ARTICLE:

ENFORCING 'SIMPLE' ELECTRONIC SIGNATURES IN AN INTERNATIONAL CONTEXT

By **William K. Norton**[1]

American companies accustomed to implementing electronic signatures domestically have sought to find ways to enforce 'simple' electronic signatures worldwide. While 'advanced', 'secure' or digital signatures can be enforced in just about every country, it is often difficult to meet the cumbersome technical requirements in each jurisdiction. Our law firm worked with a number of companies to develop policies to improve the likelihood of enforcing simple electronic signatures in approximately 50 jurisdictions. This paper summarizes the issues we encountered.

Introduction

U.S. companies have become accustomed to interacting with customers through electronic contracts using simple electronic signatures such as clickwrap signatures. Many of these companies have seen the advantages of communicating electronically and want to implement electronic contracts and signatures with customers, partners and employees around the world. To this end, a number of companies approached our law firm to try to establish policies. However, as we soon discovered, there are very few simple answers when it comes to the international use of electronic signatures.

Our clients were interested in finding ways to ensure the enforceability of electronic signatures without placing undue burden on their business processes. While 'advanced', 'secure' and digital signatures can be enforced in just about every country, it is often difficult to meet the cumbersome information technology, security and archival requirements in each jurisdiction.

Thus, the focus of our research turned to understanding the potential to enforce simple electronic signatures. Businesses were more willing to adapt their legal and procurement processes to enforce simple electronic signatures rather than to attempt to coordinate the use of digital signatures with their customers and partners.

With the aim of enforcing simple electronic signatures, also referred to simply as electronic signatures in this paper, we developed a set of recommendations for approximately 50 jurisdictions. Our investigation considered not only the enforceability of specific types of electronic signature, but also the steps that businesses could take to make electronic signatures more likely to be enforceable.

Issues with enforcing electronic signatures

There are essentially three criteria in determining whether an electronic signature will be enforced in a particular jurisdiction: 1) the type of agreement that is being signed, 2) the type of electronic signature that is being used, and 3) how each party consents to the use of the electronic signature. Enforceability is only established once both parties have consented to using an electronic signature that either meets handwritten signature requirements under the jurisdiction's electronic signature statute or is being used as a matter of proof of party conduct.

Because our clients were large, multinational corporations, they had a broad range of contracts that they preferred to sign electronically. However, for certain types of contracts, it was expected that electronic signatures may not be an option. For example, in many

1 *The author thanks Chris Sloan for his valuable advice in reviewing the paper.*

countries, the use of electronic signatures is expressly precluded for the conveyancing of real estate. Conversely, some types of contracts, such as employment contracts, raised surprising enforceability issues, particularly in European countries.

When implementing electronic signatures, the threshold question is whether or not agreements require the equivalent of handwritten signatures. In cases in which handwritten signatures are not a requirement, electronic signatures can be used as a matter of proof of the conduct or intent of other parties to assent to the terms of agreements. In other words, even though a certain type of electronic signature might not be considered equivalent to a handwritten signature, the electronic signature could still be used as evidence that a party actually intended to sign an agreement, in the absence of any handwritten signature requirements.

If handwritten signatures are a requirement for a specific type of agreement, the next step is to ascertain which types of electronic signatures are equivalent to handwritten signatures in a particular jurisdiction. This determination can usually be affected by agreement of the parties. So this question must be considered in two parts. First, the types of electronic signature that are equivalent to handwritten signatures if the parties explicitly agree to the use of specific types of electronic signature. Second, the types of electronic signature that are enforceable in the absence of such an agreement. In some countries, we found that simple electronic signatures could only be enforced if parties explicitly agreed to their use. In other countries, they could not be enforced even with such agreement.

Moreover, the issue of how to get consent of the other party to use electronic signatures creates practical problems. Even the most liberal, minimalist countries require consent of the other party in order to transact using electronic signatures. In those countries, consent may be inferred from party conduct. A customer clearly assents to a clickwrap agreement by clicking the 'I Accept' button on a webpage. However, initiating electronic transactions can be more problematic in countries that require explicit consent of both parties. Is it possible for one to consent to transact electronically using an electronic signature? If so, what ensures the enforceability of that electronic signature? This recursive problem might seem academic, but it produces difficulties for businesses looking to ensure the enforceability of major contracts.

Because consent is often crucial to enforcing electronic signatures, our advice to clients has been to use the most reliable method of gaining consent – particularly in countries requiring explicit consent of parties. When possible, it is best to obtain initial consent in a physical form with a handwritten signature. However, companies wanting to implement electronic signatures are probably doing so to avoid using paper copies. Thus, this sort of measure would only be taken in exceptional circumstances. Our clients were most interested in gaining consent electronically.

Analysis of electronic signature enforceability by jurisdiction

In order to understand the enforceability of electronic signatures in each country, we first collected the statutes and regulations governing electronic contracting. We then translated and categorized the statutes according to the likelihood of enforcing electronic signatures. Finally, we retained local counsel to help us understand the application of electronic signature laws in context. Summarized below are findings from a subset of jurisdictions considered.

Hong Kong

Electronic signatures in Hong Kong are governed by the Electronic Transactions Ordinance, as amended in 2004 ('ETO'). Under the ETO section 6(1), an electronic signature may be used to satisfy legal requirements that documents must be signed using the equivalent of a handwritten signature. The requirements necessary to enforce an electronic signature are:

c) a method is used to attach the electronic signature to or logically associate the electronic signature with an electronic record for the purpose of identifying the signatory and indicating authentication or approval of the information contained in the document

d) having regard to all the relevant circumstances, the method used is reliable, and is appropriate, for the purpose for which the information contained in the document is communicated; and

e) the recipient consents to the use of the method by the signatory.

Consent under the ETO includes consent that can be

reasonably inferred from the conduct of the person concerned. The local counsel in this jurisdiction indicated that the parameters of implied consent are far from certain, given the lack of case law and the inference that consent be subject to reasonableness. Thus, it was recommended to get explicit consent of the opposing party to transact electronically.

With regards to specific types of electronic signature, the local counsel in this jurisdiction indicated that most should be enforceable. Counsel said that there is English precedent, which remains persuasive in Hong Kong, of facsimile signatures being enforced and that PDF signatures are likely to be enforceable given similar supporting evidence of authenticity. Electronic signatures and click-through agreements were also considered likely to be enforced assuming the technologies make it possible to identify the signatory.

Local counsel indicated that clickwrap agreements may be enforceable if a signatory is given an opportunity to identify him or herself or some other mechanism exists to identify the signatory (e.g. his or her IP address is recorded upon signing, and such IP address can be traced to the relevant individual). However, without such proof, it would be difficult to prove that such an electronic signature pertained to a particular individual and therefore identified the signer.

The Netherlands

Electronic signatures in the Netherlands are governed by the Electronic Signatures Act as reflected in the Civil Code and the Code on Civil Proceedings. According to article 3:15a of the Civil Code, an electronic signature (defined as a signature which exists from electronic data linked to or logically associated with other electronic data that is used as a method for authentication) has the same legal effect as a handwritten signature, provided that the method used for its authentication is sufficiently reliable. Such method is presumed to be sufficiently reliable if it meets the following requirements:

a. it is linked in a unique way to the signatory;

b. it makes it possible to identify the signatory;

c. it comes about by means of resources which the signatory is able to keep under his exclusive control;[2]

d. it is linked in such a way to the electronic file to which it relates, that each modification of the data can be traced afterwards.

Local counsel indicated these requirements would not be likely to be met unless the signature was attached to the document using a digital signature or some other form of encryption. Thus, it is unclear whether any simple electronic signatures could meet the reliability criteria.

However, section 6 indicates that the parties may set aside these requirements as it concerns their mutual relationship. Parties may determine the admissibility and method of contracting electronically, including technical requirements that must be satisfied. According to local counsel, Dutch courts will follow such contractual arrangements in principle.

Therefore, while it is unclear that electronic signatures would be considered 'reliable' and enforced by courts on their own merit, explicit agreement between parties to contract using certain electronic methods are likely to be enforced. However, local counsel cautioned that this will only govern the rights and obligations as to the parties to the agreement, and will not affect the rights of third parties.

Japan

The use of electronic signatures in Japan is governed by the Act on Electronic Signatures and Certification. This statute deals almost entirely with digital signatures and their certification. An electronic signature is defined under the statute as a measure taken with regard to information that can be recorded in an electro-magnetic record, which indicates that the information was created by the signatory and can detect alterations to the information. According to the local counsel, this definition would require encryption technology amounting to digital signature requirements. Local counsel also pointed out, with regards to government contracts, digital signatures must be used in Japan.

On the other hand, the local counsel indicated that

2 *It is, of course, impossible for any form of electronic signature to be retained under the exclusive control of a person, for which see Stephen Mason, Electronic Signatures in Law (3rd edn, Cambridge University Press, 2012), 118-120 – it is probably for this reason that the European Union have amended article 2(1)(2)(c) of 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 013, 19.01.2000 p. 0012 – 0020, for which see 'Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance)' {SWD(2012) 135}, {SWD(2012) 136}, COM(2012) 238/2, where the revised text in proposed new article 3(7)(c) reads 'it is created using electronic signature creation data that the signatory can, with high level of confidence, use under his sole control', available at http:ec.europa.eu/information_society/policy/esignature/docs/regulation/com_2012_2038_en.pdf.*

A qualified electronic signature is equivalent to a digital signature and thus none of the simple electronic signatures would meet technical requirements

there is no Japanese equivalent to a statute of frauds. Thus, there are no significant writing requirements under Japanese law. (The one exception is wills.) Any electronic signature could be considered in evidence by a court as to its enforceability. Local counsel did warn, however, that for certain important documents, such as real estate contracts, publicly registered seals are typically used. These types of agreements would be more like handwritten signature requirements, and would be likely to require some form of encrypted digital signature, if any alternative is enforceable at all.

Local counsel stated there are no limitations as to how parties can agree to use electronic signatures, provided the authenticity and agreement of the parties can be proven. In the case of clickwrap agreements, there have been no cases directly challenging their enforceability, even though they are commonly used in Japan. For this reason, it was suggested that a business should take measures to enhance enforceability such as requiring users to scroll through terms and conditions and highlighting any important or surprising terms before users are required to accept the agreement.

Germany

Local counsel in Germany indicated that, according to § 126 of the German Civil Code, any document or declaration of intent would need to have a qualified electronic signature attached when a written form is required by law. A qualified electronic signature is equivalent to a digital signature and thus none of the simple electronic signatures would meet the technical requirements. Also, any documentary evidence for a contract needs to bear a qualified electronic signature to be admissible as proof according to § 371 of the German Code of Civil Procedure.

Local counsel, however, did indicate that many contracts are not required to be in written form by law and that parties can otherwise agree to use a simple electronic signature that satisfies the writing requirements. In other words, where the law does not require a written form, the parties can agree to use electronic signatures other than qualified electronic signatures. Unlike qualified electronic signatures that are presumed to be valid, electronic signatures have to be supported with 'witness proof,' and they still cannot be used to fulfil contracts that are required by law to be in writing. The types of agreements that are legally required to be in writing include all contracts dealing with real estate (including leases) and employment contracts. Although many types of contracts may be signed using simple electronic signatures upon agreement of the parties, some important agreements cannot.

France

French local counsel indicated that, when a signed written instrument is required, it is possible to use an electronic signature, provided that such electronic signature duly authenticates the signatory and ensures the integrity of the signed document. The requirements for electronic signatures to meet handwritten signature requirements are found in article 1316-4 of the French Civil Code:

> The signature necessary to the execution of a legal transaction identifies the person who apposes it. It makes clear the consent of the parties to the obligations which flow from that transaction. When it is apposed by a public officer, it confers authenticity to the document.
>
> Where it is electronic, it consists in a reliable process of identifying which safeguards its link with the instrument to which it relates. The reliability of that process shall be presumed, until proof to the contrary, where an electronic signature is created, the identity of the signatory secured and the integrity of the instrument safeguarded, subject to the conditions laid down by decree in Conseil d'État.

Based on these criteria, local counsel explained that facsimile or PDF copies of a signed original document may be admissible but may be challenged if the original cannot

be produced before the court. Other types of electronic signature such as EchoSign or DocuSign or click-through signatures are more likely to be enforceable, as long as it is possible to prove that the electronic signature warrants the integrity of the signatory and the content of the signed document. Local counsel, however, indicated that clickwrap agreements do not meet the legal requirements for authenticity.

On the other hand, local counsel pointed to article 1316-2 as a provision that gives parties more freedom to agree to use specific types of electronic signatures. This section provides that parties may agree to use a specific method of authenticating the signatory and to ensure the reliability of a signature. Local counsel indicated that courts are expected to enforce electronic signatures agreed to by parties in the business-to-business context, even if signatures would not normally be considered reliable. Therefore, agreement of parties provides the greatest possibility of enforcing all types of electronic signatures indicated.

However, there are two caveats to this general rule. First, there are certain types of agreement that mandate a specific type of signature pursuant to statutory provisions (e.g. sale of real estate property or wills). Second, local counsel discouraged using electronic signatures to demonstrate agreement of the parties to use electronic signatures. He suggested that an agreement to use a particular type of electronic signature might only be enforced by courts if signed using a signature considered more reliable by courts. Thus, a clickwrap agreement indicating that the parties will transact using clickwrap signatures in the future might not improve the enforceability of such a method. However, an agreement of the parties using handwritten signatures would.

Conclusion

In summary, the enforcement of any type of electronic signature requires businesses to determine if the agreement in question must be signed using the equivalent of a handwritten signature. If the type of contract requires handwritten signatures, it becomes necessary to meet the requirements of the jurisdiction's electronic signature statute. It would also be necessary to ensure that the type of contract is not explicitly excluded from the electronic signature statute and that the business retains evidence to support the authenticity of the signatory in order to demonstrate the signatory's intention to be bound to the document.

In choosing the type of electronic signature to use and the method of gaining consent of the other party, businesses must weigh the ease of implementation with the certainty of enforceability. Different types of procedures and electronic signatures might be necessary for more significant transactions. Overall, it is difficult to represent that any type of electronic signature will be enforced in all circumstances and for all types of agreements. Short of confirming the enforceability of signatures with local counsel for every potential circumstance, businesses will only be able to determine whether a method of electronic signature is broadly enforceable in most circumstances. Businesses can then use those risk assessments to determine whether to proceed with electronic signatures in a particular jurisdiction.

William K. Norton is an associate with Baker Donelson Bearman Caldwell & Berkowitz, PC, in the Business Technology and Emerging Companies practice groups. He focuses on emerging and technology-centered companies, advising clients on business issues around the use of intellectual property. He regularly presents seminars on domestic and international electronic contracting.

willnorton@bakerdonelson.com