ARTICLE:

The e-signature in Taiwan: consent, integrity and accessibility

By **Po-Hsiang Ou and Alex Tsai, with Nathan Kaiser**

The number of people using the internet in Taiwan has increased from less than 30 per cent of the population in 2000, to about 80 per cent in 2014.[1] Shopping and doing business online have clearly become part of the population's daily life in Taiwan. While transactions on the internet are now commonplace, the concept and the legal effects of signing documents online are still not as straightforward as physical signatures on documents. The situation is true in Taiwan as in many other advanced digital economies. Some scholars indicate that this is linked with a lack of understanding of the legal structure and technologies of electronic and digital signatures;[2] others suggest that there are also various risks associated with electronic records and signatures.[3]

It is therefore important for the law to provide certainty for the legal definition and effect of e-signatures[4] and to facilitate the technology, where it is considered to be necessary. Taiwan enacted the Electronic Signature Act on 14 November 2001, which governs the legal status and use of electronic records and electronic signatures. The government has also developed a digital certificate system for its citizens, and recently broadened its scope to cover foreign residents.[5] Taiwan has certainly become a mature internet society, but in terms of its law, there is perhaps still room for improvement.

This paper will introduce Taiwan's 2001 Electronic Signature Act ('the Act'). The Act centres around three main principles that render electronic records and e-signatures having the same legal effect as their traditional counterparts: consent between both parties; the integrity of the electronic records, and the accessibility of such records in the future.

The 2001 Electronic Signature Act of Taiwan

Traditional business models utilize written documents and signatures or seals to establish rights and obligations between parties. Advances in technology and e-commerce have led to businesses becoming more dependant on electronic records and e-signatures for communications, negotiations, and transactions. In order to make e-commerce popular and acceptable among enterprises and consumers, several important items are needed:

1. A relatively safe and reliable internet environment.

2. A regime that seeks to prevent illegal duplication of electronic records and e-signatures.

3. A system that helps users to identify parties involved in a transaction.

4. A legal framework that makes transactions smooth and easy.

However, we also note that it is in nearly impossible to establish a perfectly safe, secure and transparent internet environment. Moreover, as scholars have pointed out, illegal duplication of electronic records persists, and it remains difficult to identify the parties in electronic transactions.[6] The second best solution thus relies on a legal framework that can simplify electronic transactions and facilitate some basic levels of trust towards the imperfect system. In some cases where the identities of e-signatures were disputed, the court in Taiwan ruled that the risk of electronic transaction should primarily be borne by the party

[1] According to data of the International Telecommunications Union; see summary of the Internet World Stats at http://www.internetworldstats.com/asia/tw.htm .
[2] Tim Travers, 'On-line signing made simple', 1 *Digital Evidence and Electronic Signature Law Review* (2004), 44 – 50.
[3] Greg Casamento and Patrick Hatfield, 'The Essential Elements of An Effective Electronic Signature Process', 6 *Digital Evidence and Electronic Signature Law Review* (2009), 83 – 97.
[4] The term 'e-signature' is used to include both 'electronic signature' and 'digital signature', which have specific and different meanings under the Taiwanese law.
[5] Introduction of the Ministry of the Interior: http://moica.nat.gov.tw/en/about.html .
[6] For some examples of illegal e-signature duplication, see Stephen Mason, *Electronic Signatures in Law* (3rd edn, Cambridge University Press, 2012); for the challenges of identification, see 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) 21:5 *Computer and Telecommunications Law Review* 135; Nicholas Bohm and Stephen Mason, 'Identity and its verification' (2010) 26:1 *Computer Law & Security Review* 43.

providing such electronic transaction services, unless the party can prove otherwise.[7]

The critical issue involves establishing a legal system that provides clear legal criteria for the definition and validity of electronic records and e-signatures, while not hindering any transactions. These are included in the legislative purposes of the Act, as provided for in article 1: to encourage the use of electronic transactions, to ensure their security, and to facilitate the development of e-government and e-commerce. In general, the role of the law is to solve two critical concerns about using electronic signatures: whether electronic records and signatures have the same legal effect as their physical counterparts, and whether there are any specific requirements in order to make electronic records and signatures recognized legally. The Act therefore addresses these two issues, by focusing on the legal effect and the legal requirements of electronic records and e-signatures, which we discuss in the following sections.

Electronic records: the main principles

Legal definition and effect

The Act provides that an electronic record is 'a record kept in electronic form, and can consist of text, sound, a picture, an image, symbol, or other information generated via electronic or other means not directly recognizable by human perception, and capable of conveying its intended information'.[8]

Electronic records can be used with a legal effect as a declaration of intent, but only when there is consent from a counterparty.[9] For example, when two parties wish to set up a contract, the law requires both parties to 'reciprocally declare their concordant intent, expressly or impliedly'.[10] According to Taiwan's Civil Code, such intent can be declared either orally, in the presence of the other party,[11] or remotely, that is not in the presence of the other party.[12] As electronic records can be transmitted around the internet, they are contained in a medium that is different from traditional declaration methods. Whether electronic records can be deemed as a declaration of intent is a primary issue, and the Act requires that this should be based on consent. In other words, the other party's consent is a prerequisite in order to employ electronic records with a legal effect of a declaration of intent, and such consent can be either directly expressed or indirectly implied. Once the consent to using electronic records is established, the parties are not obliged to supplement electronic records with other means of communication.[13]

In certain circumstances, the law may explicitly require a transaction to be made in writing. An example is the title transfer of real estate, which must be made in the form of a written document.[14] The written document, however, can be in electronic form, if, according to the Act, the following are met:[15]

1. The content of the information can be presented in its integrity.
2. The content remains accessible for subsequent reference in the future.
3. The other party gives their consent.

Here the use and effect of an electronic record is not only based on consent, but also enhanced by ensuring its integrity and accessibility. These three criteria – consent, integrity and accessibility – are repetitively mentioned throughout the Act and form the fundamental elements of legalizing the status and effect of electronic records and e-signatures. The three criteria can also be understood as the central principles of the Act.

In some other situations, the law may request that the parties provide a document in its original form. For instance, the court may request that parties provide private documents as evidence in a civil case. The parties are required, according to the provisions of article 352, paragraph 2 of the Civil Procedure Code,

[7] In one case concerning buying stocks online, the plaintiff contested that he did not make the transaction order. While he failed to point out who actually impersonated him, the court still ruled in his favour because the defendant (the securities company) did not provide enough evidence to prove that its system was sufficiently secured (Taiwan Hsinchu District Court, 90-Su-734, 22 May 2002). In another case with similar dispute regarding an online money transfer, the claim against the bank was rejected, because the bank proved that the contested transfer was based on fraud of the third party (Taiwan High Court, 92-San-313, 11 June 2003). We also note that in most cases related to internet transactions in Taiwan, the main issues are usually not directly relevant to the legal status of electronic records or e-signatures.

[8] Article 2(1).

[9] Article 4, Paragraph 1.

[10] Article 153, Paragraph 1 of the Civil Code.

[11] Article 94 of the Civil Code.

[12] Article 95 of the Civil Code.

[13] In an interesting case concerning a stock transaction dispute, the investor argued that she did not receive confirmation in paper form after she made her order online. The court ruled that the bank did provide confirmation through electronic records, and was not obliged to provide further confirmation by post or by telephone (Taiwan High Court Taichung Division, 103-San-95, 15 October 2014).

[14] Article 758, Paragraph 2 of the Civil Code.

[15] Article 4, Paragraph 2.

to provide an original copy of the document to the court. A deposit of the original document can be satisfied by providing an electronic record if the following three elements are met:[16]

> 1. The document was originally generated in electronic form (which implies consent at the time when the document was generated).
>
> 2. The content of the document can be presented in its integrity.
>
> 3. The content of the document remains accessible for subsequent reference.

This rule includes all the criteria mentioned above. However, it should be noted that the rule does not apply to situations where verification of handwriting, seals, or other methods for authenticating the integrity of a document are required, or when there is a law or regulation that stipulates otherwise.[17]

Finally, there are some documents that must be kept for a certain period of time or permanently, as required by law or regulation. To illustrate, article 38 of the Business Entity Accounting Act provides that accounting documents must be kept for at least five years after completion of annual closing procedures, except for documents related to unsettled accounting events, which should be retained permanently. This requirement can also be satisfied with an electronic record, if, again, the content of the document can be presented in its integrity and remains accessible for subsequent reference.[18] More specifically, the use of electronic records in this case is only limited to the kind of record that, together with its main content, has information regarding its dispatching or receiving locations, date or other information or data that can verify and serve to authenticate the content of the record.[19] In other words, the two criteria of integrity and accessibility are enhanced for this type of electronic record intended for archival purposes, by requiring additional data that can prove its authenticity in the future. However, as noted by some commentators, the long-term conservation of electronic records can be challenging, and legal requirements should take into account of specific technical design and solutions for electronic archiving.[20] There is certainly room for improvement for Taiwan law to develop a more detailed understanding of data integrity and accessibility.

The effective time of electronic records

Generally, an oral expression of intent becomes effective at the moment the other party understands the expression of intent.[21] An expression of intent in writing becomes effective the moment when the notification of the expression reaches the other party.[22] However, the law in Taiwan also differs in the method and the effective time of sending an electronic record from the traditional method (such as sending a notification by post). The Act stipulates that the time of dispatching an electronic record occurs 'when it enters the information system outside the control of the originator, unless otherwise agreed to between the parties or prescribed by government agencies'.[23] For the time of receiving an electronic record, it is determined by the following rules:[24]

1. If the addressee has designated an information system for the purpose of receiving electronic records, the receipt occurs at the time when the electronic record enters the designated information system; or if the electronic record is sent to an information system that is not the designated one, at the time when the electronic record is retrieved by the addressee.

2. If the addressee has not designated an information system, the receipt occurs at the time when the electronic record enters an information system of the addressee.

The idea that an electronic record is 'entering into an information system' reflects a linear understanding of data transmission, which is in fact similar to traditional methods. A rather linear definition might face challenges in digital transactions using new technologies, such as cloud or blockchain-based communications. The current definition of the 'information system' of the Act is broad and does not provide any particular criteria to distinguish one system from another.[25] Instead of using the concept of 'enter' to define the time of dispatching and receipt of electronic records, it might make better sense for

[16] Article 5, Paragraph 1.
[17] Article 5, Paragraph 1, Sentence 2.
[18] Article 6, Paragraph 1.
[19] Article 6, Paragraph 2.
[20] Stefanie Fischer-Dieskau, and Daniel Wilke, 'Electronically signed documents: legal requirements and measures for their long-term conservation', 3 *Digital Evidence and Electronic Signature Law Review* (2006), 40 – 44.
[21] Article 94 of the Civil Code.
[22] Article 95 of the Civil Code.
[23] Article 7, Paragraph 1.
[24] Article 7, Paragraph 2.
[25] Article 2(8): 'Information system means a system that produces, dispatches, receives, stores or processes electronic data through other methods'.

the law to focus on the control and accessibility of the senders and recipients to determine the effective time of electronic transactions.

Electronic and digital signatures

Two different ways of e-signing in Taiwan

To discuss the legal requirements of an e-signature, it is important to understand the legal nature of a signature in general. One of the purposes of a signature is to provide evidence that demonstrates the intention of the signatory to authenticate the document.[26] More specifically, a signature is capable of providing evidence for the identity of the signatory; the intention to sign, and the fact that the signatory has adopted the contents of the document.[27]

In principle, the various forms of electronic signature and digital signatures, once their legal requirements are fulfilled, will provide the same legal effect in terms of evidence and authentication as traditional signatures.

An e-signature is data with a specific legal value in terms of evidence that is linked with an electronic record. In Taiwan, the Act distinguishes between two types of e-signatures: 'electronic signatures' and 'digital signatures'. An electronic signature, according to the Act, is 'data attached to and associated with an electronic record, in order to identify and verify the identity or credential of the signatory and the authenticity of the electronic record.'[28] A digital signature means 'an electronic signature formed through transforming an electronic record into a certain length of digital data by mathematical algorithm or other methods and encrypted with a private key of the signatory, which can be verified by a public key.'[29] A digital signature is considered a special kind of electronic signature, but instead of simply 'e-signing' on an electronic record in a more straightforward fashion (such as typing on or attaching a signature to the electronic version of a document), a digital signature is capable of encrypting a document or authenticating an electronic record (or both encrypting a document and authenticating data) through specific electronic methods.[30]

A digital signature in Taiwan law is therefore similar to the 'advanced e-signature' or 'qualified electronic signature' in other jurisdictions.[31] However, it should be noted that electronic and digital signatures essentially do not provide extra 'legal value' – the legal effect of signing (be it a traditional signature or e-signing) remains the same. What matters is the issue of security and the weight of the evidence to prove a signature was affixed. More importantly, as will be discussed below, the rules of e-signatures reflect the three basic principles of consent, integrity and accessibility associated with the validity of electronic records.

Electronic signatures and additional consent

In general, parties can choose freely how they wish to sign contracts, and using electronic signatures should provide the same legal protections as traditional signatures. In certain circumstances, however, the law may stipulate that a signature or seal is required for a record to be legally valid (such as the example of a real estate title transfer mentioned earlier). According to the Act, in such a situation, electronic signatures can be used only when the other party (or parties) agree.[32] This is again based on consent, and in a sense this is a 'double-consent' – the parties need to first agree on using electronic records for the transactions (as discussed previously), and then agree to use electronic signatures to sign electronic records.

In practice, such additional consent for e-signing is often already implied when the parties agree to conduct transactions or to communicate based on electronic records. The fact that Taiwan law continuously emphasizes the role of consent seems to suggest that 'e-signing' is usually not the default option for signing a document. Moreover, the Act also regulates that the competent authorities can exclude the use of electronic signatures or to impose

[26] Tim Travers, 'On-line signing made simple'.
[27] Chris Reed, 'What is a Signature?' (2003) 3 *The Journal of Information, Law and Technology*, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/; for a more detailed list of purposes, see Stephen Mason, *Electronic Signatures in Law*, 8 – 10.
[28] Article 2(2).
[29] Article 2(3).
[30] For a more detailed discussion about digital signatures in general, see Stephen Mason, *Electronic Signatures in Law*, chapter 7.
[31] For example in the European Union, a qualified electronic signature is defined in article 3(12) of 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, p. 73–114. For a discussion under the Directive that is now repealed, see Paweł Krawczyk, 'When the EU Qualified Electronic Signature Becomes an Information Services Preventer', 7 *Digital Evidence and Electronic Signature Law Review* (2010), 7 – 18.
[32] Article 9, Paragraph 1.

additional requirements on their use.[33] For example, according to the provisions of article 14 of the Security and Exchange Act, company chairpersons, managers, and accountants are required to sign or seal financial reports. Theoretically, this could be done electronically, but the Financial Supervisory Commission has issued a rule forbidding the use of electronic signatures for these matters. Similarly, the Ministry of Foreign Affairs has also promulgated regulations excluding the use of electronic signatures and electronic records for passport and visa applications.

While the requirement of 'extra' consent and the exclusion of e-signatures in certain areas can be justified, the regulatory environment in general seems to demonstrate a fundamental distrust of electronic signatures. This might be a matter of policy choice, but a distrust in the public sector can shape the behaviour of the private sector. Although there are several electronic certification technologies available that provide for a reasonably safe means of authentication, the Act recognizes and focuses only on the use of encryption keys (i.e. digital signatures discussed below). As Taiwan is poised to provide a relatively secure e-signing environment, the language and regulatory intensity of the Act still has, it is suggested, room for further improvement.

Digital signature and certification requirements

The Act establishes digital signatures as a special e-signing system and stipulates several legal requirements on its use. To elaborate, a digital signature can have the same legal effect as a traditional manuscript signature, if it meets the following requirements:[34]

> 1. It utilizes a certificate issued by an authorized Certification Authority.
>
> 2. Such certificate is still valid and has not exceeded the scope of its utilization.

Here, the term 'certificate' means 'a form of electronic attestation that links signature-verification data to a person and confirms the identity and attribute of that person'.[35] In a typical scenario of online shopping, the online shop (or the online market platform as a whole) will set up a public key infrastructure (PKI), which is certified by a certification authority. The certificated PKI manages all public-private key pairs between the shop and its customers: a customer can thus sign electronically, using her private key, and her digital signature can be verified though the public key of the shop. Certificates and certification authorities are thus of critical importance for the compliance and transaction security of this system.

The Act also regulates the issuance of digital signature certificates and the qualification of certification authorities. A certification authority can be either a public agency or a private juridical person, but it has to be first authorized by the competent authority (the Ministry of Economic Affairs) before it can effectively provide certification services.[36] In addition, the competent authority may grant permission, under the principle of reciprocity and equivalent security requirements, to foreign certification authorities organized or registered pursuant to foreign law. Certificates issued by permitted foreign certification authorities shall be equivalent to those issued by domestic certification authorities.[37] The Ministry of Economic Affairs has also issued specific guidelines that regulate the practice of certification authorities.

The act establishes a fairly comprehensive framework to regulate the use of digital signatures with a PKI. The previously discussed requirements of 'integrity' and 'accessibility' are in a way considered to be satisfied by these regulatory controls. The technology of the digital signature and public-private key pairs has, in relative terms, matured. While it is not surprising that the Act emphasizes the use of digital signatures, the law might crowd-source the use and development of other alternative e-signing technologies, and thereby limit people's choices in terms of how to conduct business online.

Electronic vs digital signatures

A digital signature is a special kind of electronic signature that uses certificated data encryption methods. The question is whether digital signatures, by providing encryption through public-private key pairs, are always safer than electronic signatures in general. It is not necessarily so, because as mentioned, there are other types of encryption techniques available, but these are not specified in the Act, and hence fall into the general category of

[33] Article 9, Paragraph 2.
[34] Article 10.
[35] Article 2(6).
[36] Article 11.
[37] Article 15; further requirements can be found in the Regulations Governing Permission of Foreign Certification Authorities.

electronic signatures. However, for the sake of discussion, let us assume that electronic signatures only refer to 'plain' e-signing methods, i.e. such as scanning a signed manuscript or typing a name in an electronic record. The issue is how businesses and individuals should choose between simple electronic signatures and digital signatures.

To answer this question, the risk analysis framework provided by Casamento and Hatfield is helpful, by looking at six different types of risks: authentication risk, repudiation risk, admissibility risk, compliance risk, adoption risk and relative risk.[38] Each type of risk should be assessed independently, and while using digital signatures may reduce certain risks, it could increase some others. For example, digital signatures might possess a lower authentication risk, but it is still possible for someone to steal an account and impersonate the signing party.

The benefits of digital signatures are much clearer in terms of repudiation and admissibility risk. Digital signatures can significantly reduce these risks, because a PKI can safeguard the coherency and integrity of an electronic transmission, and a comprehensive regulatory framework can guarantee its admissibility before the court. On the other hand, using digital signatures increase compliance and adoption risks, because they are more technically complex and involve other regulations and certification authorities. Finally, relative risk takes into account case-specific issues, such as trust between the contractual parties and the overall internet infrastructure.

There is no easy and absolute answer to the above question. While digital signatures and other types of qualified electronic signatures provide additional security measures, they tend to be costly and, as Krawczyk suggests, eventually hinder digital transactions.[39] The choice between using electronic signatures, digital signatures or traditional signatures is about comparing costs and benefits of different options and making a rational business decision. The purpose of the law here is to provide clear legal definitions and guidance, but not additional regulatory controls.

Conclusion

Taiwan's Electronic Signature Act seeks to standardize the use of electronic records and e-signatures, establish a certification regime for digital signatures, and promote the development of e-commerce. The Act creates a safer and more reliable transaction framework, reduces the possibility of forgery, and allows the parties to confirm their identities and consent. However, the Act has the potential for increasing transaction and compliance costs, and offering a relatively concise but unclear explanation of the legal status of electronic signatures.

It is intriguing that the Act actually places so much attention to the legal status and effect of electronic records (about one-third of its articles) and concentrates on three major criteria, i.e. consent, integrity and accessibility. The rules of electronic signature and digital signature further strengthen the aspect of consent and integrity, and accessibility, respectively. The Act, in this sense, can be understood as a kind of principle-based regulation, which focuses on the outcomes rather than the detailed rules.[40] Although this paper raises several issues for future reforms, we also recognize that the law of e-signature in Taiwan provides an interesting legal framework and regulatory lens for the scholarship of digital law in general and the discussion of electronic signatures in particular.

Po-Hsiang Ou is an associate at Eiger in Taipei. He specialises in administrative law, dispute resolution and regulatory compliance. He finished his Ph.D on E.U. law and transnational regulation at Oxford University in 2015, serving at the European Commission on legal issues related to food safety and genetically modified products.
ph.ou@eigerlaw.com

Alex Tsai is an experienced litigator who specialises in white collar crime, especially in relation to violations against Taiwan's Securities and Exchange Act. He also works on regulatory and compliance matters, including in the areas of e-commerce, data protection and privacy and payment solutions.
alex.tsai@eigerlaw.com

Nathan Kaiser is a founding partner of Eiger, a Greater China-focused firm with offices in Shanghai and Taipei. A Swiss national, he has over a decade of professional experience, advising clients in all matters pertaining to investments, corporate law, commercial trade, employment law and commercial disputes.
nathan.kaiser@eigerlaw.com

[38] Greg Casamento and Patrick Hatfield, 'The Essential Elements of An Effective Electronic Signature Process'.
[39] Paweł Krawczyk, 'When the EU Qualified Electronic Signature Becomes an Information Services Preventer'.
[40] Julia Black, 'The Rise, Fall and Fate of Principles Based Regulation' (2010) *LSE Law, Society and Economy Working Papers*, available at https://www.lse.ac.uk/collections/law/wps/WPS2010-17_Black.pdf .