Bond University
ePublications@bond

Law Faculty Publications | Faculty of Law

7-2010

The inadequate legislative response to e-signatures

Jay Forder
Bond University, Jay_Forder@bond.edu.au

Follow this and additional works at: http://epublications.bond.edu.au/law_pubs

Part of the Computer Law Commons

Recommended Citation
Jay Forder. (2010) "The inadequate legislative response to e-signatures" *Computer law & security review,* 26 (4), 418-426.

http://epublications.bond.edu.au/law_pubs/333

This Journal Article is brought to you by the Faculty of Law at ePublications@bond. It has been accepted for inclusion in Law Faculty Publications by an authorized administrator of ePublications@bond. For more information, please contact Bond University's Repository Coordinator.

The Inadequate Legislative Response to E-Signatures

Abstract: This article examines the two most influential international initiatives on electronic signatures (UNCITRAL's 1996 *Model Law on Electronic Commerce* and the 1999 EU *Electronic Signature Directive*). It considers whether the legislative approaches in Australia and the United Kingdom based on these initiatives are helpful in deciding whether lower level signature methods such as simple email messages are likely to satisfy a legal requirement for a signature. The conclusion reached is that they are unhelpful. The article goes on to consider whether legislative amendments based on UNCITRAL's 2001 *Model Law on Electronic Signatures* or the 2005 UN *Convention on the Use of Electronic Communications in International Contracts* would improve the identified weaknesses. It concludes that such an update would clarify some issues, but that overall it will not solve the difficulties. The article ends with a brief speculation on the likely attributes of a more helpful approach.

Keywords: electronic signatures; email messages; UNCITRAL *Model Law on Electronic Commerce*; European Union *Electronic Signature Directive*; UNCITRAL *Model Law on Electronic Signatures*; UN *Convention on the Use of Electronic Communications in International Contracts*; Australian Electronic Transactions Acts; UK *Electronic Communications Act 2000*.

1. Introduction

The term 'digital signature' established itself in the late 1970s. Work was being done on methods of authenticating electronic communications over open networks. The most useful methods involved encryption techniques that facilitated proof that data messages were from the alleged sender and hadn't been tampered with *en route*. Researchers began to call their solutions 'digital signatures'.[1] While the technology was completely different from manuscript signatures, the analogy is easy to see when one considers the functions each perform. Both technologies bind a 'signatory' to a document in a way that makes later repudiation difficult.

Encryption technology is not, however, the only way a signature or the act of signing can be replicated in the electronic world. Numerous other activities arguably fulfil similar functions. Examples include scanning one's manuscript signature and inserting it in an electronic document; typing one's name at the end of an email message; clicking on an 'I agree' button on a website; using a password or personal identification number (PIN); and using a fingerprint or other biometric identifier.[2] The wider term 'electronic signature' came to be used to encompass all electronic methods of replicating signature functions. The difficult question for lawyers is whether these methods satisfy a legal requirement that something be signed.

The two most influential international initiatives in addressing this problem were the early efforts of UNCITRAL[3] and the EU.[4] Many countries passed e-signature legislation influenced by or implementing these efforts.[5] As a result, one can be reasonably confident that use of an appropriately secure and certified digital signature is likely to satisfy a legal signature requirement in most countries.[6] But, as Mason observes, 'ordinary people do not use digital signatures, which both the IT industry and politicians have attempted to enforce upon people'.[7] Are the less formal methods that 'ordinary people' use likely to be recognised as

---

1 See the seminal papers describing the development of public key cryptography: Whitfield Diffie and Martin Hellman, 'New Directions in Cryptography' (Nov 1976) Vol 22 *IEEE Transactions on Information Theory* 644; Ronald Rivest, Adi Shamir and Len Adleman, 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems' (Feb 1978) 21(2) *Communications of the ACM* 120.

2 This is an illustrative rather than an exhaustive list.

3 UNCITRAL, *Model Law on Electronic Commerce*, GA Res 51/162, GAOR 51st sess, 85th plen mtg, UN Doc A/Res/51/162 (1996) (with additional article 5bis as adopted in 1998 and Guide to Enactment).

4 *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures* [1999] OJ L13/12, 19.1.2000.

5 See, for example, the discussion of numerous electronic signature laws by Lorna Brazell, *Electronic Signatures and Identities: Law and Regulation* (2nd ed, 2008) Ch 6.

6 Ibid.

7 Stephen Mason, *Electronic Signatures in Law* (2nd ed, 2007) [2.3].

signatures? This article examines the extent to which legislative initiatives assist in answering the validity question for signature-like activity that does not involve encryption. It is not concerned with many of the traditional e-signature issues such as the regulation of certification authorities, public key infrastructures or cross-border recognition. It will describe a typical example of one of the less formal methods—an email message containing an acknowledgment of debt. The focus will be on the two international approaches and the way they have been implemented in national legislation in Australia and the United Kingdom. Australia's legislation[8] is based on UNCITRAL's 1996 *Model Law on Electronic Commerce* (the '1996 Model Law').[9] This approach is examined in the third section of this article. The UK legislation,[10] which implements the EU's 1999 Directive on Electronic Signatures (the 'EU Directive'),[11] is considered in the fourth section. Both these approaches are commendably broad and flexible. They do not prevent any of the less formal signature-like activities being recognised as valid signatures. Ironically, however, this strength is also their weakness—it will be shown that the requirements for a valid signature are so broadly stated that they offer little guidance to decision-makers.

Since the Australian and UK legislation was passed, there have been two subsequent United Nations-sponsored developments: UNCITRAL's *Model Law on Electronic Signatures* (the '2001 Model Law')[12] and the UN *Convention on the Use of Electronic Communications in International Contracts* (the '2005 Convention').[13] The fifth section of this article considers whether these developments solve the weaknesses identified. It is submitted that, while they improve the situation to a limited extent, the basic weaknesses still remain.

The article ends by reflecting on the likely attributes of a more useful legislative scheme. It is suggested that, to achieve the desired level of certainty and flexibility, it would need to combine the strengths of a number of approaches. In particular, it is suggested that work needs to be done developing a technology-neutral system of rating the relevant attributes of online signature methods.

2. A typical electronic signature issue

Consider the following scenario.[14] It raises a signature issue that could arise in most jurisdictions, but, for the reasons explained, we will focus on Australian and United Kingdom law.

In 2010 a plaintiff, Robert Brown, takes action to recover a debt from his former girlfriend, Cathy White. The debt accrued in 2002. In both Australia and the United Kingdom, relevant statutes provide that an action for recovery of a debt shall not be brought after the expiration of 6 years.[15] Mr Brown counters this by alleging that the limitation period was interrupted by an acknowledgement of the debt[16] in an email message in 2006.

Ms White argues that the email does not satisfy the requirement that an acknowledgement must be in writing and signed by the person making it.[17] The focus of this article will be the signature requirement. In passing, we might note that the issue whether an email message is 'in writing' is no longer a controversial issue, if it ever was.[18]

---

8 *Electronic Transactions Act 1999* (Cth) and the other Acts referred to in footnote 24.

9 UNCITRAL, *Model Law on Electronic Commerce*, GA Res 51/162, GAOR 51st sess, 85th plen mtg, UN Doc A/Res/51/162 (1996) (with additional article 5bis as adopted in 1998 and Guide to Enactment).

10 *Electronic Communications Act 2000* (UK) c 7 and *Electronic Signatures Regulations* 2002.

11 *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures* [1999] OJ L13/12, 19.1.2000.

12 UNCITRAL, *Model Law on Electronic Signatures*, GA Res 56/80, GAOR 56th sess, 85th plen mtg, UN Doc A/Res/56/80 (2001).

13 United Nations, *Convention on the Use of Electronic Communications in International Contracts*, GA Res 60/21, GAOR 60th sess, 53rd plen mtg, UN Doc A/Res/60/21 (2005).

14 It is loosely based on an Australian case heard in the New South Wales Supreme Court: *McGuren v Simpson* [2004] NSWSC 35.

15 In the Australian context, the provision is in State legislation such as the *Limitation of Actions Act 1974* (Qld) s 10; in the UK the relevant provision is the *Limitation Act 1980* (UK) s 5.

16 The relevant Queensland provision is the *Limitation of Actions Act 1974* (Qld) s 35(3): 'Where a right of action has accrued to recover a debt … and the person liable or accountable therefor acknowledges the claim … the right shall be deemed to have accrued on and not before the date of the acknowledgment …'. The *Limitation Act 1980* (UK) s 29(5) is to the same effect.

17 See the *Limitation of Actions Act 1974* (Qld) s 36(1); and the *Limitation Act 1980* (UK) s 30(1).

18 Like most statutes that deal with electronic signatures, the Australian legislation puts the issue of whether an email message is 'in writing' beyond doubt. It would have been equally arguable at

Imagine that the email looks like this:

> Date: Wed, 29 Sep 2006 14 16.20+1000
> To: "Bob"<Robert-Brown@yahoo.com>
> From: "Cathy White" <cwhite@bond.edu.au>
>
> … I know I owe you the $10,000 I borrowed for the car, but in view of your breaking off our relationship, I will not be paying it back any time soon (if at all).
>
> Regards, Cathy.

Two features of the message might amount to a signature: (1) the sender's email address which includes her name and appears after the word 'From'; and (2) the typed text of her first name at the end. A court would have to decide whether one or other (or both together) amounted to a signature.

3. How helpful is the UNCITRAL/Australian approach?

Australia's legislation is based on UNCITRAL's 1996 Model Law. In this section, the signature provision of the 1996 Model Law and the way Australia has implemented it will be explained. We will then consider how helpful the Australian legislation is for a decision-maker faced with the scenario outlined.

3.1 The 1996 Model law

UNCITRAL's 1996 Model Law has been particularly influential. Since it was published, eight countries or independent territories have adopted it; 27 countries (including Australia) have adopted legislation implementing its provisions; and uniform legislation influenced by its principles has been prepared in both the United States of America and Canada and enacted by 48 US States and 11 Canadian Provinces and Territories.[19]

The 1996 Model Law is well-described as 'minimalist'.[20] It goes slightly further than merely enabling electronic signatures, since it not only recognises that they may be legally valid, but also suggests some criteria for their validity. However, the criteria are broadly stated. Article 7 provides:

> (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
> a. A method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
> b. That method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.[21]

Although expressed as two paragraphs, it should be noted there are three requirements here: (1) the method must identify the person; (2) the method must indicate the person's approval of the information in the message; and (3) the method must be as reliable as appropriate.

---

common law that if a readable version could be produced (eg on screen or printer) this would satisfy the 'writing' requirement. See, for example, *Wilkens v Iowa Insurance Commissioner* (1990) 457 NW 2d 1, *Lockheed-Arabia v Owen* [1993] 3 All ER 641, and Sharon Christensen and Rouhshi Low, 'Moving the Statute of Frauds to the Digital Age' (2003) 77(7) *Australian Law Journal* 416. This was also the conclusion of the UK Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions*, Dec 2001 [3.23].

19 UNCITRAL, *Status: 1996 - UNCITRAL Model Law on Electronic Commerce*, <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html> at 10 August 2009.

20 See, for example, Australia, Report of the Electronic Commerce Expert Group to the Attorney-General, *Electronic Commerce: Building the Legal Framework* (1998) [3.2.2]; Lorna Brazell, *Electronic Signatures and Identities: Law and Regulation* (2nd ed, 2008) 157; Jay Forder and Dan Svantesson, *Internet and E-Commerce Law* (2008) 67.

21 UNCITRAL, *Model Law on Electronic Commerce*, GA Res 51/162, GAOR 51st sess, 85th plen mtg, UN Doc A/Res/51/162 (1996) (with additional article 5bis as adopted in 1998 and Guide to Enactment), art 7.

3.2 The Australian legislation

In 1999 the Australian Federal Government promulgated the *Electronic Transactions Act*.[22] In accordance with the recommendations of the Attorney-General's group of experts,[23] the Act implements the approach in UNCITRAL's 1996 Model Law. Each of Australia's States and Territories was persuaded to follow suit.[24] As a result, while there are minor differences in the wording of each Act, Australia effectively has a national legislative scheme (collectively referred to as the Australian Acts) which implements the 1996 Model Law.[25]

Under the Australian Acts there are four requirements for a valid electronic signature. The electronic method used should (a) identify the person; (b) indicate their approval of the information communicated; (c) be as reliable as appropriate for the purposes at the time it was used; and (d) the person to whom the signature is required to be given must consent to the use of the electronic method.[26]

When compared with the 1996 Model Law it can be seen that additional words were added to the reliability requirement to make it clear that the test of reliability had to take account of circumstances at the time the signature method was used. This enables a finding of validity for a signature method even where advances in technology have rendered it unreliable, as long as, at the time of use, it was a reliable method. The Australian provisions also include the additional requirement of consent by the person to whom the signature was required to be given.

When considered in relation to our scenario, there are difficulties with each of the four requirements for a valid signature.

3.3 Difficulties applying the Australian legislation

1. Does the signature method identify Ms White?[27]

Analysing the meaning of 'identify' is not the purpose of this article. However, it is useful to note some of the difficulties. As used in this context, 'identify' could have at least two meanings:

(a) It could mean that the method must prove that Ms White is who she purports to be. We might call this the 'proof of identity' meaning. Used in this sense, we would anticipate that the method used would have to include a process of authentication of identity, in much the same way as one may be required to produce passports and drivers' licences to authenticate one's identity when opening a bank account.

(b) It could mean that the method must identify Ms White (as opposed to other people) as the person who sent the message, thus linking her to the message in a way that would make it difficult for her to deny the message was from her. Since the function links the signatory to the message, we might call this the 'linking' meaning. Used in this sense, we would anticipate that the message would have to be traceable to a source that is associated with the sender. An expert would have to be able to testify that, in the absence of contrary evidence, it must be concluded that the message must have been from the sender—in much the same way as handwriting experts can testify that a manuscript signature was made by a certain person.

---

22 *Electronic Transactions Act 1999* (Cth).

23 Australia, Report of the Electronic Commerce Expert Group to the Attorney-General, *Electronic Commerce: Building the Legal Framework* (1998).

24 *Electronic Transactions Act 2000* (NSW); *Electronic Transactions (Victoria) Act 2000* (Vic); *Electronic Transactions Act 2000* (SA); *Electronic Transactions Act 2000* (Tas); *Electronic Transactions (Northern Territory) Act 2000* (NT); *Electronic Transactions (Queensland) Act 2001* (Qld); *Electronic Transactions Act 2001* (ACT); *Electronic Transactions Act 2003* (WA).

25 For the purposes of this article, it will be assumed that the events in the scenario took place in Queensland and, where an illustrative provision is needed, reference will be made to the Queensland Act.

26 See *Electronic Transactions Act 1999* (Cth) s 10; *Electronic Transactions Act 2000* (NSW) s 9; *Electronic Transactions (Victoria) Act 2000* (Vic) s 9; *Electronic Transactions Act 2000* (SA) s 9; *Electronic Transactions Act 2000* (Tas) s 7; *Electronic Transactions (Northern Territory) Act 2000* (NT) s 9; *Electronic Transactions (Queensland) Act 2001* (Qld) s 14; *Electronic Transactions Act 2001* (ACT) s 9; *Electronic Transactions Act 2003* (WA) s 9. The Federal Act also contemplates a Commonwealth entity being able to specify certain information technology requirements that must be met when signing electronically—see *Electronic Transactions Act 1999* (Cth) s 10(c)—but this difference is unimportant for the purposes of this article.

27 *Electronic Transactions (Queensland) Act 2001* (Qld) s 14(a) and equivalent sections in the other Australian Acts.

There is an argument that simply typing her first name at the end of the message identifies Ms White. The obvious counter to this argument is that, since anyone could have typed it, on its own, her typed first name would not satisfy either meaning. Whether the sender's email address, or email address with her typed first name, satisfies the requirement would seem to depend on further facts. Ms White's email address is disclosed as originating from 'bond.edu.au'. According to the domain name system, we can surmise that this is an educational institution in Australia. Does this mean that Ms White will have had to authenticate her identity by producing a passport, driver's licence and/or other similar documents when being allocated an email account at that institution; and would this be sufficient to 'identify' Ms White (in the 'proof of identity' sense)? When considering the 'linking' meaning, with what degree of certainty could it be shown that only Ms White could have sent the message from that address? Would evidence be needed that only Ms White had access to that email account?

A decision-maker in our scenario would need to be satisfied that the typed name and/or the sender's email address answered these questions in a way that was appropriately reliable (in accordance with the third requirement discussed below).

2. Does the signature method indicate Ms White's approval of the information?[28]

This requirement appears to be designed to cater for situations in which one of the functions of the signature is to indicate agreement or consent. On the facts of our illustration, it is a rather strained interpretation to suggest that Ms White 'approves' the contents of her message. In reality, she neither approves nor disapproves. She is making a concession that she owes money and informing Mr Brown of her intention not to pay it. If we are to argue that she is 'approving' what she is saying merely because she typed and sent the message, then the 'approval' requirement is fairly meaningless—everyone will be taken to be approving the information in messages they send.

The problem stems from an assumption that a signature is always used to agree with or approve the contents of the message. On the contrary, as our illustration shows, approval is not really relevant in some situations. To belabour the point, perhaps, another example where approval would be irrelevant would be where a person signs an attendance register to prove their presence on a particular occasion. Where the signatory's approval is relevant, it is not the signature alone that indicates approval; it is the content of the message in the given context that indicates the fact of approval. The issue is whether the apparent approval can be repudiated by the alleged signatory; and this depends on the effectiveness or reliability of the 'linking' function. This is discussed under the next requirement.

3. Was the method as reliable as appropriate?[29]

On the face of it, the reliability requirement relates to both prior requirements (as well as any other functions that might be expected of a signature in this context). The issue appears to be whether the method used is appropriately reliable at identifying the signatory and indicating the signatory's approval of the information in the message. How is a decision-maker to test this reliability?

Much will depend on which meaning of 'identify' is considered to be relevant. If the 'proof of identity' meaning is assumed, identifying someone will involve a process of matching the evidence currently being presented with previously known facts about that person; or relying on someone else's prior identification, as for example with a digital certificate. The reliability of the whole process will depend on the extent and reliability of the evidence currently being presented; the extent and reliability of the previously known facts; and the accuracy of the match between the two. In an electronic context, it might include the reliability of the medium through which the message is carried. In the context of our illustration, Mr Brown would want to be able to adduce evidence that, in order to get an email account at Bond University, Ms White would have had to produce documentary proof that she was who she said she was; and that Bond would not have allocated the email account if this was not reliably proven.

If 'identify' is taken to mean 'linking' the signatory to the message, reliability will depend on the ease with which someone could pretend to be the signatory, and the likelihood that someone might do so. Mr Brown would want to be able to adduce evidence that Bond allocates unique email addresses to individual users; and that the authentication process when each user logs on to the system is secure and reliable. If, like Mr Brown, Ms White had been using a Yahoo.com account at the time, the answers to these reliability

---

28 *Electronic Transactions (Queensland) Act 2001* (Qld) s 14(a) and equivalent sections in the other Australian Acts.

29 *Electronic Transactions (Queensland) Act 2001* (Qld) s 14(b) and equivalent sections in the other Australian Acts.

questions might be different, since Yahoo.com does not require any authentication of identity when opening an email account.

The 1996 Model Law and legislation based on it give no hint as to which of these meanings is relevant, nor how one might satisfy the reliability requirement. It might be noted that, in the offline world, without prior production of identification documents and the provision of a sample signature with which the given signature can be compared, a manuscript signature does not perform the proof of identity function. Does it follow that the linking function is the more likely interpretation of the meaning of this requirement in the online world? It is suggested this does not follow. Parties are more often geographically remote and previously unknown to each other in the online world. The first meaning if 'identify' is likely to have far more significance than it might have in the case of manuscript signatures.

4. Did Mr Brown consent to the method being used?[30]

As noted earlier, this is an additional requirement in the Australian legislation which was not part of the 1996 Model Law. Once again, the language is strained—it is difficult to describe Mr Brown's conduct as 'consent'. It is more likely that at the time he received the message from Ms White, he gave no thought to the validity of the signature. When he first becomes aware of the issue or at least by the time the dispute reaches court, Mr Brown would no doubt indicate his consent since it would be in his interests to do so. It is submitted that if the receiver's acquiescence is to be a requirement (and it is not clear why it should be) the onus should be on the person who benefits from the signature to object to the method used. A more suitably expressed provision might be that a signature requirement is taken to have been met if: '… the person to whom the signature is required to be given does not object to the use of the electronic method within a reasonable time'.

3.4 Conclusions

From this discussion it can be seen that a decision-maker has little guidance from legislation based on the 1996 Model Law. We can surmise that the person alleging the validity of the electronic method might have to adduce evidence of the reliability of the electronic method used. Each of the four Australian requirements presents difficult interpretation issues.

In *McGuren v Simpson*,[31] the case on which our scenario is based, there was mention of the NSW Act, but the case was eventually decided on common law principles because the facts arose before the Act was promulgated. Harrison M invoked common law's 'authenticated signature fiction' to hold the email message to be a valid signature for the purposes of interrupting the limitation period.[32]

4. How helpful is the EU/UK approach?

At about the time the Australian legislation was introduced the EU passed the *Electronic Signatures Directive* which was to be implemented by EU member states by 2001.[33] In this section, we explain the EU's Directive and UK legislation which implements it. We then consider how helpful the UK legislation is for a decision-maker faced with the outlined scenario.

4.1 The 1999 EU Directive

The EU Directive distinguishes between an electronic signature and an advanced electronic signature. It defines an electronic signature in a broad and general way as 'data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication'.[34] An advanced electronic signature, on the other hand,

> … means an electronic signature which meets the following requirements:
> (a) it is uniquely linked to the signatory;
> (b) it is capable of identifying the signatory;

30 *Electronic Transactions (Queensland) Act 2001* (Qld) s 14(c) and equivalent sections in the other Australian Acts.

31 [2004] NSWSC 35.

32 *McGuren v Simpson* [2004] NSWSC 35 [21-22]. While the result is arguably a good one, the reasoning based on common law leaves much to be desired—but this is a topic for another day.

33 *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures* [1999] OJ L13/12, 19.1.2000.

34 Ibid art 2.1.

(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable; …[35]

In this 'two-tier' system, the requirements for an advanced electronic signature are specific. When read with the other provisions of the Directive, it becomes clear that the requirements facilitate encryption systems that use certification services.36 In this article we are not concerned with legislative provisions implementing this upper tier. We are interested in the first tier or lower level electronic signature. The Directive does not specify criteria for this type of signature. Article 5.2 merely requires:

Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
— in electronic form, or
— not based upon a qualified certificate, or
— not based upon a qualified certificate issued by an accredited certification-service-provider, or
— not created by a secure signature-creation device..[37]

It can be seen that this approach is even less intrusive than the 1996 Model Law. It merely requires that electronic methods should not be invalid simply because they are electronic or because they do not meet the criteria for an advanced electronic signature. What amounts to a valid lower level signature is left open.

4.2 The UK legislation

The *Electronic Communications Act 2000* (UK) c 7 and the *Electronic Signatures Regulations 2002* implement the EU Directive. The Regulations are not relevant for our purposes, since they deal with data protection and the supervision and liability of Certification Service Providers. Omitting the words that relate to certification, the relevant section in the Act provides:

7. Electronic signatures …
(1) In any legal proceedings—
(a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, …
shall … 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.
(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 so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both.

Interestingly, the Act also gives wide powers to the Minister in charge of a relevant Government department to authorise or facilitate electronic communications by modifying the provisions of legislation (or schemes, licences, authorisations and approvals made under legislation).[38] One of the specified purposes is where something is required to be done or to be authorised by a person's signature.[39]

4.3 Difficulties with the UK legislation

Despite the requirement in the EU Directive, the UK Act says nothing about the legal effectiveness of electronic signatures. It merely confirms that electronic signatures are admissible in legal proceedings. Presumably this is because English common law has always had a flexible approach to the acceptance of new technology. Engravings,[40] rubber stamps,[41] typewriting[42] and telegrams[43] have all been recognised as

35 Ibid art 2.2.
36 Apart from the signature-enabling aspects of art 5.2, the other articles are concerned with secure signature creation devices, certification services and cross-border issues. Stephen Mason, *Electronic Signatures in Law* (2nd ed, 2007) suggests at [4.3] that the focus is even more narrowly on smart cards.
37 *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures* [1999] OJ L13/12, 19.1.2000, art 5.2.
38 *Electronic Communications Act 2000* (UK) c 7, s 8.
39 *Electronic Communications Act 2000* (UK) c 7, s 8(2)(c).
40 *Jenkins v Gaisford & Thring* (1863) 3 Sw & T 93.
41 *Bennet v Brumfitt* (1867-1868) 3 LRCP 28.
42 *Newborne v Sensolid (Great Britain) LD* [1954] 1 QB 45.
43 *Godwin v Francis* (1870) LR 5 CP 295.

satisfying signature requirements in certain circumstances. There is no reason why electronic signatures would be treated differently. In December 2001 the UK Law Commission confirmed its view that English common law already satisfied the EU requirement and a global legislative solution was not only unnecessary but risky since it might unintentionally override desirable requirements of form.[44] The wide powers given to Ministers by s 8 make it easy to address specific problems as and when they arise, but they offer no clarity or certainty in the meantime. Ministers' powers have thus far been exercised to clarify whether various notices or applications required by statute can be made electronically. They do not clarify what is meant by an electronic signature or what types of signature would be acceptable for specific purposes. Where they do mention electronic signatures, they merely adopt the definition in s 7(2) quoted above.[45] As a result, the UK legislative approach offers no assistance in our scenario—the issue is left to the judge who must apply common law principles.

An English decision-maker operating under common law is thus likely to have just as much flexibility as a decision-maker operating under the Australian Acts. There would be nothing preventing them from recognising the various low level electronic methods as signatures. As with the Australian approach, this flexibility is also a weakness. Nor does this approach answer the need to introduce timely solutions. Brazell, for example, explains why so many jurisdictions have implemented legislation:

> Uncertainties … [were] seen as a potentially significant barrier to the expansion of e-commerce. Although it would certainly have been possible for the courts to produce equivalent guidance through future case law, this would of course have been a slow process with potentially years of commercial uncertainty in the interim.[46]

Besides being slow, development through case law is piecemeal and expensive. Waiting for case law to clarify issues depends on a particular issue being important enough to warrant litigation in a senior court. Most low level signature disputes are unlikely to warrant this—if they go to court at all, they go no further than a lower court. This leaves lower courts with the difficult task of making decisions without the benefit of any guidance.

Although section 7 has nothing direct to say about the validity of electronic signatures, it is interesting to reflect on whether the email address or the typed first name of the sender in our scenario would be admissible in evidence under this provision. Both the email address and typed name are in an electronic form and incorporated into the email communication, so would satisfy s 7(1)(a) and s 7(2)(a). It is not clear, however, that they 'purport to be … for the purpose of being used in establishing the authenticity' of the email message. The purpose of the sender's email address would normally be to provide a return address for a reply rather than to establish authenticity. In addition, except perhaps in a very broad and loose sense, Ms White's intention when typing her first name in our scenario will hardly have been so that it could be used to establish the authenticity of her email message. Section 7 may not even be effective in ensuring the signature method would be admissible in evidence.

The only reported UK judgment dealing with electronic signatures is *Mehta v J Pereira Fernandes SA*.[47] The issue was whether an email message guaranteeing a debt had been effectively signed for the purpose of the *Statute of Frauds*. The message contained the sender's email address, but no typed name at the end. Pelling J made passing reference to the *Electronic Communications Act 2000* (UK), and to the Law Commission's view that no legislative changes were necessary as existing law was adequate.[48] However, he held that without a typed name at the end of the message, there was no effective signature that was consistent with existing case law.[49] While this reasoning deserves further analysis, it is not relevant to the examination of legislative approaches undertaken in this article. The observation need only be made that the UK legislation was singularly unhelpful in deciding the issue.

5. Other approaches and International developments

Since the 1996 Model Law and the 1999 EU Directive there have been two United Nations-sponsored developments: the *Model Law on Electronic Signatures* (the '2001 Model Law')[50] and the UN *Convention*

---

44 UK Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions*, Dec 2001 [3.43]

45 See, for example, the *National Health Service (General Medical Services)(Electronic Communications) Order 2001*, SI 2890 of 2001, art 2(2).

46 Lorna Brazell, *Electronic Signatures and Identities: Law and Regulation* (2nd ed, 2008) 3.

47 [2006] EWHC 813 (Ch).

48 [2006] EWHC 813 (Ch) [30].

49 [2006] EWHC 813 (Ch) [29-30].

50 UNCITRAL, *Model Law on Electronic Signatures*, GA Res 56/80, GAOR 56th sess, 85th plen mtg, UN Doc A/Res/56/80 (2001).

on the Use of Electronic Communications in International Contracts (the '2005 Convention').[51] In late 2008 the Australian Federal Government began a consultation process with a view to amending the Australian Acts to facilitate accession to the 2005 Convention.[52] In this section consideration will be given to whether following either or both of these developments will solve the weaknesses identified.

5.1 The 2001 Model Law

UNCITRAL recognised that its 1996 Model Law needed refinement and the Working Group on Electronic Commerce continued to develop its approach. Unfortunately this work took longer than anticipated, and, by the time it produced its Model Law on Electronic Signatures in 2001 (the '2001 Model Law')[53] many countries had already implemented legislation based on the 1996 Model Law.[54] According to UNCITRAL's records, only seven countries have adopted the recommendations in its 2001 Model Law, and one country has enacted legislation influenced by its principles.[55]

The two models are in a sense complementary. The 2001 approach is more sophisticated, but it does not contradict the earlier approach. Unlike the 1996 Model Law, it defines an electronic signature; but it does so very broadly as:

> 'data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.'[56]

The 2001 Model Law also expands on criteria that will render a signature appropriately reliable for its purpose.[57] It does this without derogating from the ability to establish appropriate reliability without reference to the new criteria—reliability can still be shown in the same way as it might have been shown under the 1996 Model Law.[58] In summary the new supplementary criteria are that the signature creation data must be linked to the signatory and to no other person; the signature creation data must, at the time of signing, be under the control of the signatory and no other person; any alteration to the signature made after signing must be detectable; and where a purpose of the signature requirement is to assure the integrity of the information, any alteration to the information made after signing must be detectable.

Several other provisions in the 2001 Model Law specify general standards of conduct required of certification providers and other parties to a signature system.[59] The expanded criteria for reliability, together with these standards of conduct, are designed to facilitate the recognition and use of digital signatures based on public key encryption.[60] By facilitating public key signatures without derogating from the more general and flexible earlier approach, the 2001 Model Law achieves a 'two-tier' system similar to the EU Directive.

Would legislation along these lines help a decision-maker in our scenario? The definition of electronic signature might clarify the dilemma as to the meaning of 'identify' under the Australian Acts since, to qualify as an electronic signature, the signature data must be capable of identifying the signatory 'in relation to the data message'. It is arguable this phrase indicates that it is the linking of the signatory to the message, not the proof of identity, which is important. Where anyone could have signed the message, proof of identity might well be relevant in proving the link between the signatory and the message; but where a user's identity is already authenticated (such as where the person has logged on to a secure site with a username and password—as Ms White must have done to access her email account) the relevant issue

---

51 United Nations, *Convention on the Use of Electronic Communications in International Contracts*, GA Res 60/21, GAOR 60th sess, 53rd plen mtg, UN Doc A/Res/60/21 (2005).

52 Federal Attorney-General's Department, 'Australia's Accession to the UN *Convention on the Use of Electronic Communications in International Contracts* 2005: Proposed Amendments to Australia's Electronic Transactions Laws' (Consultation Paper, November 2008).

53 UNCITRAL, *Model Law on Electronic Signatures*, GA Res 56/80, GAOR 56th sess, 85th plen mtg, UN Doc A/Res/56/80 (2001) ('2001 Model Law').

54 Stephen Mason, *Electronic Signatures in Law* (2nd ed, 2007) [3.1].

55 UNCITRAL, *Status: 2001 - UNCITRAL Model Law on Electronic Signatures*, <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_status.html> at 10 August 2009.

56 2001 Model Law, art 2(a).

57 UNCITRAL, *Model Law on Electronic Signatures*, GA Res 56/80, GAOR 56th sess, 85th plen mtg, UN Doc A/Res/56/80 (2001) art 6.3.

58 UNCITRAL, *Model Law on Electronic Signatures*, GA Res 56/80, GAOR 56th sess, 85th plen mtg, UN Doc A/Res/56/80 (2001) art 6.4.

59 Ibid arts 8-11.

60 Lorna Brazell, *Electronic Signatures and Identities: Law and Regulation* (2nd ed, 2008) [5-013]; Stephen Mason, *Electronic Signatures in Law* (2nd ed, 2007) [3.6].

appears to be whether the signatory can be linked to the message in a way which is similar to a manuscript signature.

However, overall the 2001 Model Law's two-tier approach would still be unhelpful. The provisions relating to an upper or second tier would be relevant and useful if Ms White's email had been 'signed' using a public key or similar encryption system. In the absence of such a digital signature, a diligent court would have to go back to a basic enquiry about the purpose of the signature requirement and the technological attributes of email messages to see if they satisfy the appropriate reliability requirement in this context.

There is one other provision in the 2001 Model Law that deserves mention. It recommends that a non-legislative entity be set up with authority to make determinations about the validity of particular signature methods.[61] This has potential to address uncertainty. If such a body were energetic and proactive, it could well give considerable guidance to decision-makers and Internet users. On the other hand, if such a body was merely reactive, making determinations only when disputes arose, it would suffer from the same basic disadvantage identified above when contemplating leaving legal development to case law or to a Minister.

5.2 The 2005 UN Convention

In late 2008 the Australian Federal Government began a consultation process with a view to amending the legislation to facilitate Australia acceding to the 2005 Convention.[62]

Article 9(3) of the UN's 2005 Convention[63] states:

> 3. Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:
>
> (a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and
>
> (b) The method used is either:
>
> (i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
>
> (ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.

The wording is familiar, but there are two differences worth noting. The existing reference to the signatory's 'approval' of the information is replaced with 'intention'. This would be an improvement. Referring to our illustrative facts, it would be a much less strained interpretation if a decision-maker had to consider whether Ms White's use of the email system indicated her intention rather than her approval.

Paragraph 3(b)(ii) is also an interesting addition. It is designed to prevent a party relying on the technicality that the signature method is objectively unreliable as a general rule even though the 'signatory' admits sending the message and it has been received without error. In other words, where the potential unreliability of the signature method did not actually cause a problem on the facts, the signature method should be treated as reliable. While this might be a useful addition, it will not help a decision-maker work out how to test reliability in the first place.

The conclusion to be reached is that amendments to the Australian or UK legislation that facilitates accession to the 2005 Convention will still not be of much help to a decision-maker in our scenario.

6. The scope of the problem and suggestions

Our illustrative scenario exposes the problems when considering one particular legislative requirement for a signature and one relevant signature method. The magnitude of the problem is especially obvious when one considers the number of legislative requirements for a signature in most modern jurisdictions. It is difficult to be precise about the exact number at any point in time; but it is a large number. As at 8 March 2010, for example, a simple search in the Australasian Legal Information Institute's 'all legislation' database[64] for 'sign*' produced 68,805 occurrences; and for 'signature' produced 9,800 occurrences. A similar search in

---

61 UNCITRAL, *Model Law on Electronic Signatures*, GA Res 56/80, GAOR 56th sess, 85th plen mtg, UN Doc A/Res/56/80 (2001) art 7.

62 Federal Attorney-General's Department, 'Australia's Accession to the UN *Convention on the Use of Electronic Communications in International Contracts* 2005: Proposed Amendments to Australia's Electronic Transactions Laws' (Consultation Paper, November 2008).

63 United Nations, *Convention on the Use of Electronic Communications in International Contracts*, GA Res 60/21, GAOR 60th sess, 53rd plen mtg, UN Doc A/Res/60/21 (2005).

64 Australasian Legal Information Institute (AustLII), <www.austlii.com.au> at 8 March 2010.

the British and Irish Legal Information Institute[65] produced 36,801 and 4,156 occurrences respectively. With the volume of subordinate legislation and the ease with which it is promulgated, signature requirements are being added all the time.

As pointed out in the introduction, there are also many different ways that some or all of the functions of a signature can be simulated online. Relevant new technologies are constantly developing. It will suffice to mention two examples: smart cards can be used to manage and generate signature data more effectively and securely; and the use of biometrics such as fingerprints and iris scans have been and are being further developed to perform some of the functions of a signature. The expanding nature of potential signature methods exacerbates the problem.

Apart from *McGuren v Simpson*[66] (the Australian case on which our scenario was based) there have only been two other reported Australian decisions dealing with the signature provisions of the Australian Acts.[67] In the UK there are no decisions other than *Mehta v J Pereira Fernandes*[68] mentioned earlier. This is hardly surprising. As pointed out earlier, legal development through cases depends on the issue being regarded as important enough to warrant the considerable time and expense of litigation in a senior court; and this is not an everyday occurrence.

One of the Australian cases[69] demonstrates a meticulous attention to the requirements of the Australian Acts. The issue was whether an objection to a planning development application was a 'properly made submission' under the *Integrated Planning Act 1997* (Qld). One of the requirements for a 'properly made submission' was that it had to be in writing and signed.[70] The City Council had adopted a deliberate policy of facilitating electronic submissions via its website, and required that (i) the user include identification information, thus ensuring the method satisfied the first requirement of the signature provision in the Queensland Act; (ii) the user click on an 'I accept' button after being asked to confirm the details of the submission and agree that the electronic submission had the same status as a signed submission. This ensured the user approved the information and intended to sign it. Robin J decided that, despite an error having been made in the identification details submitted, this method was appropriately reliable for the purpose and was thus a properly made submission. While it is an interesting case, given that the City Council had taken such deliberate steps to address each of the signature requirements in the Australian Acts, the conclusion does little to clarify the uncertainty identified earlier.

On the other hand, *Faulks v Cameron*[71] demonstrates the rather superficial analysis encouraged by the difficulties in interpreting the Australian Acts. The case involved the enforceability of email correspondence as a 'separation agreement' which had to be signed under the *De Facto Relationships Act*.[72] Other than mentioning *Torrac Investments v Australian National Airline Commission*,[73] where a telex with a printed name on it was held to be signed, Young M considered it 'unnecessary to refer to the many cases about electronic or telexed signatures'.[74] After referring to the signature provisions of the Northern Territory's *Electronic Transactions Act*,[75] he merely stated:

> I am satisfied that the printed signature on the defendant's e-mails 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 subsection 45(2).[76]

None of these cases are helpful in developing a clear and consistent method or approach to the interpretation of the legislative requirements. None of them involve the adducing of relevant evidence, technical or otherwise, to prove the appropriateness or reliability of the signature method used. Again, this is understandable. It would require evidence being given by technical experts—a time-consuming and expensive exercise. This exposes another weakness in leaving development to cases: difficult issues seldom get the depth of treatment they need until they get to a senior appellate court. To summarise the difficulties: (a) There is a wide range in the extent to which signature methods or activities might achieve appropriate reliability. Satisfying this requirement might call for technological evidence of the way the signature method works; (b) The appropriate level of reliability is likely to be different for the purposes of different legal

---

65 British and Irish Legal Information Institute (BAILII), <www.bailii.org> at 8 March 2010.
66 [2004] NSWSC 35 discussed briefly in the text at footnote 31 above.
67 *Faulks v Cameron* [2004] NTSC 61; and *Harding v Brisbane City Council & Ors* [2008] QPEC 75.
68 [2006] EWHC 813 (Ch).
69 *Harding v Brisbane City Council* [2008] QPEC 75.
70 *Integrated Planning Act 1997* (Qld), sch 10.
71 [2004] NTSC 61.
72 *De Facto Relationships Act 1991* (NT) s 45(2).
73 (1985) ANZ Conv R 82.
74 *Faulks v Cameron* [2004] NTSC 61 [63].
75 *Electronic Transactions (Northern Territory) Act 2000* (NT) s 9.
76 *Faulks v Cameron* [2004] NTSC 61 [64].

signature requirements, depending on the reason why the signature is required. It is unclear what factual evidence would be necessary to prove an appropriate level of reliability in each case; (c) It would be tedious and wasteful of time if evidence of reliability had to be adduced afresh in each case; (d) Leaving clarification of the law in this area to development through cases and the doctrine of precedent is unsatisfactory.

One way to achieve absolute certainty would be to individually examine every statute that required a signature; and amend the statute to specify which Internet methods would satisfy that particular requirement. Given the number of signature requirements mentioned earlier, the number of Internet methods that could arguably be seen as a signature and the speed with which new methods or variations on existing methods develop, this suggestion is impractical.

At the conceptual level, what is needed to achieve more certainty in the ever-moving online world is a multi-tier system. The top tier might recognise the most reliable signature technology (eg digital signatures using strong encryption) as being valid for all purposes. This would achieve certainty where needed. The bottom tier would allow the sort of flexible approach advocated in the 1999 Model Law—any method that can be shown to be appropriately reliable. To overcome the uncertainty this engenders, between these two extremes an approach is needed that uses a generalised method of rating signature activity in a way that predicts that activity's suitability as a valid signature for a specific purpose. The aim would be to help a user select an appropriate method or predict whether a method they have used is likely to be considered appropriate for a particular statutory purpose. Ideally, the method of rating signature activity should be general enough to be usable with likely future online signature techniques. The rating system would need to take account of authentication, security and reliability and might be developed by technologists or standards organisations. Whether such a rating system is feasible, or has sufficient merit to warrant development, remains to be seen.

Jay Forder
Associate Professor, Faculty of Law, Bond University, Australia.

****