the private key. Further, malicious software has been developed to steal passwords and private keys.[1] Finally, even if the private key is stored on an encrypted smart card, it must be used with a computer to sign a message or document, and the computer may have been maliciously programmed to sign a document or message other than the one the user intends to sign.[2]

1 Swati Khandelwal, 'Symantec API flaws reportedly let attackers steal private SSL keys and certificates', The Hacker News, 28 March 2017, https://thehackernews.com/2017/03/symantec-ssl-certificates.html; 'How cybercrime exploits digital certificates', 28 July 2014, https://resources.infosecinstitute.com/cybercrime-exploits-digital-certificates/.

2 See Young and Yung, *Malicious Cryptography* for further examples of how the technology can be used for malicious purposes; note the discussion on this issue by Markus Rückert and Dominique Schröder, 'Security of verifiably encrypted signatures', in *Pairing-Based Cryptography – Pairing 2009, Lecture Notes In Computer Science Volume 5671* (Springer 2009), 17–34.

Quality of passwords

7.275 There are a number of issues surrounding the question of passwords, as noted above, and they are well documented. The entire edifice of the public key infrastructure and the security of the private key rests to a very large extent on the quality of the password used to protect it, and attempts are made to replace passwords.[1] Most of us prefer to use

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

passwords that are easy to remember, which in turn makes a password easy to guess and vulnerable to attack. If the user does not have effective control over the quality of the passwords used,[2] the system will be vulnerable to an offline guessing attack.[3]

1 Bonneau and others, *The Quest to Replace Passwords*.
2 Kresimir Solic, Hrvoje Ocevcic and Damir Blazevic, 'Survey on password quality and confidentiality' (2015) 56 Automatika 69.
3 Davis, 'Compliance defects in public-key cryptography'; Heiko Roßnagel and Jan Zibuschka, 'Integrating qualified electronic signatures with password legacy systems' (2007) 4 Digital Evidence and Electronic Signature Law Review 7.

7.276 If a recipient of a digital signature intends to rely on the purported authority of the signature, they have a range of options:

> (1) To rely on the signature without taking any affirmative action. In some jurisdictions, the electronic signature legislation lays down a duty on the recipient to verify the signature, although the duty is invariably set at a high level of generality. It is conceivable that judges will take into account the arrangements between the sender and recipient before reaching a conclusive judgment. For instance, if a recipient relied on a digital signature attached to a high-value contract, a court may well consider it is appropriate in the circumstances that a recipient takes reasonable steps to authenticate and verify the digital signature, and to ensure the sending party duly authorized it.
>
> (2) To rely on the signature after undertaking steps to verify and authenticate the various certificates in the chain (that is, assuming the recipient has a trusted copy of the public key of the Root Certification Authority), and checking the authenticity and reliability of any time stamps (the time the time stamp is generated should not be independent of the time the digital signature data is generated),[1] thus becoming a verifying party. Should a dispute occur, one of the questions that will need to be addressed is to what extent the actions taken by the verifying party were adequate in the circumstances of the case, including their state of knowledge at the time.
>
> (3) Ignore the infrastructure surrounding the use of the digital signature, and require the sending party to confirm their intentions by an alternative method, or to confirm, using another medium (such as letter, facsimile transmission or telephone) that the communication was sent by them.

1 Jeff Stapleton, Paul Doyle and Steven Teppler, 'The digital signature paradox' (an updated version of a paper of the same name that was originally published in the *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security*), http://docplayer.net/10585603-The-digital-signature-paradox.html.

7.277 As a result of the foregoing discussion, it becomes clear that public key cryptography is more suitable for server-to-server security, rather than for use on a desktop.

Evidence and digital signatures

7.278 Should an electronic signature become the subject of a dispute, the normal considerations will apply regarding the submission of evidence into legal proceedings, including any rules relating to the authentication of the evidence, the weight to be given to the evidence and whether it is necessary to help the adjudicator in reaching a decision by providing for expert witnesses. The following discussion aims to alert

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

the reader to some of the issues that might arise in relation to digital signatures in particular.

The evidence forming a digital signature

7.279 A certificate is issued with a digital signature,[1] which is a signed data structure that binds a public key to an identity. This certificate will purport to bind the public key to the information contained in the certificate. The subscribing party provides some of the information contained in the certificate, which may or may not be verified by the certification authority, and the certification authority is responsible for the remaining information. The subscriber will have a pair of keys, private and public. The key pairs may be generated by the keying material available to the subscribing party in their computer, by a registration authority, by the certification authority or by a trusted third party key generation facility.

1 The use of the word 'certificate' is shorthand for an individual identity certificate.

7.280 Individuals can create their own private and public key pairs, or key-generating organizations can undertake this task. The creation and certification processes are distinct. The same issues discussed here will apply to keys not certified by a third party, with the added complication that the level of authenticity may be lower because proving who the public key belonged to might be more difficult for any person wishing to rely on an uncertified key. How the key pair is generated may also be problematic if there is evidence that the software used to generate key pairs has flaws, such as being liable to generate weak keys.

7.281 A recipient can go through a list of checks to assure themselves that the certificate links the sending party to the document or message that was signed. To trust the certificate sent by Alice, Bob must check all of the certificates back to the root or foundation certificate. Only by checking back to the foundation certificate can Bob determine whether he can trust the public key in Alice's certificate in relation to the purpose for which he will use it. The certificate attached to the message or document and the corresponding public key can only be trusted if every certificate and their corresponding keys in the path from the foundation key to Alice's key can be trusted. There are two phases to this exercise:

> (1) Constructing the path, which requires Bob to bring together all the relevant certificates to form a complete path. This process may be complicated and time-consuming, because there may be a number of certification authorities in the chain, all of which have cross-certified their respective certificates. The assumption is that Bob can retrieve all of the certificates he needs to scrutinize them and put the chain of certificates together in a logical sequence. Bob must also check the issuing certificate of each of the certification authorities in the chain against a certificate revocation list.
>
> (2) Validating the path, where Bob must decide whether the path between each certificate is valid. This involves undertaking the mathematical computation to verify each digital signature; checking the validity period of each certificate for date of expiry; making sure each certificate has not been revoked, by checking the relevant certification revocation list; and then considering other issues such as the policies that apply to the certificate, any restrictions on the use of the key and if there are any other constraints on the use of the certificate.[1]

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

1 Adams and Lloyd, *Understanding PKI Concepts, Standards, and Deployment Considerations*, 147–149.

7.282 Once Bob has checked and validated the certificates and certificate path, he must then carry out the following checks:

> (1) Establishing the integrity of the certificate by ensuring the digital signature on the certificate is properly verified.
>
> (2) Checking the certificate validity period to ensure it is valid on the date and the time Bob intends to rely on it.
>
> (3) Checking the certificate has not been revoked. There are various methods to implement a certificate revocation list with a number of variations, including, but not limited to, certificate revocation lists (which is a signed data structure that contains a list of revoked certificates) and certification authority revocation lists, used to revoke the public key certificates of certification authorities and online certificate status protocol, which is a protocol that permits Bob to receive a response to his request for information.
>
> (4) Checking Alice has used the certificate in accordance with the constraints set out in the certificate, including the relevant agreements and certification policies.

7.283 As a result, when determining the nature of the evidence, it is necessary to ascertain the source of the information and the uses to which the relevant document is put. It is worth recalling the nature of the promise made to a receiving party when a sending party affixes a digital signature to a document or message:

> Bob receives a message digitally signed by Alice with Alice's digital signature certificate attached. Alice's public key is incorporated into the certificate. The certificate purports to bind Alice's name with her public key, and in turn the certificate purports to assure Bob that the message was signed using a key verifiable by a key certified in a certificate issued to Alice.

7.284 The nature of this promise is well illustrated by the following comment from the Select Committee on Trade and Industry, Seventh Report, House of Commons Session 1998–99, paragraph 12:

> Written signatures are tightly associated with people and weakly associated with documents, whilst digital signatures are tightly bound to documents and weakly bound to individuals (or identities).

7.285 The crucial point to remember is that a digital signature does not, of itself, provide evidence that the sending party actually caused the private key of the digital signature to be affixed to the message or document. This proposition is relevant in respect of any form of electronic signature. Where a certification authority is involved within the framework of a public key infrastructure, all the certification authority can do is give evidence about how the certificate was formed, where the information was obtained, and if they verified the information, what methods were used to verify the information. Thus a certification authority can give evidence as to the formation of the certificate, but the certificate cannot be adduced as evidence of the truth of the facts stated within it.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

'Non-repudiation'

7.286 By way of an introduction, the term 'non-repudiation' has become part of the vocabulary of digital signatures. This is a dangerous expression, and one that lawyers should take particular care in understanding. It does not mean the system for non-repudiation is perfect, although some technical authors (and lawyers and academics[1]) continue to assert that digital signatures are better than they actually are. By way of example, Klaus Schmeh incorrectly states that:

> The purpose of a digital signature is to ensure non-repudiation. This means that Alice cannot contest her completed signature in retrospect. When all is said and done, a digital signature is an excellent way of meeting this requirement.[2]

1 'Data encryption' (The Parliamentary Office of Science and Technology, no. 270, October 2006), incorrectly states at 2 that digital signatures 'can also be used for non-repudiation: if a party digitally signs an electronic document, they cannot later deny this'; Rouhshi Low and Ernest Foo, 'The susceptibility of digital signatures to fraud in the National Electronic Conveyancing System: an analysis' (2009) 17 Australian Property Law Journal 303 incorrectly comments, at 307, that 'When the recipient receives the coded summary and the certificate, the recipient can use the CA's public key to verify the CA's signature on the certificate. If that is successful, the recipient can have confidence that the sender's public key is what it purports to be, that is, the sender's public key actually did come from the sender'; Raymond Wacks, *Privacy: A Very Short Introduction* (Oxford University Press 2010) incorrectly states at 25–26 that 'The advantage of a public key system is that if you are able to decrypt the message, you know that it could only have been created by the sender'; Michael Bromby, 'Identification, trust and privacy: how biometrics can aid certification of digital signatures' (2010) 24 International Review of Law, Computers & Technology 133 incorrectly states at 135: 'Parties involved in such an electronic communication cannot deny their involvement subsequently'; Arne Tauber, Peter Kustor and Bernhard Karning, 'Cross-border certified electronic mailing: a European perspective' (2013) 29 Computer Law & Security Review 28, in which the authors fail to indicate the issues relating to 'non-repudiation'.
2 Schmeh, *Cryptography and Public Key Infrastructure*, 16.1.1.

7.287 Francisco Jordan-Fernádez and Jordi Buch i Tarrats assert:

> The most important benefit electronic signatures brings to e-commerce and all electronic transactional systems is that they cannot be repudiated. This service provides evidentiary value that proves that the data has been created by a specific entity and has not been altered since the date of its creation, thereby guaranteeing its irrefutability.[1]

1 'Electronic signature today: a manufacturer's viewpoint' (2004) 5 Upgrade 23, 24. See also an early paper by Roger Clarke, 'Conventional public key infrastructure: an artefact ill-fitted to the needs of the information society', prepared for submission to the 'IS in the Information Society' track of the European Conference on Information Systems (ECIS 2001), Bled, Slovenia, 27–29 June 2001, http://www.rogerclarke.com/II/PKIMisFit.html.

7.288 Professor Sorge states:

> The private key, which is to be kept secret, is used by the signatory to sign messages; signatures can be verified with the corresponding public key. Successful verification of a digital signature guarantees integrity and authenticity of the corresponding message. Non-repudiation is also achieved, i.e. it can be proven that the message was signed by the signatory.[1]

1 Christoph Sorge, 'The legal classification of identity-based signatures' (2014) 30 Computer Law & Security Review 126, 126.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.289 None of these statements is correct.

7.290 When engineers use the term non-repudiation in an engineering sense, they mean that there is a degree of probability or certainty that the protocol can demonstrate that one item of software communicated with another item of software, or to put it another way, 'Nonrepudiation provides proof of the integrity and origin of data that can be verified by a third party'.[1] Many technicians assert that non-repudiation is a fact: that is, once the software proves that a message or document was sent and received, it follows that a human being caused the message to be sent. Such an assertion is not logical and is misleading. This reasoning is often extended from the engineering domain into the legal domain, by asserting that if the system can demonstrate that one item of software communicated with another item of software, that is, that digital data comprising a message or document was sent or received, it is for the purported sender to demonstrate that they caused it to be sent – or to prove they did not cause it to be sent. The purpose of the concept is to bind users to specific actions in such a way that if they deny taking the action, they either demonstrate an intention to deceive, or they have been negligent in failing to secure the use of their private key adequately. The use of the term is inherently misleading. The logic is as follows:

> It is proven that certain items of software communicated, each with the other. (A message was sent from Alice's computer to Bob's computer, and Alice's private key was affixed to the communication.)
>
> It follows that the purported sender caused the software to communicate. (Ergo, Alice affixed the private key to the message.)

1 United States General Accounting Office, Report to the Chairman, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, 'Information security: advances and remaining challenges to adoption of public key infrastructure technology', GAO-01-277, 2001, 18.

7.291 The purpose of the term non-repudiation is to provide for causation, which it cannot. It is generally assumed that non-repudiation has a legal effect: that is, a person cannot deny causing the software to send a message or document. However, a signature can be challenged for a number of reasons. The most pertinent is where the purported sender claims that they did not cause the electronic signature to be affixed to the message or document, as in the case of Dara O'Reilly, whose digital signature was used on two occasions in India in a complex property transaction. He denied using the digital signature.[1] In effect, there is a claim that the signature is a forgery. In such circumstances, the fact that a message or document was sent might not be at issue. The dispute often turns on whether the sender caused the signature to be affixed to the message or document.[2] In such instances, it is for the party relying on the signature to prove the message or document was sent, and that the purported sender caused their electronic signature to be affixed.

1 Dearbhail McDonald, 'Sean Quinn aide at centre of mystery over $90m asset', *Irish Independent*, 23 August 2012, http://www.independent.ie/business/irish/sean-quinn-aide-at-centre-of-mystery-over-90m-asset-26889961.html.

2 For the cases where private keys were used without the authority or authorization of the person to whom the private key was linked, see the banking cases from the Russian Federation: Olga I. Kudryavtseva, 'Russia', in Stephen Mason (ed), *International Electronic Evidence* (British Institute of International and Comparative Law 2008); Olga I. Kudryavtseva, 'The use of electronic digital signatures in banking relationships in the Russian Federation' (2008) 5 Digital Evidence and Electronic

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Signature Law Review 51; Resolution of the Federal Arbitration Court of Moscow Region of 5 November 2003 N КГ-А 40/8531-03-П(2008) 5 Digital Evidence and Electronic Signature Law Review 149; Alex Dolzhich, 'Digital evidence and e-signature in the Russian Federation: a change in trend' (2009) 6 Digital Evidence and Electronic Signature Law Review 181.

7.292 Other examples where the signature may be in dispute are where the sender accepts the message or document was sent with an electronic signature, but the signature was obtained as a result of unconscionable conduct by a party to a transaction, fraud instigated by a third party or undue influence exerted by a third party, among other reasons recognized in law. It will be for the adjudicator to determine whether a particular argument is credible. That the sender caused the signature to be affixed to a message or document may not be in issue.

7.293 It is important to ensure that the technical meaning of non-repudiation does not override the need to restrain the meaning within a legal context. Where engineers use the term, it should not be understood that they are using it in a legal context, despite a general misunderstanding in the view of some engineers that the term should have a legal meaning. Even where the evidence demonstrates that a message or document was sent or received with an electronic signature affixed, it does not follow that the message was sent by the person whose username or password (or both username and password) was used at the material time, nor that it was signed by them. Carl Ellison of Intel Laboratories in his paper 'Improvements on conventional PKI wisdom' has dismissed these arguments by technicians about non-repudiation.[1] The comments in paragraph 3.4.3 entitled 'Not Achievable' demonstrate the vacuity of the link between evidence that software has communicated with software, and the assertion that such evidence is therefore proof that a particular person caused a machine to undertake a particular action:

> The main problem with the theory of non-repudiation is that it is not technically achievable. That is, the intention is to bind a human being to a digitally signed document. With a holographic signature on a paper document, the human's hand came in contact with the paper of the document. With a digital signature there is machinery between the human and the signed document: at least a keyboard, software (to display the document and to drive the signature process) and a key storage and use facility (e.g., a smart card).
>
> No one has demonstrated, in the normal computer for home or office use, the prevention of introduction of hostile software. To the contrary, we have seen a steady increase in such incursions over the years.
>
> There are secure facilities for key storage and use, but no mechanism that an average home or small business user would choose to buy has been proved secure.
>
> Meanwhile, computers are not restricted to isolated rooms with card access entry, raised floors, guards outside the glass walls, etc., that they might have been in the 1970s when much of this thinking about public key cryptography had its nascence. Computers are not only everywhere; they are unprotected to a continually increasing degree. Therefore, even if the computer has no hostile software and its private key is kept in a truly secure facility, access to the keyboard of that computer is not limited to the person certified to be associated with that private key.
>
> What might make this process of non-repudiation work would be hardware that would serve as a witness to a signature, providing tamper-proof evidence of

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> the actions of a human being (e.g., through videotape), of what that human was reading and of the human's positive action to assent to the displayed document. Such a log of human behavior could then be presented in court to prove the claim of non-repudiation.
>
> Of course, if such hardware were available, then we would not need digital signatures, much less the assumption of non-repudiation on digital signatures.

1 First Annual PKI Research Workshop – April 2002, https://users.ece.cmu.edu/~adrian/731-sp04/readings/ellison-PKI-wisdom.pdf.

7.294 This point is also considered in a slightly different way by Niels Ferguson, Bruce Schneier and Tadayoshi Kohno:

> In theory, a PKI should provide you with nonrepudiation. Once Alice has signed a message with her key, she should not be able to later deny that she signed the message. A key server system can never provide this; the central server has access to the same key that Alice uses and can therefore forge an arbitrary message to make it look as if Alice sent it. In real life, nonrepudiation doesn't work because people cannot store their secret keys sufficiently well. If Alice wants to deny that she signed a message, she is simply going to claim that a virus infected her machine and stole her private key. [1]

1 Ferguson and others, *Cryptography Engineering*, 19.9, bullet point 3.

7.295 In 2000, Carl Ellison and Bruce Schneier wrote on the same topic:

> Alice's digital signature does not prove that Alice signed the message, only that her private key did. When writing about non-repudiation, cryptographic theorists often ignore a messy detail that lies between Alice and her key: her computer. If her computer were appropriately infected, the malicious code could use her key to sign documents without her knowledge or permission. Even if she needed to give explicit approval for each signature (for example, via a fingerprint scanner), the malicious code could wait until she approved a signature and sign its own message instead of hers. If the private key is not in tamper-resistant hardware, the malicious code can steal the key as soon as it's used.
>
> While it's legitimate to ignore such details in cryptographic research literature, it is just plain wrong to assume that real computer systems implement the theoretical ideal. Our computers may contain viruses. They may be accessible to passers-by who could plant malicious code or manually sign messages with our keys. Should we then need to deny some signature, we would have the burden of proving the negative – that we didn't make the signature in question against the presumption that we did. [1]

1 Carl Ellison and Bruce Schneier, 'Risks of PKI: e-commerce' (2000) 43 Communications of the ACM 152.

7.296 Where the party whose private key is used denies they caused the private key to be affixed to the data, it is for the party relying on the signature to prove the signing party caused the private key to sign the data. The burden of proof will depend on the pleadings and what presumptions, if any, apply.

7.297 The term 'cryptographic non-repudiation' means being able to prove that where a digital signature verifies a public key, then the associated private key made that signature: it does not prove that the person whose private key is used caused the

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

private key to make the signature.[1] However, non-repudiation is of no benefit without a secure time-stamping service to demonstrate that a particular event occurred at a given time and date, or that a specific item of data existed before a specific date. This technical meaning of the term has begun to be used in a legal sense by vendors of the public key infrastructure, which in turn has tended to confuse legislators.[2]

1 Adams and Lloyd, *Understanding PKI Concepts*, 32–33, 51–53; Dr Catharina Candolin, a Policy advisor at NATO HQ (Emerging Security Challenges Division/Cyber Defence), demonstrated confusion in her PhD dissertation, 'Securing military decision making in a network-centric environment' (TKK Dissertations 20 Helsinki University of Technology, 20 December 2005), where, at 59 and 104, it is stated that the sender cannot deny having sent the packet, and at 77, the technical meaning of non-repudiation is correctly indicated: 'that is, a malicious node cannot deny having created the IP packets.'
2 Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World* (Wiley 2000), 235, and Adrian McCullagh and William Caelli, 'Non-repudiation in the digital environment', https://firstmonday.org/ojs/index.php/fm/article/view/778/687.

Certifying certificates

7.298 Regardless of the technical meaning of the term 'non-repudiation', there are a number of problems that affect the reliability of systems that are used to affix digital signatures to an electronic communication:

> (1) A confusing design on the screen, which can lead a user to activate the signing function without knowing the significance others attach to the signature.
>
> (2) The software application may be set up to send a receipt, but this does not necessarily indicate to the recipient that the sender sent the receipt. This also raises the question as to whether the receipt is authentic.
>
> (3) A design flaw in the public key infrastructure.
>
> (4) The open nature of the Internet, which means hackers could insert malicious software into computers that can be designed to steal private keys or replay the keystrokes of the user, thereby obtaining the passwords used to obtain access to a private key.

7.299 The general rule with respect to signed documents is this: a person is normally bound by their signature to a document, even if they fail to read and understand the content. Where a party relies on a signed document and wishes to enforce it against the signing party, the relying party must prove the signature is that of the signing party, or that the signing party authorized the document. This is so where the signing party claims they did not sign the document, or if they did sign the document, that they did so under duress or because of the fraud of a third party. It is not for the signing party to prove that they did not authorize the document or sign it.

7.300 A person has a defence where they have been misled into signing a document that is essentially different to that which they intended to sign, a state of affairs that has usually, but not always, been induced by a fraud perpetrated upon the party signing the document.[1] However, this does not mean that a person should fail to exercise care when they affix their signature to a document in the absence of a fundamental mistake as to the content of the document. This occurred in *Saunders v Anglia Building Society*,[2] where Mrs Gallie signed what she understood was a deed of gift of her house to her nephew, but it was, in fact, a deed of assignment to a third party. Mrs Gallie raised the defence that she thought the effect of the document was to give her house to her nephew, but in fact it assigned her rights to a fraudulent third party. The members

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

of the House of Lords agreed that the identity of the person to whom the house was assigned did not make the deed totally different in character to the document Mrs Gallie intended to sign, and her defence failed. Lord Hodson offered the following observations at 1019(E) respecting the use of a signature:

> Want of care on the part of the person who signs a document which he afterwards seeks to disown is relevant. The burden of proving non est factum is on the party disowning his signature; this includes proof that he or she took care. There is no burden on the opposite party to prove want of care. The word 'negligence' in this connection does not involve the proposition that want of care is irrelevant unless there can be found a specific duty to the opposite party to take care.

1 In *United Dominions Trust Ltd v Western* [1976] QB 513, [1976] 2 WLR 64, [1975] 3 All ER 1017, [1975] 10 WLUK 88, (1975) 119 SJ 792, Times, 28 October 1975, [1976] CLY 339 a party signed a blank hire-purchase proposal form, and the dealer inserted incorrect figures before sending it to the finance company.
2 [1971] AC 1004, [1970] 3 WLR 1078, [1970] 3 All ER 961, [1970] 11 WLUK 45, (1971) 22 P & CR 300, (1970) 114 SJ 885, Times, 10 November 1970, [1971] CLY 1805.

7.301 In his judgment, Viscount Dilhorne agreed with the comments made by Lord Hodson, and commented, at 1023(E):

> In every case the person who signs the document must exercise reasonable care, and what amounts to reasonable care will depend on the circumstances of the case and the nature of the document which it is thought is being signed. It is reasonable to expect that more care should be exercised if the document is thought to be of an important character than if it is not.

The burden of proof

7.302 A person has total control over the use of their manuscript signature, and the legal rules that apply to manuscript signatures reflect this physical reality. However, once the accepted form of the signature changes, it may be considered appropriate, depending on the nature of the transaction, for the legal rules that apply to the new form of signature to reflect the different range of risks associated with the new manifestation of signature. Consider the example of Charles Goodman, the solicitor who used a rubber stamp to sign a letter that accompanied his bill of costs.[1] Although the control of the rubber stamp was not the subject of judicial comment, Evershed MR noted at 554, that Mr Goodman 'kept the stamp locked up in his own room so as to be available only for his own use'. Although neither Mr Goodman's actions nor the comment by Evershed MR make an explicit point about taking reasonable care of the rubber stamp, nevertheless the implication that the rubber stamp should be kept safe is obvious. It is clear that Mr Goodman took reasonable care to ensure only he had access to the rubber stamp, and the observation by Evershed MR implied that this made the use of the rubber stamp acceptable as a method of authenticating documents. If Evershed MR had considered the matter further, he might have reached the conclusion that there is a reasonable expectation in circumstances where a person decides to use a rubber stamp as a form of signature that they can be expected, as a rule of law, to provide for the security of the use of the signature, and to take appropriate steps to guard against its use by unauthorized persons.

1 *Goodman v J Eban Limited* [1954] 1 QB 550, [1954] 2 WLR 581, [1954] 1 All ER 763, [1954] 3 WLUK 22, (1954) 98 SJ 214, [1954] CLY 3173.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

7.303 Williams J discussed this point in the case of *Robb v The Pennsylvania Co. for Insurance on Lives and Granting Annuities*,[1] discussed below. The matter of the security of a rubber stamp was also mentioned briefly in *British Estate Investment Society Ltd v Jackson (H M Inspector of Taxes)*,[2] where an Additional Commissioner regularly used a rubber stamp to sign significant volumes of documents. In his judgment, Danckwerts J mentioned the measures taken in the office to provide for the prevention of unauthorized use of the rubber stamp.[3] Once again, there is no explicit mention of the need for a signing party to provide for the security of the rubber stamp and to protect it against misuse. However, the action of the signing party in providing for the security of the rubber stamp suggests that, even without a rule of law requiring them to take steps to secure the rubber stamp, they took such precautions because the nature of the instrument thus created permits others to use a recognized means of identifying and authenticating a document:

> (1) The evidence from Charles Goodman in *Goodman v J Eban Limited* and of the Additional Commissioner in *British Estate Investment Society Ltd v Jackson (H M Inspector of Taxes)* demonstrates that when the signing party acquired a rubber stamp as a means of affixing their signature to a document, they took appropriate precautions to safeguard it from misuse and theft.
>
> (2) The comments by Evershed MR[4] and Danckwerts J[5] imply that the authorized use of the rubber stamp rested on the care the signing party took of the item, and because the security of the rubber stamp was assured, the signature affixed to the document by the rubber stamp was authentic and therefore valid.
>
> (3) In the event the recipient doubts the authenticity of the signature, they can undertake their own form of due diligence to verify its authenticity and validity. This point was made by Romer LJ at 564 in *Goodman v J Eban Limited*, where he pointed out that 'If in fact his clients entertained any doubt as to the authenticity of the letter, nothing could be easier than to ask him, by telephone or letter, to confirm it'. While the point made by Romer LJ is an explicit instruction as to what action the recipient could take, the comment was not necessarily meant to form a legal rule.

1 40 W.N.C. 129, 3 Pa.Super. 254, 1897 WL 3989 (Pa.Super. 1897), affirmed by186 Pa. 456, 40 A. 969, for dissenting opinion, see 186 Pa. 456, 41 A. 49.
2 (1954–1958) 37 Tax Cas 79, [1956] TR 397, 35 ATC 413, 50 R & IT 33.
3 (1954–1958) 37 Tax Cas 79 at 87.
4 *Goodman v J Eban Limited* [1954] 1 QB 550 at 554.
5 *British Estate Investment Society Ltd v Jackson (H M Inspector of Taxes)* (1954–1958) 37 Tax Cas 79 at 87.

7.304 Although none of the comments made by the judges in these two cases are sufficient to form a rule of law in relation to such matters, nevertheless they recognized that where technology is used to provide a substitute for so physical an act as the affixing of a manuscript signature to a document, new considerations relating to the presumptions that should apply to alternative methods of applying a signature must be considered.

7.305 In light of the decision of Waller J in *Standard Bank London Ltd v Bank of Tokyo Ltd*,[1] it appears that this train of thought may have already been adopted in England and Wales. In this case, the Bank of Tokyo in Kuala Lumpur arranged for three tested telexes to be sent to Standard, containing a secret code confirming and authenticating the authorized signatory of three letters of credit with a total face value

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

of US$19.8 million, and confirming that the Bank of Tokyo accepted all responsibilities and liabilities under those letters of credit. Evidence was adduced to indicate that banks not only used this system with confidence, but also used it to avoid arguments about authority. In this instance, the tested telexes were sent fraudulently.

1 [1995] 2 Lloyd's Rep 169, [1995] 3 WLUK 182, [1995] CLC 496, [1998] Mason's CLR Rep 126, Times, 15 April 1995, [1995] CLY 397.

7.306 The main thrust of the Bank of Tokyo's case was this: because they could establish that a thief must have been working in their tested telex department, Standard could only rely upon the apparent authority of the tested telexes. As a result, it argued that there was a lower test to establish the lack of apparent authority. Waller J disagreed with this argument at 502C, because the issue was not reliance on apparent authority:

> Standard rely first on a general representation by BOT that if a telex comes by tested telex that telex will be duly authorised by BOT (that representation on any view is authorised);
>
> second they rely on the use of the tested telex mechanism itself as representing that the telex is authorised as the previous representation stated that it would be; and
>
> thirdly they rely on the statement in the telex as being the authorised statement of BOT.

7.307 The Bank of Tokyo was found liable for negligent misrepresentation because the tested telexes could not have been sent without negligence on the bank's part. Whether Standard had a duty to inquire into the authenticity of the tested telexes depended on the circumstances of each case.[1] Tested telexes contain codes or tests which are secret between the sender and the recipient. This allows the recipient to accept without question that the telex was sent by and with the authority of the sender. The tested telexes in this instance were sent through other banks, because the Bank of Tokyo in Kuala Lumpur did not have a means of directly authenticating telexes between itself and Standard. By sending tested telexes, banks intend the receiving bank to act on the content without further instructions. This means the receiving bank requires the sending bank to confirm the person signing the document is an authorized signatory, verify the signatory is authorized to sign the particular document, and provide sufficient evidence to satisfy the recipient that the sending bank authorized the sending of the telex.

1 [1995] CLC 496 at 501H.

7.308 Superficially, there is a similarity between the circumstances of this case and the public key infrastructure, where the authentication process has to go through so many channels.[1] However, there is a distinction between a tested telex produced in a bank and the public key infrastructure. The authority of a telex is reliant upon internal systems within the bank.[2] No third party is involved in identifying the sender of the telex or authenticating the codes or text sent. In addition, the tested telex is sent through other banks over apparently secure lines of communication. Conversely, the public key infrastructure operates over the Internet, which was designed to be open and is, therefore, insecure. The link between the identity and authentication of a user of an electronic signature is not as cohesive as that between such trusted parties as

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

banks. There are significantly more links, which neither party has control over, in the chain between the sending party and receiving party of an electronic signature. As a result, it can be argued that there is a distinction between what can be termed a 'secure or closed communication system' and an 'open communications system'. Clearly the burden of proving that an electronic signature was used without authority must be borne by either the user or the relying party. In this instance, Waller J took the view that the sender was in full control of the environment in which the tested telex was sent, and decided that the burden should fall on the sender.

1 See also Jean-François Blanchette, *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents* (MIT Press 2012) – 'This book is not about the burden of proof or the law relating to electronic evidence. The reader must look to legal text books on electronic evidence to understand burdens of proof and the law relating to electronic evidence. However, it is a useful text in discussing the technical issues and policy decisions behind the use of technology that has an effect on electronic evidence.' Book Report, (2012) 9 Digital Evidence and Electronic Signature Law Review 181; for a similar broad introduction by the same author, see 'The digital signature dilemma', Annales des Télécommunications (May/June 2006), 908.

2 A message using an authentication code sent through the SWIFT system has the legal effect of binding the sender bank according to its contents: *Industrial & Commercial Bank Ltd v Banco Ambrosiano Veneto SpA* [2003] 1 SLR 221.

7.309 In the context of an open insecure network, however, different criteria, based upon the protection of the consumer, might be applied by the courts.

The recipient's procedural and due diligence burden

7.310 Whether it is for the user of an electronic signature to bear such a burden is debatable. If it is accepted that the recipient is required to establish whether they can rely on the certificate in all the circumstances, they may be required to provide any or all of the evidence discussed above in relation to verifying the integrity of a certificate, depending on the nature of the challenge. Providing the recipient has carried out all the relevant checks required, it is possible to argue that it has discharged what can be described as a procedural and due diligence burden and has become a verifying party.

The sending party: the burden of proof of security and integrity

7.311 Once the recipient, if required so to do, has satisfied a judge that it has discharged the procedural and due diligence burden, the user will need to address the issue of the security and integrity of their computer or system, among other topics of relevance in the circumstances. This can be described as the burden of proof of security and integrity, which comprises both a persuasive burden (or burden of proof on the pleadings) and the evidential burden of adducing evidence. In discussing this aspect, it is useful to compare identical problems that have exercised the minds of people in the past, and what mechanisms were put in place to provide for the integrity of the method of proving intent.

7.312 The use of a seal became so common by the fourteenth century in England that consideration had to be given to provide for additional evidence, other than the impression of a seal affixed to the document, that the seal impression was not a forgery or added without authority. The sovereign might have a number of seals for different purposes: a signet for the secretary; a privy seal, which was in between the secretary

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

and the Chancellor; the great seal, controlled by the Chancellor to authenticate the most formal of acts; and a finger ring, later called a privy signet, for the personal affairs of the monarch.[1] Care was taken to destroy seal matrices in a public ceremony, as occurred when Edward III ascended the throne and had the great seal used by his father and grandfather broken into tiny pieces in his presence.[2] However, the physical object of the impression of a seal can be undermined, just as any other form of authentication. For instance, the seal itself might be forged,[3] or the seal of a dead person used, as in the case of Hannibal when he forged letters in the name of the dead Roman consul Marcellus after removing the signet ring from his body.[4] In England, it was an offence to forge the royal seal. By the Statute of Edward III, counterfeiting the great and privy seals were treasonable offences, and one man who forged the seal of Henry II was only saved from being hanged by the king's mercy.[5] At common law it was a felony and regarded as a capital offence, and there are three medieval cases of this nature.

1 Patricia M. Barnes and L. C. Hector, *Guide to Seals in the Public Record Office* (2nd edn, HMSO 1968), 8; P. Chaplais, *English Diplomatic Practice in the Middle Ages* (Hambledon and London 2003), 97–98.
2 P. D. A. Harvey and Andrew McGuinness, *A Guide to British Medieval Seals* (University of Toronto Press 1996), 34.
3 T. F. Tout, 'Mediæval forgers and forgeries' (1919) Bulletin of the John Rylands Library 208 describes how a medieval forger might be clever enough to cut the wax or lead of a seal into two thin slices, introduce a new attachment of parchment, silk or leather, and affix it to a new document, then heat the sides to fasten the seal together for a second time.
4 Chaplais, *English Diplomatic Practice*, 6.
5 Harvey and McGuinness, *A Guide to British Medieval Seals*, 33, 98–99.

7.313 A person could challenge a document where the incorrect seal had been used, or the right seal was attached to the wrong document. As seals became more common, the other issue was the degree of forgery for ordinary seals.[1] There is evidence illustrating that people took their seal very seriously. In 1190, for instance, Adam, son of Peter de Birkin, broke his seal and replaced it. He went to the length of repeating a grant he had previously made to the abbey of Rievaulx.[2] There then developed a means of countersigning the main seal with the use of a secret seal as a counter-seal to one of the great seals. The great seal would be in the possession and under the control of the officer of state, and the secret seal in the possession of the owner, thus providing a double-check to the authenticity of the document, because the second seal may be imprinted on to the great seal, providing two seal impressions on the same seal. The concerns for the security of the seal were sometimes carried to what seems like extraordinary lengths, but were probably routine. In 1214 the chapter seal of Salisbury cathedral was in the care of two cannons, but by 1353 it was kept in a chest with three locks, and was only used in the presence of all three cannons, each of whom held a key. By the Statute of Acton Burnell in 1283, debts could be registered before the mayor, who issued a recognisance with a special seal supplied by the crown. However, in 1285 the Statute of Merchants amended the previous statute and ordered that the seal must be contained in two parts, the larger to be retained by the mayor and the smaller to be retained by the clerk – indicating, in the opinion of one scholar, that there had probably been a scandal.[3] In the late thirteenth century, the seal of the corporation of Winchester was placed in a box with three locks and the keys retained by two counsellors and one ordinary person, and this box in turn was itself kept in a chest with two keys, held by one counsellor and one other person.[4]

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

1 For an example of a Chinese seal in the context of documentary letters of credit, see *Deutsche Bank AG, London Branch v CIMB Bank Berhad* [2017] EWHC 3380 (Comm), [2018] 2 Lloyd's Rep 510, [2017] 12 WLUK 407, [2019] CLY 631.
2 Barnes and Hector, *Guide to Seals in the Public Record Office*, 29–30.
3 T. F. T. Plucknett, *Legislation of Edward I* (Clarendon 1949), 140, quoted in Harvey and McGuinness, *A Guide to British medieval Seals*, 111.
4 Harvey and McGuinness, *A Guide to British Medieval Seals*, 58–62, 98–99.

7.314 Conceptually, there is little difference between the seal matrix and a rubber stamp, and the nature of the security in place to prevent unauthorized use is identical. In this respect, the 1897 Pennsylvania case of *Robb v The Pennsylvania Co. for Insurance on Lives and Granting Annuities*[1] is highly instructive. This case predates the use of electronic signatures in any form by 100 years, yet the difference in time does not diminish the issues, even if they were articulated with different concepts and language by the judges at the time. In this case, money had been paid out on two cheques signed with the facsimile signature of the bank depositor by means of a rubber stamp. Mr Robb did not authorize either cheque.

1 40 W.N.C. 129, 3 Pa.Super. 254, 1897 WL 3989 (Pa.Super. 1897), affirmed by 186 Pa. 456, 40 A. 969; for a dissenting opinion, see 186 Pa. 456, 41 A. 49.

7.315 In 1893 Mr Robb, as the president of a commercial corporation, had occasion to send out a large number of invitations to a banquet. To save himself the trouble of signing each invitation, he had a rubber stamp made with a facsimile of his signature. After retiring, he rented a private office, and with the rent came the services of an office boy. He employed the boy on various errands, including sending him to the bank to draw money on cheques. It can be inferred from the report that he used the rubber stamp to sign cheques. He kept the rubber stamp in a compartment inside a fireproof safe. He locked the compartment and put the key to the compartment in a drawer in the safe, behind some papers, and covered it up. He then locked the drawer, and placed the key into an unlocked drawer in the safe. He then locked the safe, and put the key in a little box, which he put in a wooden drawer or box, and this was kept on top of another safe. The plaintiff surmised that the office boy had watched his moves at some time in the past. The majority of the judges found that Mr Robb was not negligent in the use of the rubber stamp. The basis of their decision centred on whether he was negligent in failing to exercise care in preventing the rubber stamp from falling into the wrong hands. Rice PJ rejected the proposition that Mr Robb was bound to keep the stamp in a place that prevented any person from obtaining it without authority. However, no attempt was made by the majority judges to explain how the bank was in a position to challenge the signature, given that the signature was identical each time the rubber stamp was used, with the exception that the impression will vary in quality depending on the amount of ink used and the pressure applied to the stamp as the signature is affixed to the cheque. The majority held that the bank was liable for the cheques. Williams J wrote an elegant dissenting judgment that raises the modern issues, using different language, but germane nevertheless, with which Sterrett CJ concurred. Williams J argued that it was for the bank, relying on the signature, to prove it was genuine. The image of the signature was genuine, but Mr Robb had neither applied it nor authorized the signature to be applied to the cheque. In this respect, it was a forgery, and in the words of Wills J in *The Staple of England v The Governor and Company of the Bank of England*:

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> A forgery can give no title, and those that rely upon it must be able to shew some extraneous ground – such as that of estoppel – why they should be entitled to act upon it.[1]

1 (1887) 21 QBD 160 at 166.

7.316 In *The Staple of England*, the bank was held liable for failing to make proper enquiries as to title where the company gave the safekeeping of the Company seal to their clerk (a solicitor), and the clerk, without authority, affixed the seal to a power of attorney that enabled him to sell funds of the Company for his own benefit. The seal and the rubber stamp have the same problem: the need to prevent unauthorized use. Although the use of rubber stamps was not new at the time of this case, nevertheless Mr Robb failed to notify the bank that he was using a mechanical reproduction of his manuscript signature. Arguably, if the bank had been made aware of this practice, as suggested by Williams J, it might have refused to honour such cheques, or if it accepted them, the bank might have taken additional care to ensure with each cheque that he had affixed the signature with the intention of signing it.

7.317 There is a difference of degree between securing a physical object such as a rubber stamp and a digital signature, but in the event of a dispute, it follows that it is the holder of the certificate and private key who is in the best position to prove that the security in place was adequate, such that the certificate and private key could not be used improperly.

7.318 If the user wishes to argue their security was so poor that an unauthorized third party could have gained access to the system to send an electronic communication with an electronic signature attached without authority, the user will undoubtedly be admitting breach of contract with the vendor from whom they obtained the certifying certificate. They are also probably admitting they were negligent. This is the central conundrum any user of a digital signature faces.

7.319 The flexible nature of the need to implement suitable precautions relating to securing a seal was recognized by Wills J, and in a prescient comment in *The Staple of England*, he indicated at 168 that:

> The precautions which appear to be natural in one century may appear pedantic and unnecessary in another … there can be no inflexible and unvarying rule of law as to that which is essentially a mixed question of fact and law.

Burden of proof – the jitsuin

7.320 Since the eighth century, a similar system of authentication to that of the electronic signature has existed in the physical world, by which a signing party deposits an imprint of their mark with a trusted third party, and relying parties can rest assured that when the mark is used, they can rely on the authentication of the person by the mark. This is the *jitsuin* (original seal) of Japan. Other seals include the *ginko-in* (bank seal) for banking purposes, and *mitome-in* (approval seal) for use in everyday circumstances, such as signing for a delivery of post. The seal is called an *insho*, and the word *inkan* describes the impression of the seal. The purpose of a name seal is to confirm a person's intention to enter a transaction and to act as a form of identification. The use of *mitome-in* in Japan is so much part of everyday life that foreigners, although

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

they are permitted in some situations to use a manuscript signature instead of a name seal, are advised to obtain such a seal if they are going to remain in the country for any length of time.[1]

1 For a further explanation, see G. P. McAlinn (ed), *Japanese Business Law* (Wolters Kluwer 2007), 202–204.

7.321 *Jitsuin* are used instead of manuscript signatures to execute important documents. For instance, the Jitsuin Seal Registration Certificate is required as an attachment to the document of application for the transfer of registration in the real property registry at the Legal Affairs Bureau. The importance attached to the Jitsuin Seal Registration Certificate under Japanese Law is such that the transfer of the registration is essential for the perfection of the transfer of title of a real property. The *jitsuin* is endowed with a legal presumption that is founded partly on the common understanding that a name seal either cannot be forged, or is difficult to forge, and partly on a very long history of use.

Registering a jitsuin

7.322 *Jitsuin* are required to conform to specific criteria:

> (1) The name on the seal must conform to the registered name; the seal must have a border surrounding the name (and the border must not be missing or chipped); machine-made, mass-produced seals are not acceptable; the seal must be made of a material that cannot be altered easily, and the diameter must be greater than 8 mm square but smaller than 25 mm square.
>
> (2) Only the owner of a seal or a representative can apply to register a *jitsuin*, and the applicant has to be over the age of 15 years.
>
> (3) A *jitsuin* must be registered at the offices of the local government, whether village, town or city.

7.323 Upon application for a registered seal (*jitsuin*) and Seal Registration Certificate (*inkan toroku shomeisho*), some local offices will send the applicant a letter of verification for the purpose of confirming the identity of the person applying. Alternatively, the usual range of documents will be required to be produced when the applicant attends the office. The registration takes place when the applicant attends the office with their seal, during which their identity is checked. Where a representative registers the seal, they will be required to provide a Letter of Attorney or a Letter of Advice Giving Right of Representation, which must be signed and sealed by the owner of the seal. After registering the seal, the applicant is given a Seal Registration Card (*inkan torokusho*, a plastic card) rather than a Seal Registration Certificate.

The Seal Registration Certificate

7.324 The Seal Registration Certificate includes the following information: an impression of the registered seal; the name of the seal holder; the date of birth of the seal holder; the gender of the seal holder; the address of the seal holder. The registration of the *jitsuin* is tied to a particular geographical locality, so if the seal holder moves to another part of Japan or leaves Japan for good, the seal registration becomes null and void, and a new registration process must be undertaken at the new location. Where a *jitsuin* is lost, the process is to attend the office that issued the Seal Registration

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

Certificate and initiate the procedure to delete the registration. There is no procedure to notify relying parties that the *jitsuin* has been stolen or lost.

The legal presumption of the Seal Registration Certificate

7.325 A Seal Registration Certificate proves the seal holder has adopted the impression of the seal that is recorded in the Certificate. The Civil Procedure Law provides for a legal presumption relating to the authenticity of a private document, as follows: 'A private document shall be presumed to be authentically executed if it bears the signature or seal of the principal or his representative.'[1] It appears that this presumption is rebuttable and the following discussion is restricted to private documents, and does not include government documents.[2] For this presumption to operate, the party bearing the burden of proof is required to prove that the registered owner of the seal intended to affix an impression of their seal on the document. This intention may itself be presumed if the relying party proves that the seal impressed on the document and the impression of the adopted seal held by the owner is the same. However, the relying party must also prove that the signing party has in fact adopted the seal. This fact is proved by using the Seal Registration Certificate, because the Seal Registration Certificate bears the adopted seal and the name of the signing party, thus it is easy for the relying party to prove that the signing party adopted the seal.[3] Once it is established that the signing party intended to affix an impression of their seal by operation of this presumption, the presumption under the Civil Procedure Law takes effect, and the document in question is presumed to be authentically executed.

1 Civil Procedure Law (Law No 109 of 1998) article 228(4).
2 Civil Procedure Law (Law No 109 of 1998) article 228, 228(2) and 228(3).
3 This chain of presumption is reinforced by the provisions of Civil Procedure Law (Law No 109 of 1998) article 229, which states: 'The authenticity of execution of documents may also be proved by a comparison of a specimen of handwriting or seal impression'.

7.326 This explanation demonstrates that there are two levels of presumption, a process known as the 'Two Phase Presumption'. It involves the following steps.

> If the impression of the seal and the adopted seal held by the signing party are the same, then it is presumed that:
>
> The signing party intended to affix the seal impression, which in turn creates the presumption that:
> The document bearing the seal impression was authentically executed.

7.327 It is to be noted that there is no statutory requirement of due diligence in order to utilize this presumption.

Rebutting the presumption

7.328 The owner of the seal can rebut these presumptions. However, it is difficult to effectively prove that the document was not authentically executed, which is tantamount to trying to prove a negative. Recently, this presumption has been found to pose problems in an age when it is very easy to forge name seals with the availability of advanced technology. This problem reached national importance following a series of thefts from deposit accounts held in banks using forged or stolen seals. The problem is partly explained by Matsushita Shuli:

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

> Door-picking artist quietly breaks and enters victim's house and nicks bank account passbook. The passbook, especially old ones, usually carries the seal image on the first page. The joker scans this image and prints it on the withdrawal slip with color printer. The bank teller accepts this slip and passbook as authentic, and victim's account will be emptied. Sometimes, the scanned digital image goes to hanko carving machine, too.
>
> The real cause of trouble: It's the stamped image of one's hanko that is stored in the databases of government offices, banks and other public institutions. Not the particulars of physical hanko itself! And any image can be flawlessly reproduced in this era of digital processing. QED.[1]

1 Obtaining information about this problem in the English language is difficult; but see Mayumi Negishi, 'Security concerns jeopardize future of age-old tradition of "hanko" seals', *The Japan Times*, undated, https://www.japantimes.co.jp/news/2004/01/14/business/security-concerns-jeopardize-future-of-age-old-tradition-of-hanko-seals/#.XrFKZhOYWSy. The most recent news item is Terrie Lloyd, 'Huge local fraud case, ebiz in Japan', 20 April 2010, Japan.Inc, https://www.japaninc.com/tt562_huge-local-fraud-case.

7.329 The *jitsuin* and the Seal Registration Certificate have been a very effective method of providing for the authenticity and intention of a person when entering into a legally binding agreement as a trusted third party undertakes to certify the nexus between the applicant and the *jitsuin*. The presumption worked well in a society where the accurate copying of name seals was difficult for the would-be thief.[1] However, with the advent of modern means of duplication, a tension has arisen between the assurance that an individual can prove their identity and thereby authenticate a document with the use of a Seal Registration Certificate in combination with a *jitsuin*, and the failure to require the relying party to take steps to authenticate the identity of the person who claims the name seal is their adopted *jitsuin*. The Seal Registration Certificate proves the seal holder has adopted the impression of the seal that is recorded in the Certificate. In modern Japan, the failure to balance the presumption that accompanies the use of a *jitsuin* with an accompanying duty to take steps to require the person using the name seal to provide the certificate of authenticity has meant ordinary consumers suffer the loss. This is an example where advances in technology have caused problems in a system of authentication that has worked well over an extended period of time in Japanese history. While a change to the law will not follow immediately, when a change does occur, a cultural shift will also have to take place, in which the relying party will have to take reasonable steps to verify the signing party.

1 Noriko Kawawa, 'The Japanese law on unauthorized on-line credit card and banking transactions: are current legal principles with respect to unauthorized transactions adequate to protect consumers against information technology crimes in contemporary society?' (2013) 10 Digital Evidence and Electronic Signature Law Review 71, for a general overview of the position in Japan.

Burden of proof – summary

7.330 In the context of electronic signatures, and digital signatures in particular, there is a clear lesson to be understood. In the physical world where the signature-creation device is difficult to replicate accurately, a tri-part method of providing assurance can be very effective. The owner of the Japanese seal provides evidence of their identity to satisfy a nominated authority sufficiently for the authority to create a certificate to link the seal to the owner. The authority retains the evidence of the link, and the relying

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

party can rest assured that the person with the seal, if authenticated with a certificate, is who they say they are. The flaw in this model, in an age when a name seal is easy to duplicate, is that it fails to impose a duty on the relying party to undertake sufficient due diligence to satisfy themselves that the holder of the seal is the person whose name seal is registered.

7.331 The use of a rubber stamp as a form of signature has similar properties to the name seal, but without the properties of the *jitsuin*. In the cases of *Goodman v J Eban Limited*[1] and *British Estate Investment Society Ltd v Jackson (H M Inspector of Taxes)*,[2] the respective recipients of the stamped documents did not question the authenticity of the stamped signature but sought to challenge the form of the signature. The underlying assumptions about the security of a rubber stamp were not fully articulated; that is, the owner of such a stamp is expected to keep it secure and prevent any unauthorized use. If the recipient was in any doubt as to the authenticity of the document signed with a rubber stamp, they could always take steps to verify the integrity of the document. While observations about security were made by the judges in passing and did not lay down a rule of law, nevertheless they represent underlying assumptions about the risks to be attached to the use of a means of providing authentication to a document which may not always be under the control of the owner, at least in cases where the means in question are adopted for the convenience and advantage of the user rather than the recipient.

1 [1954] 1 QB 550, [1954] 2 WLR 581, [1954] 1 All ER 763, [1954] 3 WLUK 22, (1954) 98 SJ 214, [1954] CLY 3173.
2 (1954–1958) 37 Tax Cas 79, [1956] TR 397, 35 ATC 413, 50 R & IT 33.

7.332 The risks for the participants when using electronic signatures is, to a certain extent, similar to that of the *jitsuin* and rubber stamp, depending on the type of electronic signature used. In the context of the digital signature, the trusted third party allocates the risks and responsibilities. In general, a subscribing party or receiving party that relies on such technology is either fully aware of the limitations associated with the use of a digital signature, or they have no concept of the issues, and they use a digital signature in ignorance of the risks they may face if their reliance were to be tested. Statute provides that where a trusted third party with a contractual relationship with its customer (a bank) debits the account of a customer with the payment of a cheque the customer did not sign, the bank has no authority to take the money and therefore must credit the account with the amount charged.[1] The allocation of risk with the *jitsuin* is under threat because of the ease by which a name seal can now be forged.

1 Bills of Exchange Act 1882 s 24; Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance) OJ L 319, 5.12.2007, 1–36, implemented by The Payment Services Regulations 2009 (SI 209/2009) as amended by The Payment Services (Amendment) Regulations 2009 (SI 2475/2009).

7.333 It was judges during the nineteenth century who created the protection for those customers who affixed their manuscript signature to a cheque and politicians codified this rule.[1] While it will be important to take into account the suggestion made by Romer LJ in *Goodman v J Eban Limited*[2] that the recipient of a document stamped

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms

with a rubber stamp can take action to authenticate the document, the action and effort required to check that the writer of a letter intended to affix their signature by means of a rubber stamp is far less than the magnitude of the task facing a recipient of, in particular, a digital signature. The terms and content of the certification practice policies of the certification authorities demonstrate the complexity of the task faced by a recipient if they are expected to verify a digital signature.

1 Nicholas Bohm, Ian Brown and Brian Gladman, 'Electronic commerce: who carries the risk of fraud?' (2000) 3 Journal of Information, Law and Technology, paragraph 2, https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm.
2 [1954] 1 QB 550 at 564.

This content downloaded from 81.218.45.221 on Mon, 08 Nov 2021 14:00:49 UTC
All use subject to https://about.jstor.org/terms