Articles

Electronic Form Over Substance: eSignature Laws Need Upgrades

LOTHAR DETERMANN[†]

Most professionals favor substance over form. Yet, with respect to form itself, more and more favor electronic form over substantive media and signatures. Companies, consumers, and governments increasingly use electronic communications, documents, and signatures instead of ink and paper. The COVID-19 pandemic has further accelerated an existing shift to digitization. Yet, many remain unsure about the legality or effectiveness of different forms of electronic signatures and find laws on the subject confusing.

Transactions, documents, and signatures are separate concepts. Transactions and other legally relevant actions, decisions, and declarations can be recorded in documents and effectuated with signatures. Documents and signatures can be created or copied electronically or in other formats. Transactions, actions, decisions, and declarations on the other hand exist in the abstract and independent of the electronic or other form in which they may be documented or signed.

In practice, people commonly ask whether electronic signatures are legal. But, the more relevant questions to ask are whether electronic signatures are effective and binding; whether they meet statutory form requirements; whether they protect interests as well as handwritten signatures on paper documents; and whether one is required to create, obtain, or retain paper documents with handwritten signatures in addition to electronic records and signatures. To better answer these and other questions, one has to consult not only newer laws specifically regulating electronic signatures and documents, but also older laws prescribing form requirements. Many older laws do not contemplate modern technologies and therefore do not give clear answers as to whether one can satisfy form requirements electronically.

[†] Lothar Determann teaches computer, internet, and data privacy law at Freie Universität Berlin, University of California, Berkeley School of Law, and University of California, Hastings College of the Law, San Francisco, and he practices technology law as a partner at Baker McKenzie LLP in Palo Alto, California. Opinions expressed in this Article are those of the Author, and not of his firm, clients, or others. The Author is grateful for the valuable input, research, and edits by Michael Bailey, Tania Bukhari Benz, Arian Grüner, Damian Jurrens, and Ted Karch.

Numerous different form requirements apply in myriad use cases and jurisdictions with respect to particular transactions, documents, and signatures. Legal and political uncertainties hinder adoption of electronic signature products and global harmonization of applicable laws. Existing laws are complex, confusing, and diverse due to historic factors. As electronic signatures, documents, and records were first adopted more broadly, lawmakers were uncertain regarding the purposes of existing form requirements, how well electronic signatures can address purposes of form requirements, which technologies will be adopted by businesses and consumers, and what legal problems could arise from forgeries. Additionally, lawmakers had reason to be concerned that businesses and consumers would need some time to adapt to new technologies and realize and handle the binding effect of electronically issued declarations. These considerations may have provided a valid excuse in the mid-1990s for somewhat timid, complex, and consciously incomplete and experimental legislation, but twenty years later, they no longer do. It is time for change.

Lawmakers can and should improve electronic signature laws and harmonize them internationally with clearer default rules favoring electronic form; detailed whitelists enumerating transactions that can be concluded with electronic documents and signatures; possibly blacklists specifying additional form requirements for particular use cases; less complex definitions; and clear conflicts of law rules, ideally permissive ones, possibly paired with bilateral or multilateral recognition or adequacy arrangements to drive international harmonization. At the same time, lawmakers should abandon overly prescriptive regulations that require "qualified electronic signatures" certified by nationally licensed providers, because such constructs have not been widely adopted in the last twenty years and seem to stand little chance or need of being adopted going forward.

This Article analyzes the current landscape, applicable legislation, and options for change. Following an introduction, this Article clarifies terms and definitions in Part I, reviews the history and rationale of form requirements outside the electronic sphere in Part II, compares the advantages and disadvantages of electronic signatures and documents in Part III, examines basic approaches for legislation and their potential impact on public and individual interests in Part IV, describes and compares current electronic signature legislation in key jurisdictions in Part V, examines effects of international divergence in Part VI, proposes policy arguments for changes in Part VII, and concludes with a summary.

TABLE OF CONTENTS

INTRODUCTION

Accountants, attorneys, engineers, and most other professionals generally favor substance over form.[1] But with respect to form, more and more favor *electronic* form over *substantive* media and signatures: companies, consumers, and governments increasingly use electronic communications, documents, and signatures instead of ink and paper.[2] At the same time, many remain unsure about the legality and effectiveness of different forms of electronic signatures and documents[3] and find it difficult to understand applicable laws on the subject.[4] Even lawyers and judges are confused about the complex and divergent rules and regulations covering electronic signatures.[5]

Courts have been struggling with the topic for decades.[6] Legislatures started to tackle electronic signatures in the mid-1990s, when businesses and consumers rapidly began to embrace the Internet.[7] In new statutes, lawmakers

---

1. *See* John D. McGregor, *Form over Substance*, 6 J. OBJECT TECH. 9, 10 (2007); Steven Bragg, *Substance over Form Definition*, ACCOUNTINGTOOLS (Dec. 15, 2020), www.accountingtools.com/articles/what-is-substance-over-form.html.

2. SIMONA CAVALLINI, FABIO BISOGNI, DORIANO GALLOZZI, CLAUDIO COZZA & CLAUDIA AGLIETTI, STUDY ON THE SUPPLY SIDE OF EU E-SIGNATURE MARKET: FINAL STUDY REPORT 83 (2013), https://www.researchgate.net/publication/263304956_eSignature_-_Study_on_the_supply_side_of_EU_e-signature_market_-_Final_Study_Report_by_Formit (identifying two characteristics defining digital signature use in E.U. Member States in 2012: "[(1)] wider diffusion in large enterprises; [(2)] greater importance in the service sector, especially in the financial and insurance sector"); *see also* Bruno Deffains & Jane K. Winn, *The Effects of Electronic Commerce Technologies on Business Contracting Behaviors*, *in* GOVERNANCE, REGULATIONS AND POWERS ON THE INTERNET 344, 345 (Eric Brousseau, Meryem Marzouki & Cécile Méadel eds., 2012) (citing 2004 U.S. Census Bureau study reporting e-commerce accounts for $1 trillion, or 24%, of all transactions in the manufacturing sector and $800 billion, or 17%, of merchant sale transactions); MINISTER OF JUST. OF TURK., 30TH COUNCIL OF EUR. CONF. OF MINISTERS OF JUST., MODERNISING JUSTICE IN THE THIRD MILLENNIUM 1 (2010), http://www.e-justice.gov.tr/publication/ebook.PDF.

3. Renard Francois, Comment, *Fair Warning: Preemption and Navigating the Bermuda Triangle of E-Sign, UETA, and State Digital Signature Laws*, 19 J. MARSHALL J. COMPUT. & INFO. L. 401, 418 (2001) (critiquing E-sign's preemption provision as failing to provide clarity and stating that "[a] business has to make several educated guesses as to the meaning of [a state law's effect on section 7002(a)(1) of E-sign]"); Manuel Alba, *Order Out of Chaos: Technology, Intermediation, Trust, and Reliability as the Basis for the Recognition of Legal Effects in Electronic Transactions*, 47 CREIGHTON L. REV. 387 (2014).

4. Thomas J. Smedinghoff, *The Legal Challenges of Implementing Electronic Transactions*, 41 UNIF. COM. CODE L.J. 3, 9 (2008); UNCITRAL, PROMOTING CONFIDENCE IN ELECTRONIC COMMERCE: LEGAL ISSUES ON INTERNATIONAL USE OF ELECTRONIC AUTHENTICATION AND SIGNATURE METHODS, at 69, U.N. Sales No. E.09.V.4 (2009).

5. *See* JUDICIAL STUDIES BOARD, DIGITAL SIGNATURE GUIDELINES (2014) (providing U.K. judges with an explanation of the "practical aspects of electronic signatures"); ADOBE, A GLOBAL OVERVIEW OF ELECTRONIC SIGNATURES (2017), https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/dc_esignatures_global_overview_ue.pdf.

6. For early cases, see, for example, Howley v. Whipple, 48 N.H. 487, 487–88 (1869); Entores Ltd. v. Miles Far E. Corp. [1955] EWCA (Civ) 3, [1955] 2 QB 327 (Eng.); Shattuck v. Klotzbach, No. 011109A, 2001 WL 1839720, at *2–3 (Mass. Super. Ct. Dec. 11, 2001); Toghiyany v. AmeriGas Propane, Inc., 309 F.3d 1088, 1091 (8th Cir. 2002).

7. Hartini Saripan, *Electronic Signature Legislative Models: The Reappraisal of the 'Unfortunate' Divergence*, 3 MLJA 20 (2009) (describing, *inter alia*, that Utah, Washington, Missouri, Germany, Italy, Russia, and India as the first jurisdictions to craft electronic signature legislation; these jurisdictions, modeled from the Utah statute, crafted prescriptive models of electronic signature laws that mandated uses of just one technology and set out an elaborate legal framework for rights and liabilities associated with electronic signature

focused on different aspects of the changes that electronic communication technologies brought to signatures, authentication, transactions, identification, contracts, records, and other aspects of commerce and public administration. This was evident in the diversity of names that legislatures gave their new statutes: for example, Utah passed a Digital Signature Act in 1995[8] while the State of Washington followed in 1996 with an Electronic Authentication Act.[9]

By now, most U.S. states have adopted versions of a model law named the Uniform Electronic Transactions Act (UETA),[10] which the U.S. Congress accepted and exempted from preemption in its federal Electronic Signatures in Global and National Commerce Act of 2000 (ESIGN).[11] Congress addressed in different titles of ESIGN electronic signatures, electronic records, electronic commerce, and online child protection measures.

Europe also began tackling the topic more than twenty years ago. In 1999, the European Community issued a Directive on a "framework for electronic signatures"[12] (Electronic Signature Directive) and a few months later a separate Directive on "certain legal aspects of information society services, in particular electronic commerce" (E-Commerce Directive).[13] In 2014, the European Union (E.U.) repealed and replaced the Electronic Signature Directive with a Regulation "on electronic identification and trust services for electronic transactions," also known as eIDAS.[14] In each of these laws, legislatures address the validity of electronic signatures with diverging focus and scope, as indicated in statutory titles that include terms such as electronic, digital, transactions, commerce, authentication, identification, and trust services.

---

transactions); UNCITRAL, MODEL LAW ON ELECTRONIC SIGNATURES WITH GUIDE TO ENACTMENT, at 7, U.N. Sales No. E.02.V.8 (2001); Stephen E. Blythe, *Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enhanced Security*, 11 RICH. J.L. & TECH., Winter 2005, at 1, 2.

8. UTAH CODE ANN. §§ 46-3-201 to 46-3-504 (repealed 2006). For further details, see R. Jason Richards, *The Utah Digital Signature Act As "Model" Legislation: A Critical Analysis*, 17 J. MARSHALL J. COMPUT. & INFO. L. 873, 874–75 (1999).

9. Washington Electronic Authentication Act, ch. 250, 1996 Wash. Sess. Laws 1190 (codified at WASH. REV. CODE §§ 19.34.010–19.34.903 (repealed 2019)).

10. Illinois and New York are the only states that have not adopted UETA. Both have promulgated statutes that govern electronic documents and signatures. For an example of a state statute adopting UETA, see CAL. CIV. CODE §§ 1633.1–1633.17 (West 2021).

11. 15 U.S.C. § 7002.

12. Directive 1999/93/EC, of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures, 2000 O.J. (L 13) 12.

13. Directive 2000/31/EC, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), 2000 O.J. (L 178) 1.

14. Regulation (EU) 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, 2014 O.J. (L 257) 73 [hereinafter eIDAS]. The European Union uses the acronym eIDAS, whereby "e" stands for electronic, "ID" for identification, "A" for authentication, and "S" for trust services. *What Is the eIDAS Regulation?*, ICO, https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/ (last visited May 21, 2021).

In addition to specific laws pertaining to electronic signatures, many legislatures, regulators, agencies, standard-setting bodies, and businesses around the world have formulated and adopted many other laws, regulations, and rules specific to forms for government elections, official documents, online platforms, and applications for permits, tax records, invoices, and many similar and other topics.[15] Most of these provisions are both complex and specific, so much so that a business or consumer wishing to know whether a certain signature, transaction, or document requires ink and paper to be effective or to protect one's interests adequately cannot easily find a simple answer in any one statute or even determine which statute will answer the question. Worse, after consulting a number of potentially applicable statutes, one finds the variations in terminology and methods of rulemaking unnecessarily confused and confusing.

In fact, the various laws on electronic signatures, contracts, commerce, and transactions around the world and even within jurisdictions have little in common, except a heavy use of words like "electronic" or "digital" in the titles and statutory definitions, complex constructs including double or triple negatives, and an absence of simple and unambiguous rules. For example, instead of prescribing that "a record in electronic form shall be effective," Congress mandated in ESIGN only that "a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form."[16] In the Electronic Signature Directive, the European Community created harmonized definitions and ordered its Member States to recognize advanced electronic signatures that meet certain additional requirements like handwritten signatures, but did not provide businesses and consumers with a list of contracts, records, or transactions that they can conclude with electronic signatures. eIDAS did not provide such lists, either, but instead added more and more complex definitions and licensing regimes for "trust services providers," meaning organizations that offer "creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates."[17]

One can excuse deficiencies in UETA, ESIGN, and the Electronic Signature Directive by pointing to the fact that these constituted first attempts to address a then relatively new and rapidly evolving phenomenon. But, when the European Union enacted eIDAS fifteen years after the Digital Signature Directive, it still failed to provide clear and unambiguous answers to basic questions regarding the effectiveness and validity of electronic signatures. Questions of effectiveness and validity in the U.S. context also remain unclear.

---

15. For an overview, see *eSignature Legality Guide*, DOCUSIGN, https://www.docusign.com/how-it-works/legality/global (last visited May 21, 2021); ADOBE, U.S. GUIDE TO ELECTRONIC SIGNATURES (2020), https://www.adobe.com/content/dam/dx-dc/pdf/ue/adobe-sign-us-guide-e-signatures-wp-ue.pdf; ADOBE, *supra* note 5.

16. 15 U.S.C § 7001(a)(1).

17. *See* eIDAS, *supra* note 14, art. 3(16), (19).

Two decades after President Clinton signed ESIGN into law with an electronic signature, it is time for change.

This Article analyzes the current legal landscape of electronic signatures, applicable legislation, and options for change. Part I of this Article clarifies terms and definitions, Part II reviews the history and policy objectives of form requirements outside the electronic sphere, Part III compares the advantages and disadvantages of electronic signatures and documents, Part IV examines basic approaches for legislation and its potential impact on public and individual interests, Part V describes and compares current electronic signature legislation based on research in more than sixty jurisdictions, Part VI examines the effects of international divergence in these regulatory schemes, Part VII proposes and discusses policy arguments for change, and the Article concludes with a summary.

I. TERMS

Most of us find concepts such as signatures, records, documents, and transactions relatively abstract topics. Adding new technologies and statutory definitions to topics that are already difficult to grasp exponentially increases the level of complexity. E.U. legislators defined forty-one technical terms in the eIDAS regulations with numerous cross-references and inaccessible jargon.[18] Before one tries to navigate the global jungle of statutory definitions in electronic signature laws, it will help, for orientation purposes, to recall basic concepts and plain language terms and meanings.

A. SIGNATURES

Humans have been using signatures in various forms and for different purposes for thousands of years.[19]

1. Plain Language Meanings

A signature is "the name or mark of a person, subscribed or printed by himself, or by his direction."[20] People sign contracts, judgments, laws, applications, notices, and other legal documents as well as personal letters, paintings, and other items. By applying a signature to an item, a person can declare authorship or agreement, depending on the context. Chefs mark signature dishes with particular designs, spices, or preparations.[21] Serial killers

18. *Id.* art. 3.

19. Autograph signatures date back to 3100 B.C. on Sumerian clay tablets. *See* Jeremy Norman, *Pictorgraphic Lexical Lists from Sumer Contain the Earliest Autograph Signatures*, HIST. OF INFO., www.historyofinformation.com/detail.php?entryid=2614 (last visited May 21, 2021).

20. *Signature*, THE LAW DICTIONARY (7th ed. 2002).

21. *Superstar Chefs' Signature Dishes*, FOOD & WINE (May 5, 2017), www.foodandwine.com/slideshows/superstar-chefs-signature-dishes.

mark victims or crime scenes.[22] Athletes and dancers can mark their physical performance with a "signature move," motion, or technique particular to them.[23] In each case, the signatory establishes a connection between her person and the signed item. Other persons can rely on the signature to identify the signatory and confirm the authenticity of the item and its connection to the signatory.

2. Handwritten Names, Symbols, Chops, Seals

Many people today use their first and/or last names as their signature. The traditional ink-on-paper signature is often referred to as a "wet signature," a holdover from when the ink needed time to dry.[24] A signature can also be printed, engraved, or stamped.[25] Celebrities and illiterates use symbols or abbreviations.[26] Bishops sign with a cross.[27] Government officials and company representatives use chops or stamps to sign on behalf of legal entities. A chop is "a seal or official stamp or its impression; a license validated by a seal; a mark on goods or coins to indicate nature or quality;"[28] these have been used in China for thousands of years.[29]

Today, chops are still common in some East Asian jurisdictions. In Taiwan, chops are required by law for certain transactions.[30] In Macau, chops are not required by law, but as a practical matter companies often use them, and there

22. Katherine Ramsland, *Serial Killer Signatures*, PSYCH. TODAY (Dec. 4, 2013), www.psychologytoday.com/us/blog/shadow-boxing/201312/serial-killer-signatures.

23. An example is Usain Bolt's "bolting" victory sign. *See* Adarsh Vinay, *What's the Story Behind Usain Bolt's Signature Celebration?*, SCOOPWHOOP (Aug. 15, 2016, 12:59 PM), https://www.scoopwhoop.com/Usain-Bolt-Signature-Celebration/. For particular shots in tennis, see Sivaraml, *The 'Killer' Shots in Tennis*, SPORTSKEEDA (Mar. 13, 2012), https://www.sportskeeda.com/tennis/the-killer-shots-in-tennis.

24. *Wet Signature: Everything You Need to Know*, UPCOUNSEL, https://www.upcounsel.com/wet-signature (last visited May 21, 2021).

25. *Signature*, FREE LEGAL DICTIONARY, http://legal-dictionary.thefreedictionary.com/signature (last visited May 21, 2021).

26. Skye Gould, Megan Willett-Wei & Mike Nudelman, *The 17 Coolest Signatures of Famous People Through History*, BUS. INSIDER (June 26, 2014, 1:02 PM), www.businessinsider.com/the-coolest-signatures-in-history-2014-6.

27. Irinaios Delidimos, *The Sign of the Cross in the Signatures of the Hierarchy*, PEMPTOUSIA (Sept. 18, 2017), https://pemptousia.com/2017/09/the-sign-of-the-cross-in-the-signatures-of-the-hierarchy/.

28. *Chop*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/chop (last visited May 21, 2021).

29. Qiu Gui Su, *Chinese Chops or Seals*, THOUGHTCO. (Jan. 30, 2019), https://www.thoughtco.com/chinese-chops-seals-2278409.

30. In Taiwan, an advanced electronic signature (AES) can serve as a company seal and personal chop. However, in filing for a company's registration with the Department of Commerce, Ministry of Economic Affairs, it is required to have a company's seal and a responsible person's chop affixed in the registration recordation. The requirement cannot be met through using an electronic image of the artifact. *See* Matt Slater, *Taiwan Company Registration Form—An Introduction*, CHINA CHECKUP (June 27, 2018), www.chinacheckup.com/blogs/articles/taiwan-company-registration-form; ELECTRONIC SIGNATURES ACT (2001) (Taiwan), http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=J0080037; ENFORCEMENT RULES OF THE ELECTRONIC SIGNATURES ACT (2002) (Taiwan), https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=J0080039; CIVIL CODE (2019) (Taiwan), https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=B0000001.

are common practices and conventions for their use.[31] Similarly, wax and lead seals embossed with an emblem, figure, symbol, word, or letter were once commonly used by corporations to sign documents. In the Middle Ages, documents were often closed with wax seals embossed with a mark that represented and identified the source of the seal.[32] In modern times, corporate seals are less common, but some jurisdictions still recognize them. In Nigeria, for example, every company was required to have a common seal, but legislation in 2020 rendered seals optional, and the company's articles of association regulate its use.[33]

3. Electronic and Digital Signatures

Just as physical signatures come in many flavors, so there are many electronic options, including typing one's name under an e-mail, applying a scanned image of a handwritten signature to a document, signing a paper document with ink and then scanning the document, adding a symbol or meme to a tweet or blog post,[34] or using one of many electronic signature or auto-pen products.[35] Referring to such electronic options, legislatures and companies use different terms and definitions, including "electronic," "digital," "simple electronic," "advanced electronic," and "qualified electronic" signatures.[36] Consumers are confused.[37]

The term "digital" means in everyday language that information is recorded or shown in the form of numbers, usually zeros and ones.[38] Yet, in the context of "digital signatures," the word "digital" is often used to refer to a subset of electronic signatures using a certain type of encryption technology.[39] The National Institute of Standards and Technology (NIST) defines a digital signature as "[t]he result of a cryptographic transformation of data that, when

31. *See, e.g.*, *Documents Required for Deposit Account Opening*, OCBC WING HANG BANK LTD. (Dec. 15, 2015), https://www.ocbcwhmac.com/chi/download/doc_required_for_ac_opening_en.pdf.

32. LAURA J. WHATLEY, A COMPANION TO SEALS IN THE MIDDLE AGES 1–2 (2019).

33. Companies and Allied Matters Act (2020) Cap. (B8), § 98 (Nigeria). Certain documents require signatures and a seal to be affixed for them to be legally enforceable. In addition, where the company's articles of association stipulate that the company's seal must be affixed to form a legally enforceable signature, the seal must be affixed.

34. Paul Gil, *What Is a Meme?*, LIFEWIRE, www.lifewire.com/what-is-a-meme-2483702 (June 22, 2020).

35. *See Electronic Signature Software*, SOFTWARE ADVICE, www.softwareadvice.com/electronic-signature/ (last visited May 21, 2021); *All E-Signature Products*, TECH. ADVICE, https://technologyadvice.com/e-signature-software/products (last visited May 21, 2021); *Who, What, Why: Are Machine-Written Signatures Binding?*, BBC (Jan. 21, 2015), https://www.bbc.com/news/blogs-magazine-monitor-30913121.

36. *See, e.g.*, eIDAS, *supra* note 14, art. 3; *see also* ADOBE, *supra* note 5.

37. *See, e.g.*, *The Difference Between Digital Signatures and Electronic Signatures*, SIGNiX (Jan. 2, 2013, 11:00 AM), www.signix.com/blog/different; Ostap, *What Is the Difference: Email Signature vs Electronic vs Digital Signature?*, NEWOLDSTAMP (Oct. 17, 2017), https://newoldstamp.com/blog/what-is-the-difference-email-signature-electronic-signature-and-digital-signature/.

38. *Digital*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/digital (last visited May 21, 2021).

39. Richards, *supra* note 8, at 879.

properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation."[40] Digital signatures often use encryption and multi-factor authentication to safeguard against forgery and to indicate if a document has been modified post-signature.[41]

Many jurisdictions recognize a distinct hierarchy of electronic signatures. Though the terminology can vary, most electronic signature laws around the globe recognize the differences between simple electronic signatures (as an umbrella term encompassing any electronic signature), advanced electronic signatures (which meet certain requirements regarding authentication and signatory identification), digital signatures (employing encryption technologies for added security), and qualified electronic signatures (meeting certain government-mandated or government-licensed requirements regarding the identification of signatories, authentication, and tamper-proofing, including dual-factor authentication and encryption).[42]

Modern technology has made authentication more sophisticated and complex. Instead of only using a name or a signature, multi-factor authentication strategies favor the use of several credentials to verify one's identity.[43] There are three main types of credentials: knowledge (for example, a password), possession (for example, an ATM card or a hardware authentication device), and

40. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., FIPS PUB. NO. 186-4, DIGITAL SIGNATURE STANDARD (DSS) 2 (2013), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

41. *See id.*

42. *See, e.g.*, Law No. 25,506, Dec. 11, 2001 (Arg.); Medida Próvisoria No. 2,200-2, de 24 de Agosto de 2001 (Braz.); Electronic Transactions Act (Cap. 196) (Brunei); Regissant les communications electroniques au Cameroun, loi no. 2010/013 du 21 décembre 2010 [Law on Electronic Commerce in Cameroon, Law No. 2010/03 of Dec. 21, 2010] (Cameroon); Law No. 19799 arts. 1–2, Marzo 25, 2002, DIARIO OFICIAL [D.O.] (Chile); L. 527/99, agosto 18, 1999, DIARIO OFICIAL [D.O.] (Colom.); Law No. 527, agosto 21, 1999 (Ecuador); Law No. 15 of 2004 (E-signature and Establishment of the Information Technology Industry Development Authority (ITIDA)), *al-Jarīdah al-Rasmīyah*, 12 Apr. 2004, art. 1 (Egypt); Recognition of Electronic Communications and Signatures Law (Guat.); Electronic Transactions Ordinance, (2000) Cap. 553 (H.K.); Electronic Signatures, 2001 (Act No. 28/2001) (Ice.); The Information Technology (Amended) Act, 2009 (India); Law No. 11 of 2008 on Electronic Information and Transaction (Indon.); Electronic Signature Law, 5761–2001 (Isr.); On Electronic Document and Electronic Digital Signature, 7 Jan. 2003, as amended (Kaz.); Dijiteol seomyeongbeob [Digital Signature Act] art. 2 (S. Kor.); Law of Electronic Documents and Signatures (Law No. 5/2005) (Mac.); Act 658, Electronic Commerce Act 2006 (Malay.); Act 562, Digital Signature Act 1997 (Malay.); Código de Comercio [CCom] [Commercial Code], Diario Oficial de la Federación [DOF] 07-10 al 13-12-1889, últimas reformas DOF 28-03-2018 (Mex.); Dep't of Trade & Industry & Dep't of Sci. & Tech., Admin. Ord. No. 02 (Sept. 28, 2001) (Phil.), https://lawphil.net/administ/jointdept/jdao_2_2001.html; Federal'nyĭ Zakon RF o elektronnaya podpis' [Federal Law of the Russian Federation on Electronic Signature], SOBRANIE ZAKONODATEL'STVA ROSSIĬSKOĬ FEDERATSII [SZ RF] [Russian Federation Collection of Legislation] 2011, No. 63-FZ, art. 5 (Russ.); Electronic Transactions Act (2010) (Sing.); Electronic Communications and Transactions Act 25 of 2002 (S. Afr.); Electronic Signatures Act (Taiwan); Electronic Transactions Act BE. 2544 (2001) (Thai.); Electronic Signature Law No. 5070 (Turk.); Electronic Digital Signature Law No. 852-IV (Ukr.); Documento Electrónico y Firma Electrónica [Electronic Document and Signature Act], Act No. 18.600, Sept. 21, 2009 (Uru.); Law No. 51/2005/QH11 of Nov. 29, 2005 on E-Transactions, art. 21.1 (Viet.).

43. *See generally* Elizabeth Kennedy & Christopher Millard, *Data Security and Multi-Factor Authentication: Analysis of Requirements Under EU Law and in Selected EU Member States*, 32 COMPUT. L. & SEC. REV. 91 (2016).

identity information (for example, biometric information such as a fingerprint).[44] For practical reasons,[45] often only one or two types of credentials are required to safeguard security.[46]

4. Legal Requirements and Functions

With respect to legal documents, signatures have three main functions: signatures associate the signatory with the content of a document (attribution function); make it possible to identify the signatory (identification function); and indicate personal involvement of the signatory in the act of creating or signing the document (evidentiary function).[47] The Uniform Commercial Code generally defines a signature as "using any symbol executed or adopted with present intention to adopt or accept a writing."[48] UETA defines a signature as "an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record."[49] ESIGN similarly defines a signature as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[50]

B. DOCUMENTS AND RECORDS

A record is an item—such as a piece of paper, disk, or a computer file—in which one stores information.[51] A document is a record that contains text.[52] Other records contain pictures, films, sound recordings, or computer logs. A signature is information in a document that attributes the document to its author or persons who agree with the document or acknowledge receipt.

Records exist separately from the information manifested in them. No one owns data, but people can own records.[53]

---

44. *Id.* at 93.

45. Hui Zhu et al. name Apple's fingerprint scanner as an example for the specific and costly hardware that is needed to provide reliable multi-factor authentication. *See* Hui Zhu, Xiaodong Lin, Yun Zhang & Rongxing Lu, *Duth: A User-Friendly Dual-Factor Authentication for Android Smartphone Devices*, 8 SEC. & COMMC'N NETWORKS 1213, 1214 (2015).

46. *See* Kennedy & Millard, *supra* note 43; *see also* Seth Rosenblatt & Jason Cipriani, *Two-Factor Authentication: What You Need to Know (FAQ)*, CNET (June 15, 2015, 1:39 PM), https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/.

47. *See* UNCITRAL, *supra* note 4, at 5; Susanna Frederick Fischer, *Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation*, 7 B.U. J. SCI. & TECH. L. 229, 231 (2001) ("Electronic signatures must serve the same essential functions as handwritten signatures, namely (i) *authentication*; (ii) *integrity*; and (iii) *non-repudiation*.").

48. U.C.C. § 1-201(37) (AM. L. INST. & UNIF. L. COMM'N 2020).

49. CAL. CIV. CODE § 1633.2(h) (West 2021).

50. 15 U.S.C. § 7006(5).

51. *Record*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/record (last visited May 21, 2021).

52. *Document*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/document (last visited May 21, 2021).

53. Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 42–54 (2018).

People can create records electronically from the outset, for example, by taking a photo with a digital camera or drafting a contract on a computer. People can also create electronic copies of physical documents, for example, by scanning a contract that was first typed on paper and hand-signed; in this case, the electronic record can serve as evidence that the contract was signed on paper originally. This can be important for legal purposes, if a hand-signed physical document is legally required but a court accepts an electronic copy as evidence for the existence of the required hand-signed, physical document.

C. TRANSACTIONS AND COMMERCE

In everyday language, people think of transactions primarily in the context of commerce, such as contracting, buying, selling, paying, and transferring ownership.[54] One can also document other legally relevant actions with ink on paper or electronically, including applying for permits, terminating contracts, and formalizing divorces, adoptions, indictments, lawsuits, judgments, court orders, and warrants.

Transactions or other legally effective actions are conceptually separate from the documents or records that document these transactions or the approvals or legally binding decisions of individuals who sign the records or documents. Despite titles such as UETA and eIDAS, which connect "electronic" as an attribute with "transaction," it is not a transaction that can be "electronic" or "physical," but rather it is the document or other record that effectuates the transaction and the signature that attributes a document or record to a person that can be "electronic" or "physical."

D. LEGALITY VERSUS EFFECTIVENESS

People commonly ask: are electronic signatures legal?[55] But this is usually not the right question. The terms "legal," "illegal," and "legality" indicate whether a person, item, or action complies with applicable laws.[56] A person can commit an illegal act by forging a signature, by signing a document on behalf of an entity without authorization, by creating an infringing copy of a record, or by writing libelous text in a document. One can violate these laws by forging or using either electronic or wet signatures. One can infringe copyright laws by reproducing works on paper or in electronic form. One can commit libel on paper or electronically. In each case, the legality of the actions does not typically depend on whether the person uses ink and paper or electronic technologies.

---

54. *See Transaction*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/transaction (last visited May 21, 2021).

55. *See, e.g.*, *Are Electronic Signatures Legal?*, DOCUSIGN (Mar. 20, 2020), https://www.docusign.com/blog/are-electronic-signatures-legal.

56. *See Legality*, MERRIAM-WEBSTER, www.merriam-webster.com/dictionary/legality (last visited May 21, 2021).

Moreover, one is generally not prohibited from using electronic signatures under any laws. The various laws on electronic signatures, transactions, and commerce are not usually concerned with permitting or prohibiting electronic signatures or records. Instead, such laws address the question whether signatures, contracts, documents, transactions, and other items meet certain form requirements as a condition for being legally effective and binding, and whether they constitute valid evidence in court or before authorities.

Thus, the better questions to ask are: are electronic signatures effective and binding?[57] Do electronic signatures and documents meet statutory form requirements? Do they protect interests as well as handwritten signatures do, on paper documents? Is one required to create, obtain, or retain paper documents with handwritten signatures in addition to electronic records and signatures? To better answer these—better—questions, one should consult not only newer laws specifically regulating electronic signatures and documents, but also older laws prescribing form requirements—many of which predate current technologies and practices. Such laws and their policy objectives are reviewed in Part II of this Article.

E. SUMMARY

Transactions, documents, and signatures are separate concepts. Transactions and other legally relevant actions, decisions, and declarations can be recorded in documents and effectuated with signatures. Documents and signatures can be created or copied electronically, whereas transactions, actions, decisions, and declarations exist in the abstract and independent of the electronic or other form of the documents themselves and the signatures. People create documents to record information. They sign documents and other items for purposes of attribution, identification, and evidence. Whether one should use electronic or other forms of documents or signatures does not depend on whether electronic documents or signatures are legal, but whether documents or signatures in the electronic form have the intended legal effects, constitute sufficiently robust evidence, and protect the signatory's interests. This in turn depends on form requirements established by statutes, common law, and industry norms.

II. FORM REQUIREMENTS—TYPES AND POLICY OBJECTIVES

Whether one signs a personal letter or painting depends largely on personal preferences and customs. With respect to legally relevant transactions or actions, however, one must observe form requirements in order to achieve the intended effects, in such circumstances as obtaining a government permit, creating an enforceable contract, validly terminating an employment relationship, or issuing a binding warrant. Legislatures, courts, government agencies, and businesses

57. *See Are Electronic Signatures Legal?*, *supra* note 55.

have created numerous form requirements (see Part II.A) for various purposes (see Part II.B).

A. TYPES OF FORM REQUIREMENTS

Contracting parties are required to document sales transactions in excess of certain value thresholds *in writing* under the statute of frauds rules in the U.S. Uniform Commercial Code.[58] Under German law, sales contracts for the transfer of ownership in real estate have to be read to the parties or their authorized representatives by a notary.[59] A transfer of ownership in German land is not valid until it is recorded in a government-operated land registry, a requirement also applicable in the United Kingdom and in Switzerland.[60] Legal transactions regarding the ownership of immovable property in Switzerland, such as the acquisition of purchase or pre-emption rights or certain gifts, must be recorded in the official land register by means of a public deed.[61] Certain contracts are valid only if the parties sign in front of witnesses[62] after obtaining advice from legal counsel[63] or before a court.[64]

Other form requirements apply in different contexts. For example, the incorporation of companies commonly must be recorded in the commercial register of their home jurisdiction.[65] In Switzerland, a company is established by means of a public deed and only acquires legal personality through entry in the

58. U.C.C. § 2-201 (AM. L. INST. & UNIF. L. COMM'N 2020).

59. Bürgerliches Gesetzbuch [BGB] [Civil Code], § 311b, https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.pdf (Ger.); Manfred Pieck, *A Study of the Significant Aspects of German Contract Law*, 3 ANN. SURV. INT'L & COMP. L. 111, 115 (1996) (noting under German contract law certain contracts—for example, establishment of a foundation, promise of annuity, and acknowledgement of a debt—must be in writing and require notarial or magistrate authentication).

60. Bürgerliches Gesetzbuch [BGB] [Civil Code], § 873 (Ger.); Actionstrength Ltd. v. Int'l Glass Eng'g [2003] UKHL 17, [2003] 2 AC 541 (appeal taken from Eng.); SCHWEIZERISCHES ZIVILGESETZBUCH [ZGB] [CIVIL CODE] Dec. 10, 1907, SR 210, RS 210, art. 656 (Switz.).

61. OBLIGATIONENRECHT [OR] [CODE OF OBLIGATIONS] Mar. 30, 1911, SR 2, RS 2, art. 216, art. 242, para. 2 (Switz.).

62. Such as wills, which are to be drawn in a public deed and require the attestation of two witnesses who also sign the deed. *See* SCHWEIZERISCHES ZIVILGESETZBUCH [ZGB] [CIVIL CODE], art. 501 (Switz.). This is also usually the case for a wedding, which requires the presence of two witnesses. *See* SCHWEIZERISCHES ZIVILGESETZBUCH [ZGB] [CIVIL CODE], art. 102, para. 1 (Switz.). Attestation is also usually required in the United States. *See, e.g.*, CAL. PROB. CODE § 6110-11 (West 2021); *see also Wills: Attestation Requirement*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/wills_attestation_requirement (last visited May 21, 2021); Mary Randolph, *The Witness Requirement to Execute a Will*, ALLLAW, https://www.alllaw.com/articles/nolo/wills-trusts/witness-requirement-execute.html (last visited May 21, 2021).

63. For example, under U.K. employment law, settlement agreements are invalid unless the employee sought advice from legal counsel, which employers will often pay for. *See* Joanne O'Connell, *Settlement Agreements: What Do Employees Need to Know?*, GUARDIAN (Aug. 7, 2013, 5:41 PM), www.theguardian.com/careers/settlement-agreements-employees-need-to-know.

64. Such as judicial settlements under Swiss law which must be signed in court. *See, e.g.*, SCHWEIZERISCHE ZIVILPROZESSORDNUNG [ZPO] [CIVIL PROCEDURE CODE] Dec. 19, 2008, SR 272, RS 272, art. 208, para. 1, art. 241, para. 1 (Switz.).

65. *See, e.g.*, DLA PIPER, GUIDE TO GOING GLOGAL: CORPORATE, SWEDEN 8 (2020), https://www.dlapiperintelligence.com/goingglobal/corporate/index.html?t=06-incorporation-process&c=SE (click "Download PDF" and select from dropdown "Download current countries" to download).

commercial register.[66] In the medical area, according to the California Confidentiality of Medical Information Act, an authorization for the release of medical information is valid if it is handwritten by the person who signs it or is in typeface larger than fourteen-point font.[67] With regard to employment, employers can only terminate employment contracts with German employees with a written notification of termination, which must be signed by the employer or its legal representative.[68] A prenuptial agreement under California law must be in writing and signed by both parties.[69] A will must be written by hand in order to be valid, or it must be signed by the testator and witnessed by at least two persons.[70] Promises of gifts are not binding in the United States, unless made in writing, so that the promisor's consideration is evidenced.[71] Contracts of guarantee in the United Kingdom must be given in written form in order to be valid and enforceable.[72] Under Swiss law, claims may only be assigned validly if done in writing.[73] In the context of a rental agreement, Swiss law requires the landlord to notify the tenant of the agreement's termination in writing and with a standard form, which informs the tenant of the tenant's rights.[74]

In addition to statutory form requirements, businesses often include form requirements in contracts, including for contract changes, notification of certain persons or departments at a company, and other formalities.[75]

B. PURPOSES AND POLICY OBJECTIVES OF FORM REQUIREMENTS

With statutory form requirements, lawmakers restrict individual freedom of contract and communications to pursue a number of different objectives, including the following:

1. Memorialization to Reduce Risks of Misunderstandings and Disputes

Writings reduce risks of unclear declarations, misunderstandings, faulty recollections, and, by extension, disputes.[76] Parties can remember and remind each other better of terms they document and retain in a record.

66. OBLIGATIONENRECHT [OR] [CODE OF OBLIGATIONS], art. 643, para. 1 (Switz.).
67. CAL. CIV. CODE § 56.11(a) (West 2021).
68. BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], §§ 126, 623 (Ger.).
69. CAL. FAM. CODE § 1611 (West 2021).
70. CAL. PROB. CODE §§ 6110–11 (West 2021).
71. George S. Geis, *Gift Promises and the Edge of Contract Law*, 2014 U. ILL. L. REV. 663, 671 (2014).
72. Actionstrength Ltd. v. Int'l Glass Eng'g [2003] UKHL 17, [2003] 2 AC 541 (appeal taken from Eng.).
73. OBLIGATIONENRECHT [OR] [CODE OF OBLIGATIONS], art. 165, para. 1 (Switz.).
74. *Id.* art. 266*l*.
75. For an example of a comprehensive notices provision requiring notices to a commercial contract to be in writing, see J. Gerard Legagneur, *Why Your Contract's "Notices" Provision Is Vitally Important*, NOLO, https://www.nolo.com/legal-encyclopedia/why-your-contract-s-notices-provision-is-vitally-important.html (last visited May 21, 2021).
76. UNCITRAL, *supra* note 4, at 14.

2. Evidence to Help Resolve Disputes Fairly

Courts often find clearer and more reliable evidence in written documents than in oral testimony. Signature requirements extend the evidentiary function of documents beyond the terms that were agreed to the identity of the persons who reached the agreement, prepared the document, or approved it.[77] Recipients of or other parties to a signed document receive additional information and evidence regarding the author or approver, which increases the reliability.[78] Witnesses serve an important evidentiary function in case parties or signatories dispute the authenticity of a document, for example by claiming coercion, incapacity, or forgery.[79]

3. Warning Individuals of Legal Significance

Anyone who is confronted with a signature requirement receives a warning and a call to attention regarding the legal significance of the document to be signed.[80] Requirements to write a will by hand, specifically, or to separately accept in writing particularly burdensome clauses in a contract by signing one's initials,[81] or to sign a declaration of consent to certain usage of personal data on a separate document elevate the warning function of signature requirements for the signatory who is alerted about the impact of her actions.[82]

4. Protecting Integrity of Documents and Transactions

In most jurisdictions, notaries are particularly reliable witnesses who have been trained or certified by governments. They can confirm the identities of parties (by checking government-issued photo IDs) and oversee and witness the signing process. In Germany, notaries are also obligated to prevent coercion or errors, explain unclear contract terms, or flag unconscionable contract terms and thus ensure a certain level of accuracy and integrity.[83]

5. Lend Authority to Documents

Government recording or approval requirements further elevate the evidentiary function of written documentation and signatures and lend additional authority to the recorded or approved transactions.[84]

---

77. UNCITRAL, *supra* note 7, at 35.

78. UNCITRAL, *supra* note 4, at 15.

79. *Id.* at 69.

80. UNCITRAL, *supra* note 7, at 35.

81. Italian law requires the separate writing of initials according to legislation on vexatious clauses, pursuant to C.c. art. 1341, para. 2 (It.).

82. UNCITRAL, *supra* note 7, at 35.

83. For a short summary of notarization in the United States, see *What Is Notarization?*, NAT'L NOTARY ASS'N, https://www.nationalnotary.org/knowledge-center/about-notaries/what-is-notarization (last visited May 21, 2021).

84. *Admissibility of Electronically Filed Federal Records as Evidence*, UPCOUNSEL, https://www.upcounsel.com/lectl-admissibility-of-electronically-filed-federal-records-as-evidence (last visited May 21, 2021).

6. Promote Trust

More broadly, all form requirements elevate the authority of documents in the interest of trust.[85] Trust is the backbone of civilization, peaceful society, and commerce.[86] Trust is required in any relationship, whether between individuals or between an individual and an institution. Humans are hard-wired, in an evolutionary sense, to critically evaluate risks and opportunities, and advantages and disadvantages of collaboration, and by implication, trust in others.[87] Since humans lived in small bands of hunter-gatherers, their very survival depended on their ability to navigate relationships by correctly placing trust in those who deserved it and withholding it from those who might have brought harm.[88] In the twenty-first century, many relationships in society are impersonal.[89] Trust remains critical as a basis for civilization, commerce, collaboration, and collective success.[90] As just one example, consumers are less inclined to buy goods if they do not trust the seller. Beyond the immediate concern of whether the goods would materialize after handing over payment, trusting that the seller would make things right in the event of a faulty product is also important. As people have moved from buying goods in physical stores operated by personally known merchants in small towns, to buying in large, impersonal malls, to now purchasing online, trust has remained important and becomes more difficult to obtain and maintain.[91]

When parties trust each other, they are more likely to enter into a cooperative arrangement—whether in the context of purchasing goods online, a mountaineering expedition, or leadership of a society via elected representatives. Where collaborating persons do not know each other personally, they have to trust in institutions and formal documentation of agreements and transactions.

7. Summary

Before the widespread adoption of electronic technologies and communications, lawmakers around the world had already established numerous types of form requirements, including written and handwritten form, witnesses, notarization, initialization of burdensome clauses, formal separation of important clauses, and recording in registers maintained by governments. All of these solutions were designed to promote trust, reduce risk of misunderstandings, reduce risks of disputes, create evidence to resolve disputes

85. UNCITRAL, *supra* note 4, at 6.

86. *See* eIDAS, *supra* note 14, recital 1, at 73.

87. Jack Barbalet, *A Characterization of Trust, and Its Consequences*, 38 THEORY & SOC'Y 367, 377 (2009).

88. *See generally* YUVAL N. HARARI, SAPIENS: A BRIEF HISTORY OF HUMANKIND (2011).

89. *See* Susan P. Shapiro, *The Social Control of Impersonal Trust*, 93 AM. J. SOC. 623, 634 (1987); Harvey C. Mansfield, Jr., *On the Impersonality of the Modern State: A Comment on Machiavelli's Use of* Stato, 77 AM. POL. SCI. REV. 849, 849 (1983).

90. Barbalet, *supra* note 87, at 377.

91. *See* eIDAS, *supra* note 14, recitals 1–69, at 73–81.

fairly, warn individuals of the legal impact of certain actions, protect the integrity of documents and transactions, and lend authority to formal documents. Now, lawmakers have to re-evaluate types and purposes of form requirements for the digital age.

III. ELECTRONIC FORM—ADVANTAGES AND DISADVANTAGES

Businesses, consumers, governments, and citizens appreciate and weigh numerous advantages and disadvantages of electronic signatures and documents, set out in the following Subparts.

A. SPEED, COST, AND CONVENIENCE

If multiple persons have to sign a document—for example a multi-party contract or a board resolution—circulating a paper document by mail or requiring all signatories to attend a signing ceremony takes time, creates scheduling inconveniences, and costs money. Circulating the same document by e-mail or a user-friendly online product takes seconds, is more convenient for signatories, and avoids travel costs. Similarly, companies and consumers embrace the efficiency of online shopping, electronic onboarding of new employees, policy rollouts by e-mail, online permit applications, electronic tax filings, and many other transactions that can be completed much faster and more efficiently electronically than with ink on paper.

B. DOCUMENT ANALYSIS, ARCHIVING, RETRIEVAL, AND RETENTION

Companies and consumers can archive, search, find, and ultimately delete electronically signed documents much more easily than paper contracts, with the help of automation software and search tools. They do not need to create, maintain, and move binders—which take up office space and are much harder to search. They can, for example, use computer programs to translate electronic documents into other languages within seconds, copy text from one document into another at low cost, and adapt it rather than having to rewrite it, and use a search function to find all documents containing a name or certain references within seconds—provided the text content of these documents is digital.

C. AUTHENTICITY AND INTEGRITY

Electronically signed documents can be stored with time stamps in file formats that are protected against tampering. Signature pages on physical paper can often no longer be found or clearly connected to a particular contract version or set of attachments when attorneys exchange signature pages separately for convenience. Sometimes, the wrong attachments are included in the final version of a contract. Or perhaps a party makes changes to the document just before its execution that go undetected. Frequently, a "battle of the forms" arises in the context of paper contracting programs because customers attach or include references to their own standard terms. Software companies that can prompt a

customer to click on a particular set of contract terms, on the other hand, tend to be in a better position to control and show what exactly a contract is comprised of and consequently improve document accuracy. Electronic signatures can tie these documents together and at the same time provide authentication.

Of course, electronic documents and signatures can also be forged. Anyone can type someone else's name on a signature page. With sophisticated software tools, even photos and videos can be manipulated in ways that are extremely difficult to detect.[92] The level of security varies with the technology that is used.[93]

Forging electronic signatures is not necessarily easier to do, detect, or prevent than forging handwritten signatures. Throughout human history, people have embodied their trust in written signatures and other physical marks which, at the same time, have always been susceptible to forgery. If one can successfully forge something as personal as a painting, forging signatures surely is trivial. Recall the cases of Frank Abagnale, Jr. (famous forger of checks),[94] Paul Ceglia (who claimed to own half of Facebook, Inc. based on a contract with a wet signature that was proven to have been fraudulently manipulated),[95] or Michael Avenatti (recently charged with fraud for forging the signature of his client, Stephanie Clifford, also known as Stormy Daniels, to send payments of nearly $300,000 to his accounts).[96]

Just as forgery has been a problem for wet signatures, electronic signatures can also present security issues. Nevertheless, electronic signatures do have the edge with respect to security. By fully leveraging available technology and benefitting from iterative technological progress, fraud can be prevented or at least proven more easily than with paper contracts, for example because subsequent changes to a file can be electronically detected.[97] Advances in automated learning and other technologies present great opportunities in this area.

---

92. Matt Beard, *To Fix the Problem of Deepfakes We Must Treat the Cause, Not the Symptoms*, GUARDIAN (July 22, 2019, 10:30 PM), www.theguardian.com/commentisfree/2019/jul/23/to-fix-the-problem-of-deepfakes-we-must-treat-the-cause-not-the-symptoms.

93. For an overview of potential security risks of electronic signatures, see A. Srivastava, *Electronic Signatures and Security Issues: An Empirical Study*, 25 COMPUT. L. & SEC. REV. 432 (2009).

94. FRANK W. ABAGNALE, JR., CATCH ME IF YOU CAN (1980).

95. Kashmir Hill, *Facebook Offers Court 'Smoking Gun' Against Paul Ceglia*, FORBES (Aug. 16, 2011, 10:18 AM), https://www.forbes.com/sites/kashmirhill/2011/08/16/facebook-offers-the-court-its-smoking-gun-against-paul-ceglia/.

96. Tom McParland, *Michael Avenatti Charged with Fraud, Stealing from Ex-Client Stormy Daniels in New Indictments*, RECORDER (May 22, 2019, 5:42 PM), https://www.law.com/therecorder/2019/05/22/avenatti-charged-with-defrauding-stormy-daniels-in-new-indictments/.

97. Benjamin Wright describes some of the risks of handwritten signatures that could be avoided by using electronic ones in Benjamin Wright, Eggs in Baskets: Distributing the Risks of Electronic Signatures 1 (Nov. 7, 1996) (unpublished manuscript), https://ssrn.com/abstract=15090.

D. IDENTIFICATION

If a person signs an e-mail or online form by typing their name, the recipient usually receives additional information that can identify the signatory, such as an e-mail address, IP address, time stamp, computer settings, or other information that is automatically transmitted or stored in the signed document. Depending on circumstances, this additional information can be more or less valuable for identifying the signatory than the person's handwritten signature. If the person uses qualified electronic signature technologies with dual-factor authentication and via an account with a government-licensed provider, the electronic signature will offer superior identification information than typical ink-on-paper signatures.[98]

E. EVIDENCE

Electronic signatures also facilitate the preservation of evidence. Companies can leverage commercially available technologies to preserve electronic records and documents, either to satisfy record-keeping requirements under tax and accounting rules or to prepare for potential disputes regarding contract validity. Traditionally, companies kept signed originals in secure locations, sometimes even with every page initialed. In practice, however, paper contracts have often fallen victim to being physically destroyed through fire or other means or being missing or lost. Increasingly, companies are satisfied with exchanging fax copies or scanned versions of signature pages, even where the signature is originally inked on paper. This practice, however, often creates uncertainties regarding the actual version of the contract terms that were finally accepted, and forensic experts cannot determine the authenticity of scanned or faxed copies with the same certainty as hand-signed originals.

F. REDUCE VARIETY AND DEVIATIONS IN STANDARD TERMS

In the context of electronic contracting, companies can create processes that automatically and cost-efficiently log the initial contract formation and keep track of electronic delivery. Even where companies rely on implied acceptance methods (for example, downloads), companies may be able to substantiate or prove contract formation on the basis that the process was set up in a certain manner and the licensee must have accepted the terms in order to have gained use rights in the first place, because downloading from a legitimate site involved the presentation and acceptance of license terms. Such evidence can be easily recorded, searched, and accessed.

Consumers find electronic contracting and signature processes convenient and readily click on often lengthy and complex contract terms that they may not

98. The German Bundesnetzagentur (the Federal Network Agency) has summarized the advantages of qualified electronic signatures. *See* BUNDESNETZAGENTUR, https://www.bundesnetzagentur.de/EN/General/Bundesnetzagentur/Bundesnetzagentur-node.html (last visited May 21, 2021).

fully understand.[99] They also do so on paper—for example, in the context of real estate purchases or when they rent a car at the airport—but electronic contracting and signature processes tend to make it even easier for companies to present contracts on a take-it-or-leave-it basis. Courts can correct resulting inequities based on doctrines such as contracts of adhesion, or unconscionability.[100] In the electronic sphere, companies can simulate the warning function of offline contracting ceremonies (such as having a notary read out the contract to the parties) by requiring consumers to click to accept particular contract terms (instead of initialing them on paper), scrolling through all contract terms on a screen, and separately clicking on a confirmation button declaring that they have read and understood the agreement or document that they are signing electronically. Alternatively, or additionally, a similar process can be conducted with video or audio explanations or recital of contract terms or certain legal aspects tied to the transaction in such a way that the contracting party must watch or listen before being able to click through. A short survey to conclude such a procedure could function as a confirmation and thus proof of the contracting party's attention and comprehension in order to secure the company against potential reproaches for having imposed take-it-or-leave it terms. There are thus numerous ways to ensure contracting parties' understanding of the legal transactions they conduct electronically, which might perhaps even prove more reliable on occasion than possibly unclear, rushed, or merely formalistic contracting ceremonies involving handwritten signatures, which also fail to verify or prove the contracting party's full understanding of a transaction.

Companies that present template contract forms on paper or via e-mail for the customer's signature often find that the customer feels inclined to negotiate the contract or present its own procurement contract templates, whereas prompting customers with simple "click through" options often results in shortened sales cycles as more customers tend to accept electronic contract terms followed by a "click to accept" button. Moreover, paper contracts tend to be concluded only with direct business partners, whereas software companies can bind even indirect resellers, authorized end users, and secondary purchasers if they integrate click-through terms in products; they can also require renewed acceptance at regular intervals, such as during updates, in order to ensure any later user of the software is also bound by their terms. Thus, software companies can impose contract terms not only on the initial license purchaser, but also successor entities and secondary purchasers when users try to resell or assign software. Doing this using wet signatures would be painstaking, but using electronic signatures facilitates this to a great degree.

---

99. *See* Aaron Perzanowski & Chris Jay Hoofnagle, *What We Buy When We Buy Now*, 165 U. PA. L. REV. 315, 320–21 (2017).

100. *See* Lothar Determann & Agnieszka Purves, *The Glue that Holds It Together: Enforceability of Arbitration Clauses in Click-Through Agreements and Other Adhesion Contracts*, 14 ELEC. COM. & L. REP. 1 (2009).

G. TRUST AND MARKET EXPECTATIONS

Despite the many obvious advantages of electronic signatures, some businesses and government agencies are relatively slow to fully embrace new technologies. One reason may be a general reluctance to change. Another key reason is that many remain concerned about legal uncertainty due to overly complex, outdated, and diverging national and international laws. If a contract is found invalid because of misunderstandings about legal standards for signatures or how those standards will be enforced, the seller may have already shipped the product or the bank extended a loan.[101] From a practical perspective, the ramp-up costs for implementing an electronic signature system by selecting and acquiring software and possibly hardware also have to be taken into account, and can pose a challenge, especially for smaller businesses.

Qualified digital signatures could theoretically be used to overcome trust deficits, particularly signatures with technologies that are offered by government-approved providers in accordance with laws that expressly declare such qualified electronic signatures fully equivalent to hand-written signatures.[102] Yet, decades after some U.S. states enacted the first digital signature laws and the European Community tried to harmonize digital signature requirements, first with the Electronic Signature Directive in 1999 and then with eIDAS in 2014, qualified electronic signatures are still rarely used in practice, due to costs and inconveniences associated with acquiring the licensed technologies and the fact that uncertainties remain because technologies approved in one country by a government authority may not be recognized in other countries. Also, even qualified electronic signatures cannot achieve the objectives of all form requirements, for example, the purposes of witness, notarization, and recording requirements.

H. SUSTAINABILITY

Last but not least, electronic signature technology providers flag reasons for why going paperless is better for the environment.[103] Authors of e-mails and

---

101. *See, e.g.*, *Bendigo and Adelaide Bank Ltd. (ACN 068 049 178) & Ors v Kenneth Ross Pickard & Anor* [2019] SASC 123 (Austl.).

102. For example, at the European level under eIDAS, equivalence is affirmed in paragraph 2 of Article 25, and requirements for qualified electronic signatures that are government-approved in Member States are laid down in subsections 28–30 of Article 3 and Annexes I–II. *See* eIDAS, *supra* note 14, art. 25, para. 2; *id.* art. 3(28)–(30); *id.* annexes I–II, at 111–12. In Switzerland, a qualified electronic signature is defined as a signature based on a qualified certificate in Article 2 of the Federal Act on Electronic Signatures, which in turn must fulfill legal requirements as set out in Article 8 of the same Act. SYSTEMATISCHE SAMMLUNG DES BUNDESRECHTS [SR] [SYSTEMATIC COMPILATION OF FEDERAL LAWS] Dec. 2, 2004, SR 943.032, arts. 2, 8 (Switz.). Qualified electronic signatures are thus government-approved and considered as valid as a handwritten signature according to paragraph 2bis of Article 14 of the Swiss Code of Obligations (which translates qualified electronic signature into "authenticated electronic signature"). OBLIGATIONENRECHT [OR] [CODE OF OBLIGATIONS] Mar. 30, 1911, SR 2, RS 2, art. 14, para. 2bis (Switz.).

103. *See, e.g.*, *Sustainability Runs on Agreements*, DOCUSIGN (Nov. 26, 2020), https://www.docusign.co.uk/blog/sustainability-runs-agreements.

other electronic documents increasingly add pleas to their documents to "save a tree—don't print this document," although the paper industry has raised counterarguments in favor of using paper.[104]

I. SUMMARY

Electronic records and signatures offer governments, companies, and individuals many advantages over ink and paper, including speed, cost savings, convenience, easier search and analysis, cheaper archiving and retrieval, automation of retention and deletion, additional options to protect authenticity and integrity, better evidence and identification, chances of scalability, opportunities to standardize and reduce variety and deviations, and arguably a plus for sustainability (don't print this Article, save a tree). Forgery concerns apply equally to electronic and ink-on-paper signatures, but electronic signature technologies offer additional security measures. A key reason that electronic records and signatures have not been more widely adopted despite significant advantages appears to be legal uncertainty regarding the validity and effectiveness of electronic form under applicable law.

IV. POLICY OBJECTIVES AND LAWMAKERS' OPTIONS

In light of the many advantages of electronic records and signatures and the fact that legal uncertainties seem to be the main obstacle to adoption, as discussed in the preceding Part, lawmakers around the world had their work cut out for them as they began considering these issues in the 1990s. As businesses and companies started to rapidly embrace the Internet and electronic commerce, legislatures had a number of options, including action or reaction: they could wait and see how courts would address the deployment of new technologies and react to any problems that become apparent, or they could actively permit, prohibit, or regulate the use of electronic signatures. By the turn of the century, lawmakers in the United States and Europe chose action over inaction, albeit with different approaches: cautiously permissive in the United States and complex regulations in Europe. Most other countries followed with national legislation of their own.

In preparation for a comparative analysis of the hodgepodge of existing legislation around the world in Part V and considerations for improvements and harmonization in Part VI, it is helpful to identify the basic options lawmakers had—and still have—to address electronic signatures, commerce, documents, records, and transactions. This Part reviews declarations of policy objectives and legislative intent in the U.S. and European laws in Subpart A and then explores options to pursue the policy objectives in Subpart B.

104. *See* Alison Moodie, *Is Digital Really Greener than Paper?*, GUARDIAN (Feb. 24, 2014, 2:10 PM), www.theguardian.com/sustainable-business/digital-really-greener-paper-marketing.

A. LEGISLATIVE INTENT AND OBJECTIVES

Governments on both sides of the Atlantic realized the advantages of electronic signatures and documents early on. They also recognized legal uncertainty as a major obstacle to the acceptance of these technologies and declared an intent to remove this legal uncertainty by providing clear legal frameworks. Lawmakers in Europe additionally stressed a desire to balance the interests of businesses and consumers in "secure, trustworthy and easy-to-use electronic transactions."[105] In a prefatory note to the Uniform Electronic Transactions Act of 1999 (UETA), the drafters stated:

> With the advent of electronic means of communication and information transfer, business models and methods for doing business have evolved to take advantage of the speed, efficiencies, and cost benefits of electronic technologies. These developments have occurred in the face of existing legal barriers to the legal efficacy of records and documents which exist solely in electronic media. Whether the legal requirement that information or an agreement or contract must be contained or set forth in a pen and paper writing derives from a statute of frauds affecting the enforceability of an agreement, or from a record retention statute that calls for keeping the paper record of a transaction, such legal requirements raise real barriers to the effective use of electronic media. . . . It is important to understand that the purpose of the UETA is to remove barriers to electronic commerce by validating and effectuating electronic records and signatures.[106]

In the United States, Congress prescribed in ESIGN that:

> The Secretary of Commerce shall promote the acceptance and use, on an international basis, of electronic signatures . . . . [and] take all actions necessary . . . to eliminate or reduce, to the maximum extent possible, the impediments to commerce in electronic signatures, for the purpose of facilitating the development of interstate and foreign commerce.[107]

The European Community noted in the recitals for its Electronic Signature Directive:

> Electronic communication and commerce necessitate 'electronic signatures' . . . . [A] clear . . . framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies . . . .
>
> [I]nteroperability of electronic-signature products should be promoted . . . .
>
> . . . .
>
> [T]he availability of electronic communication could be of great service . . . .
>
> Rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies . . . .

---

105. eIDAS, *supra* note 14, recital 3, at 73; *accord* Directive 1999/93/EC, *supra* note 12, recital 14, at 13.

106. UNIF. ELEC. TRANSACTIONS ACT, prefatory note (UNIF. L. COMM'N 1999).

107. Electronic Signatures in Global and National Commerce Act of 2000 § 301(a)(1), 15 U.S.C. § 7031(a)(1).

> . . . .
>
> It is important to strike a balance between consumer and business needs . . . .[108]

The European Union confirmed its support for electronic signatures in 2014 in the recitals to eIDAS, while acknowledging that the Electronic Signature Directive of 1999 had failed to deliver a comprehensive framework for secure, trustworthy, and easy-to-use electronic transactions:

> Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.
>
> This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.
>
> [The Electronic Signature Directive] dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. This Regulation enhances and expands the *acquis* of that Directive.
>
> . . . .
>
> One of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means . . . .[109]

B. LEGISLATIVE OPTIONS AND PROBLEMS

Lawmakers had—and still have— numerous options to support the adoption of electronic signatures by simplifying and clarifying applicable laws. A key problem they face is that applicable laws with potential relevance for electronic signatures are numerous, complex, and subject to different degrees of international harmonization, national legislative jurisdiction, political sensitivities, and vested interests. Most notably, special form requirements are contained in thousands of different laws, which were enacted at different times for various policy objectives, set out in Part II of this Article. In addition to form requirements, lawmakers have to consider how electronic signatures and documents will fare under rules of evidence in civil, criminal, and administrative proceedings, as well as record retention requirements under tax, customs and other laws.

For example, if lawmakers wanted to clarify that copyright owners can transfer their copyrights by way of an electronic document with an electronic

108. Directive 1999/93/EC, *supra* note 12, recitals 4–14, at 12–13.

109. eIDAS, *supra* note 14, recitals 1–3, 12, at 73–74.

signature,[110] they would have to first check whether the current written form requirements derive from the Berne Convention or affect certain groups of artists unfairly. Or, if they wanted to allow employers to use electronic signatures for purposes of agreeing with employees on non-compete covenants or to issue unilateral termination notices, lawmakers would have to consider the views and interests of labor unions and employer associations.

In lights of these complexities, lawmakers have to choose between a number of approaches that come with varying degrees of unknown potential problems and disadvantages:

1. Comprehensive Acceptance of Any Electronic Signatures and Documents

If legislatures pass laws that simply recognize any electronic signatures and documents for any purpose, they would greatly simplify adoption of these electronic solutions. But, such a simple and broad rule may end up abolishing form requirements that serve important purposes and ultimately causing an erosion of trust among consumers and businesses that could be counter-productive to the stated goal of increasing adoption.

2. Selective Acceptance of Any Electronic Signatures and Documents

Short of recognizing *any* electronic signatures and documents for *any* purpose, legislatures could create a positive whitelist of use cases where some or all kinds of electronic signatures and documents are deemed sufficient by law. They could also add a separate blacklist for scenarios where some or all types of electronic signatures are not sufficient. Any transactions, documents, or records not specifically regulated would remain in limbo, subject to separate legislation or court interpretations of existing laws.

Such an approach would simplify adoption and create certainty for listed use cases and reduce the risk of inadvertently abolishing form requirements that serve important purposes. This option was less easily available to lawmakers twenty-five years ago, when electronic commerce and signatures were a novel and rapidly evolving issue. But it should be considered now that many use cases have been tried in practice and a lot of data and experience is available for analysis.[111]

3. Regulating Replacement of Traditional Form Requirements with Specific Electronic Technologies

Legislatures could also define legal requirements that electronic signatures and documents have to meet in order to serve the policy objectives of current form requirements in different statutes. For example, laws could distinguish

110. *See, e.g.*, 17 U.S.C. § 205(a).
111. *See* cases cited *infra* Part V.B.3.

between simple, advanced, and qualified electronic signatures and regulate technology providers in order to encourage or mandate security measures and accountability.

This approach can create certainty if government-approved providers offer businesses and consumers secure, trustworthy, and easy-to-use electronic signature technologies. However, this approach may not drive adoption if providers are unable or unwilling to develop products that meet the prescribed requirements or if global markets do not accept the regulated products. Any prescriptive, detailed, regulatory approach tends to result in complex and rigid regulations and create barriers to international interoperability, particularly where national authorities license electronic signature providers, and signatures created with foreign technologies may not be permitted or accepted in national markets.

4. Conceptually Supporting Electronic Signatures by Prohibiting Discrimination

Stopping short of clearly accepting all or certain regulated electronic signature products, legislatures can declare support and enthusiasm for electronic commerce and documents as a concept and prohibit courts from negating the validity of documents, records, or signatures simply because they are in electronic form (while allowing courts to negate their validity for other reasons).

5. Mixed Approaches

As Part V will show, legislatures have combined and permutated the four basic approaches sketched out in the preceding Subparts. For example, ESIGN prohibits discriminating against electronic signatures,[112] as does most other electronic signature legislation around the world, including the Electronic Signature Directive[113] and eIDAS in Europe.[114] Whitelists remain rare and narrowly framed or contained in sector-specific statutes, although UETA at least clarifies that electronic documents and signatures shall meet basic written form requirements established by other statutes.[115]

C. SUMMARY

Based on policy statements, governments in the United States and Europe were and remain aligned in their desire to promote adoption of electronic records and signatures and remove legal obstacles to their use. To achieve this, lawmakers have had to repeal, replace, or update existing form requirements.

112. 15 U.S.C. § 7031(a)(2)(D).

113. Directive 1999/93/EC, *supra* note 12, arts. 3, 5.

114. eIDAS, *supra* note 14, art. 25.

115. UNIF. ELEC. TRANSACTIONS ACT § 8(a) (UNIF. L. COMM'N 1999); *see,e.g.*, CAL. CIV. CODE § 1633.8(a) (West 2021).

This affects myriad statutes, regulations, and administrative processes. In the late 1990s, lawmakers found it difficult to assess the potential impact on the policy objectives which the various form requirements were originally created to serve. Therefore, legislatures resorted to minimally invasive corrections and prohibited discrimination against electronic form, rather than implementing more sweeping legislation recognizing electronic form as sufficient to meet existing form requirements in general or in specific circumstances.

V. CURRENT LAWS

Lawmakers have weighed the different factors, legislative objectives, options, advantages, and disadvantages explored in Parts II to IV of this Article differently around the world and have responded to electronic commerce and communication developments with diverging laws. Early laws were enacted in the United States and Europe in the late 1990s,[116] followed by a United Nations Convention on the Use of Electronic Communications in International Contracts in 2005.[117] By the end of 2020, more than seventy countries had enacted specific laws to recognize electronic documents and signatures and admit electronic signatures as evidence in court.[118]

In all surveyed jurisdictions, parties can use electronic signatures to create valid contracts and documents that are not subject to a specific statutory form requirement. Viable use cases generally include commercial agreements between businesses (including non-disclosure agreements, purchase orders, order acknowledgements, invoices, other procurement documents, sales agreements, distribution agreements, and service agreements), consumer agreements (including new retail account opening documents, sales terms, services terms, software licenses, purchase orders, order confirmations, invoices, shipment documentation, user manuals, and policies (but not consumer loan agreements in many jurisdictions)), service agreements, software license agreements, copyright licenses, patent licenses, trademark licenses, and intangible property transfers (for example, patent and copyright assignments) other than agreements on the ownership of employee inventions. In several jurisdictions, many human resource documents (such as regular employment contracts, non-disclosure agreements, privacy notices, benefits paperwork, and other new employee onboarding processes) and short-term leases can also be

116. *See infra* Part V.A–B.

117. *See* UNCITRAL, UNITED NATIONS CONVENTION ON THE USE OF ELECTRONIC COMMUNICATIONS IN INTERNATIONAL CONTRACTS, U.N. Sales No. E.07.V.2. (2007).

118. In researching this Article, the Author reviewed legislation in Argentina, Australia, Austria, Belgium, Brazil, Brunei, Cameroon, Canada, Chile, China, Colombia, the Czech Republic, Denmark, Ecuador, Egypt, Estonia, Finland, France, Germany, Greece, Guatemala, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Kazakhstan, Latvia, Lithuania, Luxembourg, Macau, Malaysia, Mexico, the Netherlands, New Zealand, Nigeria, Norway, Peru, the Philippines, Poland, Portugal, Romania, Russia, Saudi Arabia, Singapore, South Africa, South Korea, Spain, Sri Lanka, Sweden, Switzerland, Taiwan, Thailand, Turkey, Ukraine, the United Arab Emirates, the United Kingdom, the United States, Uruguay, and Vietnam. eIDAS applies in all member states of the European Economic Area.

effectuated by e-signatures. All jurisdictions contain additional form requirements for particular transactions, which arise from numerous statutes of varying vintages and cover certain matters in the areas of family, real estate, employment law, and other areas that vary from jurisdiction to jurisdiction. The next Subparts provide an overview and a few examples to illustrate the fragmented landscape of current laws pertaining to electronic signatures.

A. EUROPE

In Europe, the Commission of the European Community began working on a Directive to address electronic commerce and signatures in 1997[119] to preempt Member States from enacting national legislation.

1. The Electronic Signature Directive

In Europe, until the turn of the last century, the only valid way to sign a contract was by hand.[120] On December 13, 1999, the European Community enacted the Electronic Signature Directive,[121] directing the Member States to pass national laws in line with the provisions and objectives of the Directive.[122] The Member States remained free, however, to decide in national legislation what kinds of transactions could be effectuated with an electronic signature, and if so, with what kind of electronic signature.[123]

2. eIDAS

In 2014, the European Union adopted Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) to replace the Electronic Signature Directive. [124] One of the Regulation's key objectives is to achieve general recognition of electronic identification schemes across the E.U. Member States.[125] The European Union decided to adopt a regulation as a directly binding law instead of a directive, which requires Member States to pass national laws,[126] in the interest of greater harmonization. In a Commission Staff Working Paper of June 7, 2012, the

119. Directive 1999/93/EC, *supra* note 12, recitals 1–3, at 12.

120. *What Is the Legislation?*, CEF DIGITAL, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+the+legislation+-+esignature (last visited May 21, 2021).

121. Directive 1999/93/EC, *supra* note 12.

122. For internal markets, see *id.* art. 4. For international aspects, see *id.* art. 7.

123. *Id.* art. 1 ("It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.").

124. eIDAS, *supra* note 14.

125. *Id.* art. 1(a).

126. For difference between the two, see *Regulations, Directives and Other Acts*, EUR. UNION, https://europa.eu/european-union/law/legal-acts_en (last visited May 21, 2021) ("A 'regulation' is a binding legislative act. It must be applied in its entirety across the EU. . . . A 'directive' is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals.").

Secretary-General of the European Commission noted that "adopting a Directive . . . has shown its limits since 1999"[127] and that "the freedom given to [Member States] when transposing a directive (in terms of interpretation and of implementation of the systems) contributed to the current problems of mutual recognition of services and products and of cross-border interoperability."[128] In contrast, a regulation is a tool that provides "immediate applicability and stronger harmonisation."[129]

To harmonize electronic signature laws across Europe, eIDAS provides that an electronic signature "shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form" or that it does not meet requirements for a higher standard of electronic signatures.[130] eIDAS contemplates three tiers of signatures: "electronic signatures" (also known as "simple electronic signatures", or SES), "advanced electronic signatures" (AES), and "qualified electronic signatures" (QES). eIDAS requires that QES and certain categories of AES be recognized as equivalent to handwritten signatures and that all E.U. Member States must recognize QES that were approved in accordance with eIDAS in any E.U. Member State.[131]

a. Simple Electronic Signatures

The most basic form of electronic signature is the SES. Pursuant to article 3(10) of eIDAS, "electronic signature" means "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign." The definition covers, for example, a name typed at the end of an e-mail and also covers a scanned signature. An SES is not uniquely linked with the signatory and is generally validated through circumstantial means. Unlike QES, a basic SES does not have to meet any qualified authentication or security requirements (for example, a scanned signature can be copied and used in other documents).

b. Advanced Electronic Signatures

An AES is an electronic signature that is: (a) uniquely linked to the signatory; (b) capable of identifying the signatory; (c) created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) linked to the signature in a way that any

127. *Commission Staff Working Paper, Impact Assessment: Accompanying the Document Proposal for a Regulation of the European Parliament and of the Trust Services for Electronic Transactions in the Internal Market*, at 40, SWD (2012) 135 final (June 7, 2012).

128. *Id.*

129. *Id.* at 41.

130. eIDAS, *supra* note 14, art. 25(1).

131. *Id.* art. 25(2)–(3). This category is that of "qualified electronic signatures," which are discussed in more detail below. *See infra* Part V.A.2.c.

subsequent change in the data is detectable.[132] The data associated with an AES means that it is much more easily and reliably linked to the signatory. Many jurisdictions outside the European Union recognize a concept similar to AES, though some use the label "digital signature."[133]

c. Qualified Electronic Signatures

A QES is essentially an AES with the added layer of prescriptive requirements and state certification. It is an advanced electronic signature that is created by a qualified electronic signature creation device issued by a qualified trust service provider and which is based on a qualified certificate for electronic signatures (a "qualified certificate").[134] In the European Union, QES has the same legal effect as a handwritten signature.[135]

Requirements for QES certificates are specified in Annex 1 of eIDAS. A QES shall contain:

> (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate;
>
> (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates, including at least the Member State in which that provider is established . . . .
>
> (c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;

132. eIDAS, *supra* note 14, art. 26.

133. *See, e.g.*, Law No. 25,506, Dec. 11, 2001 (Arg.); Medida Próvisoria No. 2,200-2, de 24 de Agosto de 2001 (Braz.); Electronic Transactions Act (Cap. 196) (Brunei); Regissant les communications electroniques au Cameroun, loi no. 2010/013 du 21 décembre 2010 [Law on Electronic Commerce in Cameroon, Law No. 2010/03 of Dec. 21, 2010] (Cameroon); Law No. 19799 arts. 1–2, Marzo 25, 2002, DIARIO OFICIAL [D.O.] (Chile); L. 527/99, agosto 18, 1999, DIARIO OFICIAL [D.O.] (Colom.); Law No. 527, agosto 21, 1999 (Ecuador); Law No. 15 of 2004 (E-signature and Establishment of the Information Technology Industry Development Authority (ITIDA)), *al-Jarīdah al-Rasmīyah*, 12 Apr. 2004, art. 1 (Egypt); Recognition of Electronic Communications and Signatures Law (Guat.); Electronic Transactions Ordinance, (2000) Cap. 553 (H.K.); Electronic Signatures, 2001 (Act No. 28/2001) (Ice.); The Information Technology (Amended) Act, 2009 (India); Law No. 11 of 2008 on Electronic Information and Transaction (Indon.); Electronic Signature Law, 5761–2001 (Isr.); On Electronic Document and Electronic Digital Signature, 7 Jan. 2003, as amended (Kaz.); Dijiteol seomyeongbeob [Digital Signature Act] art. 2 (S. Kor.); Law of Electronic Documents and Signatures (Law No. 5/2005) (Mac.); Act 658, Electronic Commerce Act 2006 (Malay.); Act 562, Digital Signature Act 1997 (Malay.); Código de Comercio [CCom] [Commercial Code], Diario Oficial de la Federación [DOF] 07-10 al 13-12-1889, últimas reformas DOF 28-03-2018 (Mex.); Dep't of Trade & Industry & Dep't of Sci. & Tech., Admin. Ord. No. 02 (Sept. 28, 2001) (Phil.), https://lawphil.net/administ/jointdept/jdao_2_2001.html; Federal'nyĭ Zakon RF o elektronnaya podpis' [Federal Law of the Russian Federation on Electronic Signature], SOBRANIE ZAKONODATEL'STVA ROSSIĬSKOĬ FEDERATSII [SZ RF] [Russian Federation Collection of Legislation] 2011, No. 63-FZ, art. 5 (Russ.); Electronic Transactions Act (2010) (Sing.); Electronic Communications and Transactions Act 25 of 2002 (S. Afr.); Electronic Signatures Act (Taiwan); Electronic Transactions Act BE. 2544 (2001) (Thai.); Electronic Signature Law No. 5070 (Turk.); Electronic Digital Signature Law No. 852-IV (Ukr.); Documento Electrónico y Firma Electrónica [Electronic Document and Signature Act], Act No. 18.600, Sept. 21, 2009 (Uru.); Law No. 51/2005/QH11 of Nov. 29, 2005 on E-Transactions, art. 21.1 (Viet.).

134. eIDAS, *supra* note 14, art. 3(12).

135. *Id.* art. 25(2).

> (d) electronic signature validation data that corresponds to the electronic signature creation data;
>
> (e) details of the beginning and end of the certificate's period of validity;
>
> (f) the certificate identity code, which must be unique for the qualified trust service provider;
>
> (g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
>
> (h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;
>
> (i) the location of the services that can be used to enquire about the validity status of the qualified certificate;
>
> (j) where the creation data related to the validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.[136]

The qualified certificate must be issued by a qualified trust service provider, which are listed by Member States on the E.U. Trusted Lists.[137] Each Member State is responsible for maintaining and publishing its own trusted lists of qualified trust services providers.[138] The statute specifies that qualified electronic signature creation devices should be developed using an "IT security certification based on international standards such as ISO 15408 and related evaluation methods and mutual recognition arrangements."[139] The requirements for a qualified electronic signature creation device are set out in Annex II of eIDAS.[140]

---

136. *Id.* annex I, at 111.

137. *See EU Trusted Lists*, EUR. COMM'N (Mar. 11, 2021), https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers.

138. eIDAS, *supra* note 14, art. 22.

139. *Id.* recital 55, at 80.

140. The requirements are the following:

> 1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:
>
> (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;
>
> (b) the electronic signature creation data used for electronic signature creation can practically occur only once;
>
> (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;
>
> (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.
>
> 2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.
>
> 3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.

3. National Laws

In practice, harmonization in the European Union leaves much to be desired. While eIDAS harmonized European laws on electronic signatures with respect to (1) the legal equivalence of QES and handwritten signatures and (2) the fact that signatures must not be denied legal effect and admissibility as evidence in legal proceedings solely because of their electronic form, eIDAS remains silent as to the situations in which electronic signatures could be used.[141] Thus, each E.U. Member State remains free to specify in its laws whether electronic signatures are permissible for a given context and, if so, which type of electronic signature is sufficient (SES, AES, or QES).

Despite certain commonalities, there is great variation in the situations in which Member States permit the use of electronic signatures and the tier of signature required for the task. The result is that, for many use cases, businesses hesitate to adopt electronic signatures because of a need for a review of local laws, in addition to E.U. regulations.

a. Germany

In Germany, the main national legal framework for electronic signatures is codified in the Trust Services Act.[142] The German Civil Code[143] and the German Code of Civil Procedure[144] contain the form requirements for contracts and rules of evidence. German national laws remain in place and were updated by an "eIDAS Implementation Act" on July 29, 2017.[145]

Following the categories of eIDAS, German law distinguishes between SES, AES, and QES. However, because German law specifies several different form requirements for documents in order for them to be valid, SES and AES are of limited utility for many applications, as they do not satisfy the German "written form" (*Schriftform*) requirement.[146] Because *Schriftform* is required for many documents, an alternative to SES or AES is sometimes required. SES is

---

4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:

(a) the security of the duplicated datasets must be at the same level as for the original datasets;

(b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

Id. annex II, at 12.

141. *See id.* recital 49, at 79.

142. *See* Vertrauensdienstegesetz [VDG] [Trust Services Act], July 18, 2017, § 126(a), https://www.gesetze-im-internet.de/vdg/VDG.pdf (Ger.).

143. Bürgerliches Gesetzbuch [BGB] [Civil Code], http://www.gesetze-im-internet.de/bgb/index.html (Ger.).

144. Zivilprozessordnung [ZPO] [Code of Civil Procedure], http://www.gesetze-im-internet.de/zpo/index.html (Ger.).

145. eIDAS-Durchführungsgesetz [eIDAS Implementation Act], https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl117s2745.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2745.pdf%27%5D__1553280463103 (Ger.).

146. *See* Bürgerliches Gesetzbuch [BGB] [Civil Code], §§ 126, para. 3, 126a, para. 1 (Ger.).

sufficient, however, whenever only "text form" (stipulated in section 126 b of the German Civil Code) is required, because in such cases, no signature at all is legally required.

In court proceedings, SES does not have the probative value of a deed, but is subject to evaluation pursuant to section 371, paragraph 1, clauses 2 and section 286 of the German Code of Civil Procedure.

In practice, as a general rule, contracts and legal actions can be rendered effective by SES or AES. This applies, for example, to service agreements,[147] to sales agreements in general,[148] and to software license agreements.[149] Some types of contracts or legal actions require more, however, such as a handwritten signature or other formal requirements like notarization.[150]

QES satisfies the written form requirement and may substitute for a handwritten signature, so it can be used in many situations where SES or AES would not be appropriate—thanks to eIDAS, even in situations where the "electronic form" is expressly excluded in national law. These include contracts of surety,[151] consumer loan agreements,[152] terminations of employment agreements,[153] and residential lease agreements.[154]

Notarization requirements mean that even a QES is not enough. So it would generally not be possible to execute contracts to purchase or transfer real property[155] or contracts of inheritance,[156] for example, using only electronic signatures.

Before eIDAS, German courts took a conservative approach to electronic signatures. Since eIDAS, they have emphasized that only QES is equivalent to handwritten signatures. For example, in 2012 the Higher Regional Court of Munich decided that a signature on an electronic tablet does not meet the German written form requirement.[157] In 2013, the same court decided that if the parties contractually agreed that amendments require the written form, a declaration per e-mail is not valid.[158] The District Court of Tübingen ruled in January 2019 that filing a protest against a penalty notice via e-mail is only possible if the e-mail contains a QES.[159]

147. *Id.* § 611.
148. *Id.* § 433.
149. *Id.* §§ 433, 535.
150. For example, real estate sales contracts, *id.* § 311(b), and promises of gifts, *id.* § 518.
151. *Id.* § 766, para. 1, sentence 2.
152. *Id.* § 492, para. 1, sentence 1.
153. *Id.* § 623.
154. *Id.* § 568, para. 1.
155. *Id.* § 311b, para. 1.
156. *Id.* §§ 2276, 2371.
157. Oberlandesgericht [OLG] [Higher Regional Court of Munich] June 4, 2012, Doc. No. 19 U 771/12 (Ger.).
158. Oberlandesgericht [OLG] [Higher Regional Court of Munich] Oct. 23, 2013, Doc. No. 7 U 321/13 (Ger.).
159. Landgericht [LG] [Tübingen District Court] Jan. 28, 2019, Doc. No. 9 Qs 6/19 (Ger.).

b. France

Before eIDAS, the main legal framework for electronic signatures in France was set out in Act No. 2000-230 of March 13, 2000, adapting evidence law to IT and electronic signatures,[160] now codified in articles 1366 and 1367 of the French Civil Code (FCC).[161] Generally, in France, electronic writing has the same probative force as writing on paper, provided that it is possible to properly identify the person from whom the electronic writing originates and that the writing is created and stored in conditions ensuring its integrity.

French law in general differentiates between SES, AES, and QES as defined in eIDAS, whereas SES and AES are considered to have the same legal effect as each other. Per eIDAS, QES is equal to handwritten signatures.

As in Germany, contracts are generally valid if legally competent parties reach an agreement, whether they agree verbally, electronically, or in a physical paper document.[162] Article 1366 of the FCC specifically confirms that contracts cannot be denied enforceability merely because they are concluded electronically.[163] However, some transactions like private deeds governed by family law and the law of succession require the paper form, and the "electronic form" is excluded.[164] Other specific transactions have to be notarized.[165]

French courts have been relatively liberal throughout the years in recognizing electronic signatures. In a 2016 decision, the Cour de Cassation (the highest court in France for civil law matters) acknowledged that the admissibility of electronic evidence of a written and signed document does not require a QES and the judge must therefore weigh on his or her own whether the process is reliable or not.[166] In the case at issue, the electronic evidence was delivered via an online contract platform operated by a non-qualified provider. In the eyes of the court, the electronic document was (1) created and stored in conditions ensuring its integrity, (2) using a reliable eSignature process, and (3) enabling the identification and authentication of the signatory precisely. Moreover, when the admissibility of a contract requires a written notice, the Cour de Cassation in another case acknowledged that the written notice need not

160. Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique [Law 200-230 of March 13, 2000 Adapting the Rules of Evidence to Information Technology and Related to Electronic Signatures] (Fr.), https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000399095.

161. Code civil [C. civ.] [Civil Code] arts. 1363–68 (Fr.).

162. *See id.* arts. 1102, 1109, 1172–73.

163. *See id.* art. 1366.

164. *Id.* art. 1175.

165. For example, contracts to purchase or transfer real property, *see id.* art. 4, decree no. 55-22, art. 28, decree no. 71-941.

166. Cour de cassation [Cass.] [supreme court for judicial matters] 1e civ., Apr. 6, 2016, Bull. civ. I, No. 15-10732 (Fr.).

necessarily be handwritten, so long as the notice complies with form requirements under electronic signature law.[167]

c. Belgium

In Belgium, the eIDAS regulation is supplemented by the Electronic Economy Law,[168] an Act dating from the year 2000 that introduced the use of telecommunications and electronic signatures in judicial and extra-judicial procedure[169] and the Belgian Civil Code.[170]

In its current form, the Belgian Civil Code provides that any set of electronic data from which one can derive with certainty the identity of the author and the integrity of the contents to be signed satisfies the requirements of a signature.[171] Provided they meet these requirements, both SES and AES are generally acceptable under Belgian law for private deeds (for example, deeds that do not need to be signed in the presence of a notary or other public authority). The satisfaction of these requirements, and therefore the enforceability of the electronic signature, will ultimately be left to the assessment of a court, on a case-by-case basis.

Belgian law does not currently treat SES and AES the same. An AES should systematically qualify as a Civil Code-grade signature and can therefore be used as a signature in the legal sense for all private deeds except where specific electronic signature requirements apply (for example, for employment contracts). An SES may qualify as a Civil Code-grade signature only if one can infer from it with certainty the identity of the author and if it guarantees the

167. Cour de cassation [Cass.] [supreme court for judicial matters], 1e civ., Oct. 28, 2015, Bull civ. I. No. 14-23110 (Fr.).

168. Wet tot uitvoering en aanvulling van de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, houdende invoeging van titel 2 in boek XII "Recht van de elektronische economie" van het Wetboek van economisch recht, en houdende invoeging van de definities eigen aan titel 2 van boek XII en van de rechtshandhavingsbepalingen eigen aan titel 2 van boek XII, in de boeken I, XV en XVII van het Wetboek van economisch recht [Act of 21 July 2016 Implementing and Supplementing 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, Inserting Title II in Book XII "Law of the Electronic Economy" of the Code of Economic Law, and Inserting the Definitions Proper to Title II of Book XII and the Law Enforcement Provisions Specific to Title II of Book XVII, in books I, XV, and XVII of the Code of Economic Law], B.S., Sept. 28, 2016, http://www.ejustice.just.fgov.be/mopdf/2016/09/28_1.pdf#Page10 (Belg.).

169. Wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure [Act of 20 October 2000 Implementing of the Use of Telecommunication Means and of the Electronic Signature in Judicial and Extrajudicial Proceedings], B.S., Dec. 22, 2000, https://www.ejustice.just.fgov.be/mopdf/2000/12/22_1.pdf#Page1 (Belg.).

170. Specifically, paragraph 2 of Article 1322 of the Belgian Civil Code as of November 1, 2020, is replaced with the new Title VIII of the Belgian Civil Code on the rules of evidence. *See* C.Civ. (Belg.), art. 1322, para. 2; Wet van 13 april 2019 tot invoering van een Burgerlijk Wetboek en tot invoeging van Boek 8 "Bewijs" in dat Wetboek [Act of 13 April 2019 Introducing a Civil Code and Inserting Book 8 "Evidence" in that Code], B.S., May 14, 2019, http://www.ejustice.just.fgov.be/mopdf/2019/05/14_1.pdf#Page9 (Belg.).

171. *See* C.Civ. (Belg.), art. 1322, para. 2.

integrity of the signed data. If an SES does not qualify as a Civil Code-grade signature, it will not be considered a signature in the legal sense (but could be referred to as written evidence for formation of a contract that is not in writing).

After Belgium's eIDAS implementing law took effect on November 1, 2020, however, Belgium *does now* treat SES and AES more similarly to each other as compared to QES (which are treated as a handwritten signature).[172] The validity and enforceability of non-QES (for example, SES and AES) are still left to the discretion of courts, but non-QES will directly qualify as signatures for private deeds under the Belgian Civil Code. On the other hand, under the eIDAS, SES cannot simply be deprived of any legal effect because of its electronic character.

d. Sweden

eIDAS applies directly in Sweden and, in addition, Swedish law contains supplementary rules in relation to local supervision and enforcement of eIDAS.[173] As a general rule, all contracts and legal actions that do not require a handwritten signature can be rendered effective by SES, AES, or QES in Sweden.[174] As an exception to this rule, some types of contracts, legal actions, or transactions require an AES, a QES, or other formalities.[175] It is unclear how a Swedish court would approach the intersection between eIDAS and requirements in Swedish law for handwritten signatures, but given the approach Germany has taken in response to similar issues, it is likely that QES would satisfy the requirements for handwritten signatures in the absence of other form requirements.

e. Summary

Although eIDAS has harmonized some aspects of European laws on electronic signatures, the answer to the question whether a certain record or signature is valid or effective in electronic form still varies depending on the national law.

B. UNITED STATES

In the 1869 case of *Howley v. Whipple*, one contracting party challenged the validity of assent to an agreement via a telegraph message, and the Supreme Court of New Hampshire found:

---

172. *See* Wet van 13 april 2019 tot invoering van een Burgerlijk Wetboek en tot invoeging van Boek 8 "Bewijs" in dat Wetboek [Act of 13 April 2019 Introducing a Civil Code and Inserting Book 8 "Evidence" in that Code], B.S., May 14, 2019, http://www.ejustice.just.fgov.be/mopdf/2019/05/14_1.pdf#Page9 (Belg.).

173. LAG MED KOMPLETTERANDE BESTÄMMELSER TILL EU:S FÖRORDNING OM ELEKTRONISK IDENTIFIERING [The Act with Supplementary Rules to EU's Regulation on Electronic Identification] (SFS 2016:561) (Swed.), http://rkrattsbaser.gov.se/sfst?bet=2016:561.

174. *See id.*

175. *See id.*

> [I]t makes no difference whether the [telegraph] operator writes . . . with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. . . . [N]or does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office.[176]

Howley marked a judicial recognition of the effects of advancing technology on commerce and articulated an understanding that parties separated by long distances could conduct business and agree to contracts without putting pen to ink. So, long before the rise of the Internet, courts had begun to test the boundaries of electronic transactions and dealt with new ways of forming contracts.

1. Early State Laws, UETA, and ESIGN

In 1995, Utah became the first U.S. state to enact a law specifically for electronic signatures.[177] Other states followed, implementing their own solutions. Concerned that a lack of uniformity among the states might lead to confusion, the Uniform Law Commission issued the first draft of its model provisions for what was initially called the Electronic Communications in Contractual Transactions Act[178] but was soon rechristened the Uniform Electronic Transactions Act (UETA) and finalized in 1999.[179] In 2000, the federal government enacted its own legislation in the form of the Electronic Signatures in Global and National Commerce Act (ESIGN).[180] President Clinton used a smart card encrypted with his digital signature to sign the bill into law.[181]

Both ESIGN and UETA state that a "signature . . . may not be denied legal effect . . . or enforceability solely because it is in electronic form."[182] UETA goes a step further and explicitly states that electronic documents signed electronically are legally equivalent to documents and/or agreements signed by hand when the law requires a written agreement: "[i]f a law requires a record to be in writing, an electronic record satisfies the law," and "[i]f a law requires a signature, an electronic signature satisfies the law."[183] Both ESIGN and UETA are technology-neutral and do not prescribe different types of electronic signatures (such as SES, AES, or QES in European law). Both ESIGN and UETA exclude from permissions for electronic contracts certain classes of documents, such as employment terminations, certain real estate documents, and

176. Howley v. Whipple, 48 N.H. 487, 488 (1869).

177. *See* UTAH CODE ANN. §§ 46-3-201 to 46-3-504 (repealed 2006).

178. ELEC. COMMC'NS IN CONTRACTUAL TRANSACTIONS (UNIF. L. COMM'N, Draft Apr. 10, 1997).

179. UNIF. ELEC. TRANSACTIONS ACT (UNIF. L. COMM'N 1999).

180. 15 U.S.C. §§ 7001–06.

181. Amy Norcross, *President Clinton e-Signs Digital Signature Act, June 30, 2000*, EDN (June 30, 2019), https://www.edn.com/president-clinton-e-signs-digital-signature-act-june-30-2000/. Note, however, that this was purely a symbolic gesture, as the official signing took place via a traditional wet signature.

182. 15 U.S.C. § 7001; UNIF. ELEC. TRANSACTIONS ACT § 7(a).

183. UNIF. ELEC. TRANSACTIONS ACT § 7.

family law documents. UETA has been enacted in forty-eight states,[184] not including Illinois and New York, two states that have each enacted their own statutes governing electronic signatures.[185]

ESIGN expressly preempts state laws to the extent that they are inconsistent with ESIGN,[186] subject to certain exceptions.[187] If a state has enacted UETA as approved and recommended by the National Conference of Commissioners on Uniform State Laws in 1999, the state law will govern. However, if a state has accepted the invitation in UETA section 3(b)(4) to exclude bodies of state law other than those listed by the drafters from the provisions of UETA, ESIGN specifies that those exclusions are preempted to the extent that they are inconsistent with ESIGN.[188]

Both ESIGN and the UETA contain several exceptions to the general acceptance of electronic signatures. ESIGN lists a number of transactions that are excluded from the applicability of the statute, including contracts or documents governed by a statute or regulation governing wills, codicils, or testamentary trusts,[189] contracts or documents governed by a statute or regulation governing adoption, divorce, or other matters of family law,[190] and contracts or documents governed by the Uniform Commercial Code (UCC), other than sections 1-107 and 1-206 and articles 2 and 2A.[191] Section 3 of UETA allows states to include their own lists of exceptions. California's version of UETA, for example, provides a laundry list of cases to which the statute does not apply, including transactions involving laws governing the creation and

184. *UETA—Uniform Electronic Transactions Act*, CITRIX RIGHT SIGNATURE, https://rightsignature.com/legality/ueta-act.html (last visited May 21, 2021).

185. N.Y. STATE TECH. LAW § 540 (McKinney 2021); 5 ILL. COMP. STAT. 175/1-101 to 99-1 (2021).

186. 15 U.S.C. § 7002. This preemption includes the non-UETA laws promulgated in Illinois and New York.

187. *Id.* § 7002(a).

188. *Id.* § 7002(a)(1).

189. *Id.* § 7003(a)(1).

190. *Id.* § 7002(a)(2).

191. There are a number of specific provisions in the U.C.C. that deal with electronic documents. U.C.C. § 1-108 limits the effect of ESIGN within the U.C.C., as contemplated by section 102(a) of ESIGN. *See* U.C.C. § 1-108 (AM. L. INST. & UNIF. L. COMM'N 2020). The U.C.C. is intended to provide alternative means for the use and acceptance of electronic signatures and records. U.C.C. § 1-201(b)(37) defines "signed" for purposes of the U.C.C. to include "using any symbol executed or adopted with present intention to adopt or accept a writing" (although "writing" is limited to something expressed in tangible form under U.C.C. § 1-201(b)(43)). *Id.* § 1-201(b)(37). U.C.C. § 1-201(b)(31) defines "record" for purposes of the U.C.C. to be "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." *Id.* § 1-201(b)(31). Various U.C.C. articles contemplate certain types of electronic documents (or documents that are intended to be medium-neutral), such as article 7 (which has its own definitions of "sign" and "record," its own exclusion from ESIGN in 7-103(c), and provides for electronic documents of title) and article 9 (which defines electronic chattel paper). *Id.* §§ 7-102(10)–(11), 7-103, 7-104, 9-102(11). In these cases, an "electronic" document is given equivalent treatment to its tangible counterpart.

execution of wills, codicils, or testamentary trusts[192] and divisions 1, 3, 4, 5, 8, 9, and 11 of the U.C.C.[193]

UETA "applies only to a transaction between parties each of which has agreed to conduct the transaction by electronic means," and the existence of such an agreement "is determined from the context and surrounding circumstances, including the parties' conduct."[194] While no handwritten signature or separate document is required, both parties must agree to the use of electronic records and signatures.

ESIGN does not "require any person to agree to use or accept electronic records or electronic signatures"[195] or require a separate agreement to conduct business electronically. In cases where a statute, rule, or regulation requires that disclosures be provided to a consumer in writing, then electronic documents and signatures satisfy such a requirement only if the consumer "consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent."[196] In other words, consumers must consent electronically to receive disclosures electronically. Once the consumer has consented to the use of electronic documents and signatures in a transaction, those electronic documents and signatures satisfy statutory or regulatory requirements of providing disclosures to a consumer in writing.

2. Washington and Its Electronic Authentication Act

After Utah's Act of 1995,[197] Washington followed in 1996 with the Washington Electronic Authentication Act (WEAA),[198] which was the oldest such statute still on the books until its repeal in 2019.[199] While New York and Illinois, the other two states that have not adopted UETA, have modeled their own laws closely after UETA and ESIGN, WEAA took an independent approach which raised questions in regard to a potential preemption analysis

192. CAL. CIV. CODE § 1633 (West 2021). The prefatory comments to the final version of UETA note that the Act is intended to govern "transactions related to business, commercial (including consumer) and governmental matters," and that the exclusion of wills, codicils, or testamentary trusts "is largely salutary given the unilateral context in which such records are generally created and the unlikely use of such records in a transaction as defined in this Act (i.e., actions taken by two or more persons in the context of business, commercial or governmental affairs)." *See* UNIF. ELEC. TRANSACTIONS ACT § 3 cmt. 1, cmt. 4 (UNIF. L. COMM'N 1999).

193. CAL. CIV. CODE § 1633.3(b)(2)–(3).

194. *Id.* § 1633.5(b).

195. 15 U.S.C. § 7001(c)(1)(A).

196. *Id.* § 7001(c)(1)(C)(ii).

197. UTAH CODE ANN. §§ 46-3-201 to 46-3-504 (repealed 2006). For further details, see Richards, *supra* note 8.

198. Washington Electronic Authentication Act, ch. 250, 1996 Wash. Sess. Laws 1190 (codified at WASH. REV. CODE §§ 19.34.010–19.34.903 (repealed 2019)).

199. The Utah Digital Signature Act was repealed in 2006, six years after Utah adopted its version of UETA.

under ESIGN.[200] A bill to adopt UETA in Washington State, which was introduced in 2012, died in committee.[201] In 2020, however, Washington finally adopted UETA too.[202]

WEAA originally only regulated digital signatures.[203] It required specific security protocols for them to be legally accepted, defining digital signatures as "a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (a) Whether the transformation was created using the private key that corresponds to the signer's public key; and (b) Whether the initial message has been altered since the transformation was made."[204] Complex licensing mechanisms including "certification authorities" issuing certificates to ensure the identity of the subscriber were meant to provide a high level of security and reliability.[205] Requiring technological standards for legal recognition differs from the technology-neutral approach of UETA and ESIGN. In 1999 and 2011, WEAA was amended to keep pace with evolving technology. "Electronic signatures" were added[206] with a requirement that they "[cannot be] denied legal recognition solely because they are in electronic form."[207] In addition, amendments to WEAA made the use of digital signatures and the accompanying complicated licensing process entirely voluntary.[208] At the same time, the term "digital signatures" remained defined and referred to in the Act and therefore distinguished from electronic signatures which made it harder to determine to which extent electronic signatures were legally valid in the state.[209]

This uncertainty became even more clear against the backdrop of various court rulings. For example, in *Neuson v. Macy's Department Stores, Inc.*, a former employee sued her employer for retaliation, disability discrimination, and wrongful termination, but the employer moved for summary judgment to compel arbitration based on an in-house program it implemented to resolve all employment-related disputes.[210] The trial court granted the employer's motion

200. Stephanie Curry, *Washington's Electronic Signature Act: An Anachronism in the New Millennium*, 88 WASH. L. REV. 559, 585–86 (2013).

201. *Id.* at 581–83.

202. Effective June 11, 2020, Washington adopted UETA in Chapter 1.80 RCW with Senate Bill 6028. S.B. 6028, 66th Leg., 2020 Reg. Sess. (Wash. 2020) ("Adopt[ing] the uniform electronic transactions act and aligning statutory provisions relating to signatures, declarations, and documents.").

203. Washington Electronic Authentication Act § 401 ("Where a rule of law requires a signature . . . that rule is satisfied by a digital signature . . . .").

204. *Id.* § 103(10).

205. For a summary of the licensing process, see Curry, *supra* note 200, at 578–79.

206. Act of May 13, 1999, ch. 287, § 2(14), 1999 Wash. Sess. Laws 1203 (codified as amended at WASH. REV. CODE § 19.34.020(14) (repealed 2019)) (defining an electronic signature as "a signature in electronic form attached to or logically associated with an electronic record, including but not limited to a digital signature").

207. *Id.* § 3 (codified as amended at WASH. REV. CODE § 19.34.010(2) (repealed 2019)).

208. Act of Apr. 29, 2011, ch. 183, § 2(2), 2011 Wash. Sess. Laws 1377 (codified as amended at WASH. REV. CODE § 19.34.231 (repealed 2019)) ("A city or county *may* become a licensed certification authority . . . ." (emphasis added)).

209. Curry, *supra* note 200, at 579, 584.

210. Neuson v. Macy's Dep't Stores, Inc., 249 P.3d 1054, 1055 (Wash. Ct. App. 2011).

to uphold electronic signatures, holding that the employer had established the existence of an arbitration agreement by producing evidence: (1) that it had a procedure to mail employees relevant forms; (2) that it required employees to electronically sign an acknowledgment of the arbitration agreement; and (3) that it followed the procedure with the employee.[211] The Washington Court of Appeals for the Third Division reversed and remanded, holding that because the employee presented evidence that she never actually received the forms and never electronically signed the acknowledgment, there was a genuine factual dispute.[212] The court of appeals explained:

> The resolution of the underlying factual dispute here is complicated by the use of an electronic signature. This signature is essential to [the employer's] position that [the employee] received the materials and form necessary to opt out of arbitration. It is not a signature in the traditional sense but rather a string of numbers consisting of an employee's social security number, birth date, and zip code. The information in [the employee's] electronic signature is unique to her, and [the employer] urges that it is sufficient to show that [the employee] received the opt-out form. We find evidence that the [employer] has a procedure and that its procedure was followed, but *we do not find evidence of how or why the information on this electronic signature would be unavailable to anyone other than [the employee] and, ultimately, why it is the same as or better than a traditional signature*.[213]

In summary, the employer needed to demonstrate that the electronic signature was actually submitted by the employee because it had access to the very information used to verify the employee's identity. The court did not elaborate on how the employer might satisfy this requirement.

Several years later, a federal district court in Washington State decided a similar case—at least at first sight—differently. In *Sturtevant v. Xerox Commercial Solutions, LLC*, a former employee sued his employer for disability discrimination, but the employer moved to dismiss and compel arbitration pursuant to the company's dispute resolution program.[214] The U.S. District Court for the Western District of Washington granted the employer's motion, distinguishing *Neuson* on the grounds that the employee in *Sturtevant* did not produce evidence of a genuine factual dispute under Washington law.[215] The employee asserted that he never signed the agreement and claimed that this presented a genuine issue of material fact, relying on *Neuson* for the proposition that an electronic signature on an arbitration agreement is not reliable when the employer had access to the employee's identifying information.[216] The court

211. *Id.* at 1055–56.

212. *Id.* at 1056.

213. *Id.* (emphasis added).

214. Sturtevant v. Xerox Com. Sols., LLC, No. C16-1158RSM, 2016 WL 4992468, at *1–2 (W.D. Wash. Sept. 19, 2016).

215. *Id.* at *3–5.

216. *Id.*

analyzed *Neuson* and distinguished it on the grounds that, unlike the employee in *Neuson*, the employee in *Sturtevant* never produced evidence that he failed to receive relevant forms and never produced evidence that the employer had an opportunity to forge his electronic signature.[217] Indeed, the employer had included the arbitration agreement with the online employment application, and argued there was no way the employee could have applied for the job without electronically signing the agreement.[218]

3. Case Law

Ever since the enactment of ESIGN and UETA, the courts have borne the primary responsibility of determining the legal validity of electronic signatures because neither ESIGN nor UETA specifies the technological requirements for electronic signatures.

One example is case law on the interaction between the U.S. Copyright Act and ESIGN. The former requires that assignments be in writing.[219] After ESIGN was enacted, an open question was whether this writing requirement could be satisfied by electronic signatures or whether it required a handwritten signature.[220] In *Vergara Hermosilla v. Coca-Cola Co.*, a federal district court held that the Copyright Act's requirement that an agreement to convey copyright ownership must be "in writing and signed by the owner of the rights conveyed"[221] was satisfied by an agreement reached via e-mail.[222] The Southern District of Florida held that the songwriter plaintiff assigned his rights to a copyrighted work when he and the defendant agreed to the assignment via e-mail. Citing prior case law and ESIGN, the court stated that "emails [] constitute signed writings."[223]

In a different case, a federal appellate court agreed, similarly holding that that requirement was satisfied by electronic agreement to a website operator's terms of use.[224] In *Metropolitan Regional Information Systems v. American Home Realty Network, Inc.*, the Court of Appeals for the Fourth Circuit held that

217. *Id.*

218. *Id.*

219. 17 U.S.C. § 204.

220. *See* MELVILLE B. NIMMER & DAVID NIMMER, 3 NIMMER ON COPYRIGHT § 10.03 (Matthew Bender, rev. ed. 2021) ("How do these features apply to the copyright sphere? Nothing about ESIGN Act overtly mentions copyrights in particular or other federal enactments in general. But it does purport to apply 'to any transaction in or affecting interstate or foreign commerce.' That formulation immediately raises the imputation that it applies to some copyright grants, and not to others. For instance, Eminem's grant of his rap music implicates commerce in a significant way. But a ditty composed by an anonymous songwriter could be one of many copyrights that, if granted, would seem not to exert any meaningful impact on interstate or foreign commerce. By itself, that disparity creates an open issue whether e-mails and like devices may serve as vehicles to grant copyright interests." (citations omitted)).

221. 17 U.S.C. § 204.

222. Vergara Hermosilla v. Coca-Cola Co., No. 10-21418-CIV, 2011 WL 744098, at *3 (S.D. Fla. Feb. 23, 2011), *aff'd*, 446 F. App'x 201 (11th Cir. 2011).

223. *Id.* (citing Lamle v. Mattel, Inc., 394 F.3d 1355 (Fed. Cir. 2005)).

224. Metro. Reg'l Info. Sys. v. Am. Home Realty Network, Inc., 722 F.3d 591, 602 (4th Cir. 2013).

electronically transferring copyright ownership of photographs on a real estate website—by clicking "yes" to the terms of use of the website prior to uploading the photographs—satisfied the requirement that such an agreement must be "in writing and signed by the owner of the rights conveyed."[225] The court stated that failing to recognize "copyright transfer agreements solely because they were made electronically would thwart the clear congressional intent embodied in [ESIGN]."[226]

Similarly, another federal appellate court held that the Federal Arbitration Act's "written provision" requirement[227] was satisfied by a mass e-mail notice sent out to employees.[228] In *Campbell v. General Dynamics Government Systems Corp.*, the Court of Appeals for the First Circuit held that ESIGN "prohibits any interpretation of the [Federal Arbitration Act's] 'written provision' requirement that would preclude giving legal effect to an agreement solely on the basis that it was in electronic form."[229] *Klein v. Delbert Services Corp.*, a recent case in the Northern District of California, echoed the holding of *Campbell* and held that checkmarks in a web form "are sufficient to establish [defendant's] acceptance of the terms of the Note and the arbitration provision."[230]

It is not just ESIGN that has been subject to court rulings. State courts have addressed questions of authenticity of electronic signatures under UETA as well. For example, an employee in *Ruiz v. Moss Brothers Auto Group, Inc.* sued his employer for various wage and hour violations and his employer petitioned to compel arbitration based on an agreement to arbitrate all employment-related disputes.[231] The trial court denied the employer's petition, holding that the employer had not met its burden under California's version of UETA to establish that the employee was actually the one who executed his electronic signature, and the California Court of Appeal affirmed.[232] The employer's personnel records custodian summarily asserted that Ruiz electronically signed the agreement and that the same agreement was presented to all persons who seek

225. *Id.* at 600–01 (quoting 17 U.S.C. § 204(a)).

226. *Id.* at 602. It should be noted that the leading treatise on copyright law in the United States has cautioned against relying on the holding in *Metropolitan Regional*, stating:

> In the physical world, a piece of paper bearing ink containing the handwritten signature of the copyright owner suffices to memorialize a transfer. In the electronic world, devices such as [a digital signature block produced in Adobe Acrobat] serve the same role. Because the gulf separating those deliberate devices from the type of blanket assent validated by *Metropolitan Regional* is so vast, it is respectfully submitted that the Fourth Circuit's ruling should not be followed.

3 NIMMER & NIMMER, *supra* note 220, § 10.03 (citations omitted).

227. 9 U.S.C. § 2.

228. Campbell v. Gen. Dynamics Gov't Sys. Corp., 407 F.3d 546, 555 (1st Cir. 2005).

229. *Id.* at 556.

230. Klein v. Delbert Servs. Corp., No. 15-CV-00432-MEJ, 2015 WL 1503427, at *5 (N.D. Cal. Apr. 1, 2015).

231. Ruiz v. Moss Bros. Auto Grp., Inc., 181 Cal. Rptr. 3d 781, 783 (Ct. App. 2014).

232. *Id.*

or seek to maintain employment with the employer, and she did not explain how she verified that the employee electronically signed the agreement.[233] She explained that "[e]ach employee is required to log into the Company's HR system—each with his or her unique login ID and password—to review and electronically execute the Employee Acknowledgement form, which includes the arbitration agreement."[234] However, because the employee did not recall signing the agreement and stated that she would not have done so, she needed to explain how the electronic signature came to appear on the agreement, and thus, how it was the act of the employee.[235] The court stated that "[t]his was not a difficult evidentiary burden to meet, but it was not met here."[236]

Subsequent to *Ruiz*, California courts have been willing to enforce electronic signatures where the deficiencies laid out in *Ruiz* are addressed.[237] For example, in *Espejo v. Southern California Permanente Medical Group*, a former employee sued his employer for wrongful termination and whistleblower retaliation, but the employer petitioned to compel arbitration pursuant to an electronically signed arbitration agreement.[238] The trial court denied the petition, holding that the employer had not met its burden to establish the signature's authenticity.[239] The California Court of Appeal reversed and remanded, holding that the employer adequately addressed all of the concerns raised by the court in *Ruiz*—specifically by showing that a combination of a unique username and password were required in order for employees to sign the arbitration agreement.[240]

While usually courts come out in favor of electronic signatures, not all judicial decisions have been positive. In 2005, the *In re Vee Vinhnee* case cast a shadow over the admissibility of electronic documents generally.[241] In that case, a bankruptcy court in the Central District of California examined the process for authenticating electronic documents under the Federal Rules of Evidence and elected to use an eleven-step test for computer records developed by Professor Edward Imwinkelried.[242] Based on the Imwinkelried method, the trial court

233. *Id.* at 784.
234. *Id.* at 785.
235. *Id.* at 788.
236. *Id.*
237. *See* Espejo v. S. Cal. Permanente Med. Grp., 201 Cal. Rptr. 3d 318 (Ct. App. 2016).
238. *Id.* at 320.
239. *Id.* at 323.
240. *Id.* at 329.
241. *See In re* Vee Vinhnee, 336 B.R. 437, 444 (B.A.P. 9th Cir. 2005).
242. *Id.* at 446. The eleven steps of Imwinkelried's method include:

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.
6. The witness had the computer readout certain data.
7. The witness used the proper procedures to obtain the readout.

refused to admit electronic records of monthly billing statements submitted by the plaintiff.[243] Though the plaintiff attempted to cure its defective evidentiary foundation by submitting a declaration from a qualified witness, the court still refused to admit the electronic records because (a) the declaration failed to establish that the witness was qualified to testify as to the authenticity of the records, and (b) "the declaration did not contain information sufficient to warrant a conclusion that the '[plaintiff's] computers are sufficiently accurate in the retention and retrieval of the information contained in the documents.'"[244] The Court of Appeals for the Ninth Circuit affirmed the trial court's judgment, noting "the cursory nature of the declaration and the lack of basic information that would provide assurance that the record reproduced from the electronic media is identical to the record that was originally stored."[245] *In re Vee Vinhnee* has been cited sparingly and does not appear to have established the Imwinkelried method as a standard test for determining the admissibility of electronic documents. In fact, it merely appears to reinforce the fact-specific nature of the admissibility of electronic documents and signatures. Had the plaintiff in *In re Vee Vinhnee* offered something more than a cursory declaration, the outcome would likely have been different. It therefore remains likely that courts will enforce electronically signed documents where a party can demonstrate that the electronic signature is authentic.

Besides disputes regarding whether certain form requirements have been met, courts are occasionally confronted with a relevant document that seems to meet all applicable form requirements, but the apparent signatory claims not to have signed the document. In *Newton v. American Debt Services*,[246] the plaintiff tried to avoid an arbitration clause based on the assertion the defendant lacked proof that plaintiff was the one who signed the relevant contract. The plaintiff did not actually dispute that she signed the contract, but merely challenged the defendant based on an alleged lack of evidence. In response, the defendant corporation substantiated that it had used the DocuSign electronic signature product to send the relevant contract to the plaintiff for her signature, she had opened the document for review, created a signature, and clicked a button confirming her signature once she had completed all form fields and signed in

8. The computer was in working order at the time the witness obtained the readout.

9. The witness recognizes the exhibit as the readout.

10. The witness explains how he or she recognizes the readout.

11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

Id.

243. *Id.* at 439–40. The plaintiff in the case, American Express, erroneously relied on the assumption that their electronic business records were inherently admissible under the exceptions to hearsay provided by Rule 803(6) of the Federal Rules of Evidence. *Id.*

244. *Id.* at 448.

245. *Id.* at 449.

246. Newton v. Am. Debt Servs., Inc., 854 F. Supp. 2d 712, 731 (N.D. Cal. 2012).

all required places. The court considered this sufficient evidence and upheld the electronic signature created with DocuSign.[247]

By contrast, in *Fabian v. Renovate America, Inc.*,[248] the plaintiff expressly stated that she did not sign the relevant contract. Defendant referred summarily to an electronic signature created with DocuSign's technology, but did not substantiate how this signature was created, by whom, and following what process. The court sided with plaintiff and noted that:

> Renovate's reliance on *Newton* is misplaced because, unlike here, the declarant in that case proved that the "docusigned" electronic signature was the plaintiff's by explaining the process used to verify the signature. There, the defendant submitted a declaration stating that it sent a contract to the plaintiff using DocuSign, and that the plaintiff signed the Client Signature portion of the contract. Once signed, the signature was assigned an identifying code, such as the one that appeared above the plaintiff's signature on the subject contract.
>
> Here, Renovate did not provide any evidence from or about DocuSign in its petition, reply, or supplemental declaration. Indeed, the word "DocuSign" does not appear in any of Renovate's moving papers. Renovate offered no evidence about the process used to verify Fabian's electronic signature via DocuSign, including who sent Fabian the Contract, how the Contract was sent to her, how Fabian's electronic signature was placed on the Contract, who received the signed the Contract, how the signed Contract was returned to Renovate, and how Fabian's identification was verified as the person who actually signed the Contract. We thus find Renovate's DocuSign authentication argument unsupported and unpersuasive.[249]

It is worth noting that the court did not find any fault with DocuSign's product specifically or electronic signatures more generally, but merely noted that defendant failed to allege the necessary facts to substantiate that plaintiff signed the relevant contract. The court would presumably have come to the same conclusion if plaintiff had stated that a handwritten signature was not hers and defendant failed to allege any facts or present any evidence to the contrary.

C. COMPARING THE U.S. AND EUROPEAN MODELS

The European and American approaches to electronic signatures as set out in the preceding Subparts show a few similarities and significant differences: The two systems share a common goal of granting legal acceptance to electronic signatures.[250] In this regard, they even use similar language. Article 25(1) of

247. *Id.* at 731–32.

248. Fabian v. Renovate Am., Inc., 255 Cal. Rptr. 3d 695, 697 (Ct. App. 2019).

249. *Id.* at 701 (citing *Newton*, 854 F. Supp. 2d at 731).

250. For example, in the recitals of eIDAS, "mutual recognition" is used numerous times in regard to electronic signatures. *See, e.g.*, eIDAS, *supra* note 14, recital 6, 10, 11, at 74. The prefatory note to UETA states that "the purpose of the UETA is to remove barriers to electronic commerce by validating and effectuating electronic records and signatures." UNIF. ELEC. TRANSACTIONS ACT, prefatory note (UNIF. L. COMM'N 1999).

eIDAS states "[a]n electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form," and UETA, for example in its California version, says that "[a] record or signature may not be denied legal effect or enforceability solely because it is in electronic form."[251] ESIGN almost identically states that "a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form."[252] Whereas both eIDAS and ESIGN acknowledge the legal effect of electronic signatures by clarifying that they shall not be denied such effect "solely on the ground of/because of" their electronic form, UETA positively declares that "[i]f a law requires a record to be in writing, an electronic record satisfies the law" and "[i]f a law requires a signature, an electronic signature satisfies the law."[253] Lawmakers in the European Union and the United States generally support electronic signatures.

The question of which transactions one can use electronic signatures for—and what types of signatures—varies significantly, however, between the United States and Europe. Neither ESIGN nor UETA nor eIDAS contains a whitelist of transactions which can be effectuated with electronic signatures. Form requirements can be found in myriad federal and state laws in the United States, and in European Union and national laws in Europe.

Perhaps the most important difference between the European and U.S. approaches is the fact that U.S. law does not require any specific technology for electronic signatures to be valid. Instead of naming certain security protocols or a particular licensing process, the United States only creates a general legal framework for all electronic signatures. In contrast, in Europe eIDAS provides for three types of electronic signatures, each with a different level of technological requirements.[254] Moreover, true harmonization of electronic signature laws in Europe is limited to the use of QES—the type of electronic signature with the most complicated requirements.

D. OTHER COUNTRIES

Just as e-commerce has crossed boundaries, electronic signatures have reached all corners of the world. Many countries have adopted specific laws and regulations. Some follow the European approach of specific technical requirements; others are more in line with the U.S. idea and just refer to electronic signatures in general. Still other countries pursue their own models.

251. CAL. CIV. CODE § 1633.7(a) (West 2021).
252. 15 U.S.C. § 7001(a)(1).
253. *See, e.g.*, CAL. CIV. CODE § 1633.7(c)–(d).
254. *See supra* Part V.A.**Error! Reference source not found.**

1. European-Style Regulations

The influence of the European model can be seen in several countries, even if some have adopted alternative terminology that nevertheless provides a close parallel to the tiered system of electronic signatures under eIDAS. This Subpart reviews jurisdictions that distinguish between certified and un-certified signatures. In other words, while not all of the jurisdictions below recognize SES, AES, and QES as such, all do recognize or give additional probative weight to certified or qualified signatures.

a. Argentina

In Argentina, digital and electronic signatures are regulated by the Digital Signature Law No. 25,506,[255] Executive Order No. 2628/2002,[256] and Administrative Decisions Nos. 6/2007[257] and 927/2014[258] (hereinafter referred to collectively as the DSL).

The DSL provides for two types of signatures: an "electronic signature" and a "digital signature." The DSL defines *electronic signature* as electronic data that is integrated and/or associated with other electronic data in a logical manner, using the signatory as the connector.[259] The electronic signature is not subject to any specific technological standards. The Argentine definition of electronic signature corresponds roughly to the SES.[260] On the other hand, a *digital signature*, as defined by the DSL, is the result of applying a mathematical procedure to a digital document that requires information only known by the signatory and that is capable of being verified by third parties allowing them to identify the signatory and detect any alteration of the document.[261] In order to use a digital signature, the signatory must be previously registered with a certifying licensee, who is required to obtain a license from the regulator (government) to conduct its activities.[262] Digital signatures are subject to various technological standards (some applicable to signatories themselves and others to certifying licensees). Thus, the Argentine definition of digital signature is similar to the E.U. concept of a QES.

In general, Argentinian law allows documents and contracts that do not have a specific legal form requirement to be executed in the fashion agreed

255. Law No. 25,506, Dec. 11, 2001 (Arg.), http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm.

256. Regulatory Decree No. 2628/2002, Dec. 19, 2002 (Arg.), https://www.argentina.gob.ar/normativa/nacional/decreto-2628-2002-80733/texto.

257. Administrative Decision No. 6/2007, Feb. 7, 2007 (Arg.), https://www.argentina.gob.ar/normativa/nacional/decisi%C3%B3n_administrativa-6-2007-125115/texto.

258. Administrative Decision No. 927/2014, Oct. 30, 2014 (Arg.), https://www.argentina.gob.ar/normativa/nacional/decisi%C3%B3n_administrativa-927-2014-237642/texto.

259. Law No. 25,506, Dec. 11, 2011, art. 5 (Arg.).

260. For the definition, see *supra* Part V.A.2.a.

261. Law No. 25,506, Dec. 11, 2011, art. 2 (Arg.).

262. *Id.* art. 14.

between the parties (for example, by using electronic signatures).[263] Section 1106 of the Argentine Civil and Commercial Code (CCC) expressly states that whenever the CCC requires contracts to be in writing, such a requirement would be satisfied by an electronic contract.[264]

On the other hand, digital signatures can satisfy special signature requirements if and to the extent a digital signature serves to authenticate the signatory and ensure the integrity of the instrument.[265] Electronic documents signed with a digital signature have the same effect in proof as documents signed in writing (in Spanish, *principio de prueba por escrito*).[266]

Hand-written signatures are required for public deed requirements, in which case a digital signature is not sufficient. The CCC requires certain acts to be executed by public deed, such as agreements related to the acquisition, modification, or extinction of real estate rights,[267] lease agreements,[268] and marriage contracts.[269]

In summary, Argentina does not give electronic signatures the same level of enforceability as digital signatures: there is a clear difference between digital signatures and electronic signatures, as there is in Europe between SES/AES and QES.

b. Mexico

Mexico does not have a general umbrella law for electronic signatures applicable to transactions between private entities. However, Mexico does have a law which governs the use of advanced electronic signatures for public entities that pertain to the federal public administration (including public trusts and government-owned companies). The Advanced Electronic Signature Law (LFEA) provides for the implementation and use of those signature schemes in government-related activities and transactions with citizens, including the issuance of digital certificates and the rules for homologation of digital certificates issued by different government ministries and private entities.[270] Under the law, if a particular entity covered by the law intends to release an electronic signature solution including advanced electronic signatures, government officers must follow the provisions of this law as they implement that solution. Besides that, different legal bodies have incorporated the concept of electronic signatures and addressed their validity, such as the Federal Civil

263. *See* CÓDIGO PROCESAL CIVIL Y COMMERCIAL DE LA NACIÓN [CÓD. PROC. CIV. Y COM.] [CIVIL AND COMMERCIAL PROCEDURE CODE] art. 107 (Arg.).

264. *Id.* art. 1106.

265. *See id.* art. 288.

266. *See id.* art. 314.

267. *See id.* art. 1017.

268. *See id.* art. 1234.

269. *See id.* art. 448.

270. Ley de Firma Electrónica Avanzada [Law of Advanced Electronic Signature], Diario Oficial de la Federación [DOF] 11-01-2012 (Mex.), https://www.dof.gob.mx/nota_detalle.php?codigo=5228864&fecha=11/01/2012.

Code,[271] the Federal Code for Civil Proceedings,[272] the Federal Administrative Litigation Procedural Law,[273] and the Federal Commercial Code.[274]

Mexico's Commercial Code (CC) allows the use of electronic means in the conclusion of all commercial acts.[275] The CC also provides that electronic signatures can be used when law requires the use of, or parties agree to use, a signature, if the chosen electronic signature is appropriate for the purpose for which the data message was generated or communicated.[276] The CC states that data messages are acceptable as evidence in court.[277] Handwritten signatures and data messages/electronic signatures are regarded as functionally equivalent, as long as data messages abide by the provisions of the CC and applicable regulations.[278]

For commercial transactions, the CC defines two categories of electronic signature: electronic signature (*firma electrónica*) and advanced or reliable electronic signatures (*firma electrónica avanzada o fiable*). "Electronic signature" is defined as:

> data in electronic form consigned in a data message or logically associated with, a data message, through any technology, 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 and that produces the same legal effects as the handwriting signature, being therefore admissible as evidence in court.[279]

"Advanced or reliable electronic signatures" are similar to AES.[280] While the CC does not specifically define a third category akin to QES, an AES that is supported by a certificate issued by an authorized Certificate Service Provider

---

271. Código Civil [CC] [Federal Civil Code], art. 1803, Diario Oficial de la Federación [DOF] 26-05-1928, últimas reformas DOF 11-01-2021 (Mex.).

272. Código Federal de Procedimientos Civiles [CFPC] [Federal Code of Civil Procedures], Diario Oficial de la Federación [DOF] 24-02-1943, últimas reformas DOF 9-4-2012 (Mex.).

273. Ley Federal de Procedimiento Administrativo [LFPA] [Federal Administrative Procedure Law], art. 69 C Bis., Diario Oficial de la Federación [DOF] 04-08-1994, últimas reformas DOF 18-05-2018 (Mex.).

274. Código de Comercio [CCom] [Commercial Code], art. 89, Diario Oficial de la Federación [DOF] 07-10 al 13-12-1889, últimas reformas DOF 28-03-2018 (Mex.).

275. *Id.* art. 89.

276. "Data message" is defined as information generated, sent, received or stored by electronic means, optics, or any other technology. *Id.*

277. *See id.* art. 1205. In assessing the evidential weight of such data messages, courts assess the reliability of the manner in which the data message was generated, stored, communicated, and maintained. *Id.* art. 1298-A.

278. *Id.* art. 89.

279. *Id.*

280. *See id.* art. 97. These are electronic signatures that comply with the following requirements: (a) The signature creation data are, within the context in which they are used, linked exclusively to the signatory; (b) The signature creation data were, at the time of signing, under the exclusive control of the signatory and of no other person; (c) Any alteration to the electronic signature made after the time of signing is detectable; and (d) As to the integrity of the information of the data message to which it relates, any alteration made to that information after the time of signing is detectable. *Id.*

(CSP) would in practice be a QES. CSPs need to obtain authorization from the Ministry of Economy to operate as CSPs.[281]

c. Russia

Under Russian law, a written signature is not necessarily required for a valid contract—contracts are generally valid if legally competent parties reach an agreement, whether in a physical paper document and in some instances electronically or verbally.[282]

Because the legal enforceability of electronic signatures comes up in disputes regarding the authenticity of a signature, Russia has an overarching statute that codifies the main legal framework for electronic signatures (the "Electronic Signature Law").[283] The Russian Electronic Signature Law distinguishes SES, AES, and QES and establishes different rules for each category of electronic signature.

A SES is an electronic signature which confirms the fact of the electronic signature creation by a particular person using codes, passwords, or other means.[284] An AES is an electronic signature which (i) is created by way of encryption processing of information using an electronic signature code; (ii) permits identification of a person who signed an electronic document; (iii) permits detection of any changes to the electronic document after its execution; and (iv) is created with use of electronic signature means.[285] For a QES, in addition to all the criteria applicable to AES, an electronic signature verification key has to be indicated in a qualified certificate approved by the Russian government subject to a certificate of compliance or declaration of conformity.[286]

Information in electronic form signed with QES is generally considered an electronic document equal to a paper document signed in ink unless applicable legislation requires a document to be executed on paper only.[287] QES verification keys must be specified in the relevant certificate issued by the Ministry of Digital Development, Communications and Mass Communications of the Russian Federation ("Minsvyaz") or certifying centers accredited under Minsvyaz.[288]

281. *Id.* art. 89.

282. GRAZHDANSKII KODEKS ROSSIISKOI FEDERATSII [GK RF] [Civil Code] arts. 158–60 (Russ.).

283. Federal'nyĭ Zakon RF o elektronnaya podpis' [Federal Law of the Russian Federation on Electronic Signature], SOBRANIE ZAKONODATEL'STVA ROSSIĬSKOĬ FEDERATSII [SZ RF] [Russian Federation Collection of Legislation] 2011, No. 63-FZ (Russ.).

284. *Id.* art. 5(2).

285. *Id.* art. 5(3).

286. *Id.* art. 5(4).

287. *Id.* art. 6(1).

288. *Id.* art. 14.

Russia is one of only several countries in which the parties may be required to enter into a preliminary agreement in order to utilize SES or AES.[289] This is because, as a general rule, SES and AES may be used only in specific cases provided by law. Where Russian law is silent on the possibility of using either SES or AES, there remain three possibilities: (i) QES must be used, (ii) there must be a valid prior agreement between the parties to use SES or AES, or (iii) the parties accept legally compliant rules on the use of SES and AES adopted by a system operator of electronic signatures.

Despite the fact that using SES is only explicitly prohibited in the case of documents containing state secrets,[290] the use of SES or AES in Russia is limited. The need to conclude either an agreement to use SES or to accept a system operator's rules complicates matters and makes electronic signatures less attractive. In addition, some documents and agreements are subject to state registration/notarization and have to satisfy specific requirements. Electronic signatures are therefore not sufficient in the case of agreements on transfer of participation interests in Russian limited liability companies, long-term real estate lease agreements, or certain IP contracts.

2. U.S.-Style Laws

While many countries followed the European approach of a more detailed regulation that distinguishes between different types of electronic signature and provides certain requirements for the technology to be used, others adopted a more open and technology-neutral model similar to the United States.

a. Australia

One example is Australia. The use of electronic signatures to execute documents under Commonwealth law is codified in the Electronic Transactions Act 1999 (Cth).[291] Use of electronic signatures to execute documents (including contracts or other agreements) is also covered under state or territory law.[292]

Australian law does not distinguish between SES, AES, and QES. Any transaction in the nature of a contract, agreement, or other arrangement,

289. Although this is one option among several in Russia, Taiwan expressly requires parties to agree to the use of electronic signatures before use. *See* Electronic Signatures Act (電子簽章法) art. 4, http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=J0080037 (Taiwan). Hungary has a narrower requirement for the use of electronic invoices, which require consent of the receiving party in any form which confirms the agreement of the recipient. 2007 évi CXXVII. Act CXXVII of 2007 on Value Added Tax § 175 (3)(b)) (Hung.).

290. *See* Federal Law of the Russian Federation No. 63-FZ "On Electronic Signature" dated 6 April 2011 (as amended), art. 9(4), http://www.consultant.ru/document/cons_doc_LAW_165011/ (Russ.).

291. *Electronic Transactions Act 1999* (Cth) (Austl.).

292. *Electronic Transactions Act 2000* (NSW) (Austl.); *Electronic Transactions (Victoria) Act 2000* (Vic) (Austl.); *Electronic Transactions (Queensland) Act 2000* (Qld.) (Austl.); *Electronic Transactions Act 2011* (WA) (Austl.); *Electronic Communications Act 2000* (SA) (Austl.); *Electronic Transactions (Northern Territory) Act 2001* (NT) (Austl.); *Electronic Transactions Act 2000* (ACT) (Austl.); *Electronic Transactions Act 2000* (Tas.) (Austl.).

including any non-commercial transaction, is not invalid solely because it took place by means of electronic communication.[293] If a signature is required, electronic forms can be used if (i) "a method is used to identify the person and to indicate the person's intention in respect of the information communicated;" (ii) the method used was either "as reliable as appropriate for the purpose for which the information was generated or communicated, in light of all the circumstances, including any relevant agreement; or proven in fact to have fulfilled the functions [of identification] by itself or together with further evidence;" and (iii) the person from whom the signature is required consents to that requirement being met by way of the use of the method mentioned in (i).[294] However, the legislation and instruments issued under the legislation identify certain transactions and laws that cannot rely on the provisions in the Electronic Transactions Act for validity of an electronic transaction. Examples are wills, codicils, and any other testamentary instrument (for which a handwritten signature from the person making the statement is effective, in addition to other formalities such as having that signature witnessed)[295] or transactions effecting the disposition of land in the State of South Australia (for which only a handwritten signature is effective).[296]

b. Canada

In Canada, all of the provinces and territories have enacted electronic transactions statutes.[297] With the exception of Quebec, these statutes are based substantially on the model Uniform Electronic Commerce Act (UECA), which was adopted by the Uniform Law Conference of Canada in 1999 and which sets out the basic premise that "information shall not be denied legal effect or enforceability solely by reason that it is in electronic form."[298] The UECA defines an "electronic signature" as "information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to or associated with the document."[299] Most provincial implementations of the

293. *See Electronic Transactions Act 1999* (Cth) (Austl.), pt II div 1 s 8.

294. *See id.* pt II div 1 s 10.

295. *See, e.g.*, *Succession Act 2006* (NSW) s 6 (Austl.).

296. *See, e.g.*, *Law of Property Act 1936* (SA) s 26 (Austl.).

297. Electronic Transactions Act, S.A. 2001, c E-5.5 (Can.); Electronic Transactions Act, S.B.C. 2001, c 10 (Can.); Electronic Commerce and Information Act, C.C.S.M. 2000, c E55 (Can.); Electronic Transactions Act, R.S.N.B. 2011, c 145 (Can.); Electronic Commerce Act (An Act to Facilitate Electronic Commerce by Removing Barriers to the Use of Electronic Communication), S.N.L. 2001, c E-5.2 (Can.); Electronic Commerce Act 2000, S.N.S. 2000, c 26 (Can.); Electronic Transactions Act, S.N.W.T. 2011, c 13 (Can.); Electronic Commerce Act, S. Nu. 2004, c 7 (Can.); Electronic Commerce Act, 2000, S.O. 2000, c 17 (Can.); Electronic Commerce Act, R.S.P.E.I. 1988, c E-4.1 (Can.); An Act to establish a legal framework for information technology, C.Q.L.R. 2001, c 32 (Can.); Electronic Information and Documents Act, 2000, S.S. 2000, c E-7.22 (Can.); Electronic Commerce Act, R.S.Y. 2002, c 66 (Can.).

298. UNIFORM ELECTRONIC COMMERCE ACT § 5 (UNIF. L. CONF. OF CAN. 1999), https://www.ulcc.ca/en/uniform-acts-new-order/older-uniform-acts/703-electronic-commerce/1793-uniform-electronic-commerce-act-consol-2011 (Can.).

299. *Id.* § 1(b).

UECA adopt this definition, which does not distinguish between electronic (SES) and digital (AES) signatures. Some go further: for example, New Brunswick's Electronic Transactions Act states that, without limiting or modifying the general definition, an electronic signature may include "(a) an electronic representation of the manual signature of the person signing the document, or (b) electronic information by which the person signing the document (i) provides his or her name, and (ii) indicates clearly that the name is being provided as his or her signature to the document."[300]

The UECA also allows enacting jurisdictions to provide that an electronic signature will only be valid if it identifies the person signing and if it is "reliable" for the purpose of identifying that person, in light of all the circumstances. Prince Edward Island's Electronic Commerce Act applies a strict reliability test that requires electronic signatures to be (a) uniquely linked to the signatory, (b) capable of identifying the signatory, (c) created using means that the signatory can maintain under the signatory's sole control, and (d) linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.[301] Legislation in several other provinces includes a general reliability standard where a signature is required by law and allows the regulator to prescribe specific circumstances in which such standard applies.[302] However, in practice there appears to be minimal application of these requirements to date.

Under Canadian law, contracts are generally valid if legally competent parties reach an agreement, whether they agree verbally, electronically, or in a physical paper document.[303] Only for some types of deeds and other documents, parties need to satisfy additional formal requirements under Canadian law, such as notarization before a public notary. For example, depending on the province or territory, this applies to real property transfer contracts and deeds, marriage contracts, contracts of inheritance, contracts waiving inheritance, and estate sales.[304]

300. Electronic Transactions Act, R.S.N.B. 2011, c 145, § 11(2) (Can.).

301. Electronic Commerce Act, R.S.P.E.I. 1988, c E-4.1, § 1(1)(b) (Can.).

302. *See, e.g.*, Electronic Information and Documents Act, 2000, S.S. 2000, c E-7.22, §§ 11(3)(b), 14(2)(b) (Can.); Electronic Commerce Act, 2000, S.O. 2000, c 17, §§ 8(1), 11(2) (Can.).

303. *See, e.g.*, Le Soleil Hotel & Suites Ltd. v. Le Soleil Management Ltd. 2009 BCSC 1303, paras. 323, 328 (Can.). For validity of electronic agreements, see in particular Electronic Transactions Act, S.A. 2001, c E-5.5, § 27 (Can.); Electronic Transactions Act, S.B.C. 2001, c 10, § 15 (Can.); Electronic Commerce and Information Act, C.C.S.M. 2011, c E55, § 19(1) (Can.); Electronic Commerce Act, 2000, S.O. 2000, c 17, § 16 (Can.); Electronic Information and Documents Act, 2000, S.S. 2000, c E-7.22, § 18 (Can.); UNIFORM ELECTRONIC COMMERCE ACT § 20(1)(b) (Can.).

304. *See, e.g.*, Electronic Information and Documents Act, 2000, S.S. 2000, c E-7.22, § 4(1) (Can.); Electronic Commerce Act, 2000, S.O. 2000, c 17, § 31(1) (Can.).

c. China

The main legal framework for electronic signatures in China is codified in the People's Republic of Chine (PRC) Contract Law[305] (the "Contract Law") and the PRC Electronic Signature Law.[306] According to article 11 of the Contract Law, the written requirement for a contract is satisfied if the contract takes a "form which is capable of expressing the content in a tangible manner such as formal contracts, letters and data messages (including telegrams, telexes, facsimiles, electronic data interchange and electronic mails)."[307] Moreover, article 11 provides that both the conventional written forms of contract (formal contract and letters) and digital-form data messages (such as electronic data interchange and e-mails) are legally recognized written forms of contract. Article 11 can also be read to stipulate that aside from conventional written forms of contract, a contract taking the form of a data message (such as electronic data interchange and e-mails) shall also be considered a written form contract where it "is capable of expressing the content in a tangible manner," whether such a contract in data message form is printed and kept in hard copy form or not.[308]

This legal position finds further support in the PRC Electronic Signatures Law (ESL). Article 3 of the ESL provides that "the parties to contracts or other documents used in civil activities may agree to use or not use electronic signatures or data messages."[309] Article 3 further provides that "if the parties agree to use documents in the form of data messages or with electronic signatures, they may not deny the legal validity of such documents solely based on the fact that they are in the form of data messages or with electronic signatures."[310]

PRC law does not give any preference to electronic evidence created using certain technology or methods. In other words, PRC law treats different types of electronic signatures (for example, SES, AES, and QES) the same. Therefore, all transactions that can be effectuated by use of electronic signature can be effectuated with SES, AES, or QES. This would include, for example, most types of commercial contracts. However, according to article 3 of the ESL, the following four types of documents (such as contracts) may not be valid if they are in data message or electronic form only: (1) documents pertaining to human relations, such as marriage, adoption, succession, etc.; (2) documents pertaining

305. Hé Tong Fǎ (合同法) [Contract Law] (promulgated by the Second Session of the Ninth Nat'l People's Cong., Mar. 15, 1999, effective Oct. 1, 1999), art. 11 (China), http://www.npc.gov.cn/npc/lfzt/rlyw/2016-07/01/content_1992739.htm.

306. Diàn Zǐ Qiān Míng Fǎ (电子签名法) [Electronic Signature Law] (promulgated by the Standing Comm. Nat'l People's Cong. Aug. 28, 2004, effective Apr. 1, 2005), art. 3 (China), http://www.npc.gov.cn/wxzl/gongbao/2015-07/03/content_1942836.htm.

307. Hé Tong Fǎ (合同法) [Contract Law], art. 11 (China).

308. *Id.*

309. Diàn Zǐ Qiān Míng Fǎ (电子签名法) [Electronic Signature Law], art. 3 (China).

310. *Id.*

to the transfer of rights and interests in real property, such as land, buildings, etc.; (3) documents pertaining to the suspension of public utilities such as water supply, heat supply, gas supply, electricity supply, etc.; and (4) other circumstances specified in laws and regulations where electronic documents are not appropriate.[311]

3. Other Approaches

A few countries pursue models that resemble neither the U.S. nor the European frameworks in regard to legal treatment of electronic signatures, but rather add distinct features:

a. Brazil

Electronic signatures are not highly regulated in Brazil and, in many specific areas, the framework lacks precise legal provisions. Provisional Measure 2,200-2/01 sets forth what can be considered the umbrella legal provision for electronic signatures and is commonly referred to as "ICP-Brasil" (*Infra-Estrutura de Chaves Públicas*).[312] Also, Law 11,419/06 regulates the use and acceptance of electronic signatures in documents used in the course of lawsuits (including civil, criminal, and labor claims) and amends the Brazilian Civil Procedure Code to this effect.[313]

Digital certificates that comply with ICP-Brazil rules will be presumed valid for the purposes of establishing the authenticity, integrity, and legal validity of electronic documents (as per article 10, section 1). Therefore, Brazilian law does at least somewhat distinguish between different types of electronic signatures, and an ICP-Brazil-verified signature can be seen as the Brazilian equivalent to a QES. Such an electronic document is recognized by Brazilian authorities and presumed to be a valid and authentic document. However, ICP-Brazil also expressly indicates that other electronic certifications not in compliance with ICP-Brazil requirements may be considered valid for purposes of attesting the authenticity, integrity, and legal validity of electronic documents, as long as such alternative certification is deemed valid by the parties or accepted by the person to whom the electronic document is presented.[314] This means that if parties have declared their acceptance of electronic signatures not meeting the requirements of ICP-Brazil, such electronically signed documents shall be considered valid and binding between them. This is not dissimilar to the approach taken in Russia.

311. *Id.*

312. Medida Próvisoria No. 2,200-2, de 24 de Agosto de 2001, art. 1 (Braz.), http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm.

313. Lei No. 11,419, de 19 de Dezembro de 2006, art. 1 (Braz.), http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm.

314. Medida Próvisoria No. 2,200-2, art. 10 § 2.

b. Japan

The Act on Electronic Signatures and Certification Business codifies the main legal framework for electronic signatures in Japan.[315] The Act does not differentiate between SES, AES, and QES, but only refers to "Electronic Signatures." To qualify as an "Electronic Signature," a signature must: (i) indicate that the information was created by the person who signed and (ii) make it technically possible to detect whether the document has been altered.[316]

The Act does not provide any further guidance regarding these requirements. However, electronic signatures that use encryption technology other than certain public key cryptosystems are not likely to be considered an "Electronic Signature" under the Act.

Once document is affixed with an "Electronic Signature," it is assumed to have been executed by the individual who applied the Electronic Signature.[317] However, the individual who sought and obtained the Electronic Signature has the burden of proof regarding the signer's identity.[318]

In terms of execution of documents, the Act treats Electronic Signatures like handwritten signatures; therefore, any transactions that can be effectuated by handwritten signatures (ink on paper) can also be effectuated with an Electronic Signature. However, for some types of deeds and other documents, for example, certain types of land/building lease agreements, voluntary guardianship contracts, and notarized wills, parties may need to satisfy additional formal requirements, such as notarization before a public notary.[319]

c. Nigeria

Nigeria has not yet passed an umbrella law specifically governing electronic signatures, but a number of existing laws contain rules on electronic signatures. For example, the validity and admissibility of an electronic signature is governed by the Evidence Act (as amended), which contains the most relevant provisions.[320]

Nigerian law does not distinguish between different types of electronic signatures. Until recently, every company was required to have a common seal, the use of which is regulated by the Articles of Association of the company. But, in 2020, this requirement was relaxed.[321] There are no specific provisions that contemplate whether the common seal of a company can be represented by an electronic image, and there are no judicial precedents to support the use of an

315. Denshishomei o Yobi Ninshou Sabisu Ni Kansuru Houritsu [Act on Electronic Signatures and Certification Business], Act No. 102 of 2000 (Japan), http://www.japaneselawtranslation.go.jp/law/detail/?id=109&vm=04&re=01.

316. *Id.* art. 2.

317. *Id.* art. 3.

318. *Id.* art. 4.

319. Kōshōninhō [Notary Act], Act No. 53 of 1908, art. 1 (Japan).

320. *See* Evidence Act (2011), Cap. (C14), §§ 84, 93 (Nigeria).

321. Companies and Allied Matters Act (2020) Cap. (B8), § 98 (Nigeria).

electronic image of a common seal. However, the Companies and Allied Matters Act provides that a contract of the company has been duly sealed by the company if it bears what purports to be a seal of the company attested by what purports to be the signatures of two persons who can be assured to be a director and the secretary of the company.[322] This suggests that an electronic image of the common seal of a company should suffice.

Despite the lack of general judicial recognition of electronic signatures, in 1991 the Nigerian Supreme Court adopted a definition of "signature" in *Black's Law Dictionary* which reads as follows:

> The act of putting one's name at the end of an instrument to attest to its validity; the name thus written. A signature may be written by hand, printed, stamped, typewritten, photographed, or cut from one instrument and attached to another, and a signature lithographed on an instrument by a party is sufficient for the purpose of signing it; it being immaterial what kind of instrument a signature is made: the name or mark of a person, written by that person at his or her direction. In commercial law, any name, word or mark used with the intention to authenticate a writing constitutes a signature.[323]

The above definition appears to allow for an electronic signature that would consist of a digital image of a handwritten signature, as this would be analogous to a "photographed" or "lithographed" signature. This case is binding on all courts in Nigeria and therefore serves as a good authority that an electronic signature may be recognized by the Nigerian courts. This is a notable departure from other jurisdictions that require some element of reliability for an electronic signature to be valid—instead, here, what matters is that a mark is used "with the intention to authenticate a writing."[324]

Considering this ruling, certain transactions that can be effectuated by handwritten signatures can also be effectuated by electronic signatures.

d. Singapore

In 2010, Singapore enacted an Electronic Transactions Act (ETA) that provides generally that:

> Where a rule of law requires a signature, or provides for certain consequences if a document or a record is not signed, that requirement is satisfied in relation to an electronic record if—
>
> (a) a method is used to identify the person and to indicate that person's intention in respect of the information contained in the electronic record; and
>
> (b) the method used is either—
>
> (i) as reliable as appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement; or

322. *Id.* § 69(d).
323. Tsalibawa v. Habiba [1991] 2 NWLR 461, 475 (Nigeria).
324. *See id.*

(ii) proven in fact to have fulfilled the functions described in paragraph (*a*), by itself or together with further evidence.[325]

Whoever needs to rely on the validity of an electronic signature would have to prove that the technology used meets these requirements.

If one signs with a "secure electronic signature," one can benefit from a statutory presumption that "the secure electronic signature is the signature of the person to whom it correlates; and the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record," unless that presumption is rebutted by "evidence to the contrary."[326] To benefit from the presumption, one would have to prove that the technology used qualifies as a "secure electronic signature," which requires proof of a commercially reasonable security procedure that ensures that the electronic signature is:

(a) unique to the person using it;
(b) capable of identifying such person;
(c) created in a manner or using a means under the sole control of the person using it; and
(d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated.[327]

A number of transactions are expressly excluded from the scope of the ETA, including wills, "negotiable instruments, documents of title, bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts," indentures, declarations of trust or power of attorney, and contracts for the sale of immovable property.[328] In June 2019, the Infocomm Media Development Authority published a request for comments in connection with a review of the ETA "to ensure it continues to be progressive, facilitate innovation in the Digital Economy, strengthen Singapore's position as a hub for electronic transactions, and support Digital Government efforts."[329] Another purpose was to "[e]nable more transactions under the ETA, including property transactions, Lasting Powers of Attorney, and negotiable instruments such as bills of lading; [o]ffer certainty on the use of technologies such as Distributed Ledger Technology (DLT), Smart Contracts and Biometrics; and [update] the Certification Authority (CA) framework to ensure currency with latest international standards."[330]

325. Electronic Transactions Act (2010), § 8 (Sing.).
326. *Id.* §§ 18, 19.
327. *Id.* §§ 17, 18.
328. *Id.* § 4 sched. 1.
329. *See Public Consultation on the Review of the Electronic Transactions Act*, INFOCOMM MEDIA DEV. AUTH. (June 27, 2019), https://www.imda.gov.sg/regulations-and-licensing/Regulations/consultations/Consultation-Papers/2019/Public-Consultation-on-the-Review-of-the-Electronic-Transactions-Act.
330. *See id.*

E. SUMMARY

Legislatures around the world have enacted numerous laws with different terminologies, varying categories of records and signatures, and complex rules. All laws declare an intent to support digitization, but most fall short of providing simple and clear rules to prescribe which transactions companies and consumers can effectuate with electronic records and signatures.

VI. EFFECTS OF INTERNATIONAL DIVERGENCE

As described in the preceding Part, companies and consumers face different laws and regulations governing the effectiveness, validity, recognition as evidence, and other form requirements of electronic signatures. Different jurisdictions also regulate electronic signatures differently depending on the field of law, type of transaction, or use case. In addition to diverging rules within a particular country, companies and consumers have to consider differing laws from jurisdiction to jurisdiction, which multiplies complexities. For example, a company that wants to launch an electronic commerce platform has to consider not only different form requirements in its home country for different types of transactions and use cases (including consumer sales, enterprise licenses, employment documentation, invoices, tax records, government applications, etc.), but also diverging rules in fifty U.S. states, thirty-one Member States of the European Economic Area, and more than 150 other countries in the world, plus potentially different rules even at provincial, state, or local level.

Equally, where parties to a contract or other transaction are in or act in several jurisdictions, one single document and signature may be subject to form requirements in multiple jurisdictions. For example, if a consumer in Argentina buys a book, software license, and support services package from a seller based in Switzerland on an e-commerce platform operated by a Delaware corporation headquartered in California under a contract governed by English law, the validity of the contracts concerning the three transactions may be subject to different rules under the laws of five jurisdictions, each of which may provide for different form requirements for sales of books, software licenses, and services contracts. An additional risk factor regarding contract validity to consider may be if buyers or sellers act as consumers for personal, family, or household purposes, which could trigger additional protections against unconscionable clauses in many jurisdictions. If contracts contain valid arbitration clauses, on the other hand, they may be less exposed to challenges based on national public policy grounds, as commercial arbitrators tend to be more likely to apply contracts as they are written. Contracting parties need to consider also in what situations and where they may have to enforce the contracts, including in commercial courts, before arbitration panels, in bankruptcy proceedings or via dispute resolution systems established by the platform operator. Legal uncertainties cannot be addressed simply by resorting to government-approved "qualified electronic signatures," because approvals

and licensing schemes tend to be national. A qualified electronic signature recognized in the European Union under eIDAS is not automatically recognized in any country outside the European Union.

Within the European Union, businesses and individuals find a relatively detailed, harmonized, and permissive set of rules with respect to the question which national law determines the formal validity of a commercial contract. According to the "Rome I" Regulation, a contract is formally valid if all parties are in the same country at the time of contract formation and the contract satisfies the formal requirements of either the law which governs it in substance, or the law of the country where the contract is concluded.[331] Where the parties are in different countries at the time of contract formation, the contract is "valid if it satisfies the formal requirements of the law which governs it in substance," the law of either country where the parties, or their agents, are present at the time of contract formation, or the law at the place of habitual residence of either party.[332] Therefore, the complexities concerning form requirements regarding documents that have nexus to several countries are mitigated within the European Union. But, the Rome I regulation applies primarily only to situations involving a conflict of laws relating to contractual obligations in civil and commercial matters and not, for example, to "revenue, customs or administrative matters" or a long list of other enumerated transactions.[333] Therefore, even within the European Union, businesses and individuals may have to navigate form requirements of several countries with respect to one document and resort to handwritten form just to avoid potentially overlooking a form requirement in one of several potentially applicable national laws.

In the United States, individual states define their conflicts of law rules in statutes and common law with the effect that businesses have to consider fifty different sets of rules. Other countries have enacted their own conflicts of law rules.

In light of overwhelming complexities, many businesses and consumers gravitate towards traditional means of doing business and continue to use paper and ink despite the many advantages of electronic documents and signatures noted in Part II of this Article and despite the fact that electronic commerce and signatures could be particularly effective in the cross-border context.[334]

VII. POLICY CONSIDERATIONS AND OPTIONS FOR CHANGE

In more than two decades, businesses, governments, and individuals have gathered significant experience in dealing with electronic signatures and documents. More and more people are getting comfortable with different

331. Regulation (EC) No. 593/2008, of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (Rome I), art. 11, 2008 O.J. (L 177) 6.

332. *Id.*

333. *See id.* art. 1.

334. *See supra* Part II.

electronic options for various use cases. Technologies have matured. A few electronic signature products are gaining traction and trust globally,[335] despite the fact that they do not meet all the requirements of "qualified electronic signatures" under eIDAS or similar regimes. At the same time, few organizations—let alone individuals—have adopted "qualified electronic signature" products, due to implementation costs and complexities. If enough organizations adopt qualified electronic signatures, other organizations and consumers may follow, but currently, a lack of critical mass in practice prevents significant adoption.

Consequently, legislatures around the world should revisit their national legal frameworks. If they continue to support adoption of electronic signatures and commerce as a matter of policy—as they did in the late 1990s—they should consider updating, simplifying, and internationally harmonizing laws in light of currently established electronic documentation and signature practices and based on lessons learned from the last two decades. At a minimum, they should consider upgrading mere anti-discrimination provisions (as in ESIGN) to a default recognition of the electronic form as equivalent to the written form (as in UETA). Additionally, legislatures could set out a default presumption of sufficiency for electronic signatures and/or documents that can be overridden in special legislation only subject to certain processes and with clear and unambiguous references to the general sufficiency declaration.

Moreover, businesses, government agencies, and consumers would greatly benefit from general conceptual and detailed whitelists that declare electronic signatures and/or documents sufficient for certain transactions and use cases, possibly accompanied by blacklists with cross references to existing laws that require stricter form requirements, such as notarization or recording.

In support of cross-border transactions and global commerce more generally, legislatures should consider adopting permissive conflict of law rules that recognize the validity and effect of electronic signatures and/or documents if they meet the requirements of any one jurisdiction involved. Where countries do not trust form requirements of other jurisdictions, they could work with mutual recognition or unilateral adequacy determinations, as they already do in the area of privacy laws with a significant impact on global harmonization.[336]

Legislatures should avoid excessively prescriptive regulation and rigid, statutory categorization of electronic signature types, such as SES, AES, and

335. *See* Rebecca Buckman, *Signing Up for E-Signatures*, WALL ST. J. (July 3, 2007, 12:01 AM), www.wsj.com/articles/SB118341662407555908; Austen Hufford & Maureen Farrell, *Docusign Shows Strong Demand, Closes Up 30%*, WALL ST. J. (Apr. 27, 2018), www.wsj.com/articles/docusign-shows-strong-demand-as-shares-jump-30-1524844389; John Schwartz, *E-Signatures Become Valid for Business*, N.Y. TIMES (Oct. 2, 2000), https://www.nytimes.com/2000/10/02/business/e-signatures-become-valid-for-business.html.

336. More and more countries are adopting E.U.-style data protection laws to qualify for adequacy findings by the E.U. Commission and other countries, which can help overcome trade barriers. *See, e.g.*, Lothar Determann & Chetan Gupta, *India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Actof 2018*, 37 BERKELEY J. INT'L L. 481 (2019).

QES in the European Union. Twenty years after the creation of QES in the Electronic Signature Directive of 1999, and five years after the doubling down in eIDAS of 2014, companies and consumers still have not adopted QES, and they do not seem likely to change course any time soon. Lawmakers should accept that markets, consumers, and technological progress are favoring other solutions. For example, block chain arrangements can support contract conclusion, performance, and enforcement automation with "smart contracts"[337] that are not contemplated or adequately addressed in eIDAS or in any other overly prescriptive regulation. Technology-neutral legislation is better suited to pursue the stated policy objective of support for digitization that appears in most legislation on electronic documents around the world.

National government licensing schemes for digital signature providers, such as those contemplated in the Electronic Signature Directive of 1999, eIDAS of 2014, and many national laws, are equally counterproductive. Consumers and businesses within a country may trust and adopt a particular electronic signature technology more quickly if their government grants a formal approval or license to the technology provider. But, government license requirements create additional costs, delays, and market entry barriers that can deter adoption. Moreover, national license requirements make global adoption and harmonization more difficult, as few businesses can afford to obtain licenses in multiple countries, particularly if licensing and product requirements are defined differently in national legislation and vary across borders.

To support digitization and adoption of electronic records and signatures, legislation should be fairly simple and easy to find. Based on the policy considerations and existing legislation examined in this Article, lawmakers should consider the following basic rules:

> §1. If a law requires a record to be in writing, an electronic record satisfies the law. If a law requires a signature, an electronic signature satisfies the law.
>
> §2. All legal form requirements, including, without limitation, requirements to initial clauses within a contract, to separately accept important clauses, to provide disclosures or specific information, or to deliver declaration, can be satisfied electronically, except as expressly stated in the list of actions and transactions that are subject to additional or different form requirements attached in Annex A. For the avoidance of doubt and in the interest of practical guidance, Annex B lists transactions and actions that can be rendered legally effective with any electronic records and signatures.
>
> §3. If a record or signature is created outside this jurisdiction or if parties to a contract or other transaction are in different jurisdictions, that contract, transaction, record, or signature shall be valid and effective if it satisfies the

337. *See, e.g.*, James Grimmelmann, *All Smart Contracts Are Ambiguous*, 2 J.L. & INNOVATION 1 (2019); Mark Fenwick & Erik P.M. Vermeulen, *A Primer on Blockchain, Smart Contracts & Crypto-Assets* 5 (Lex Rsch. Topics in Corp. L. & Econ., Working Paper No. 2019-3, 2019), https://ssrn.com/abstract=3379443; Angelo Borselli, Smart Contracts in Insurance. A Law and Futurology Perspective 1 (Feb. 10, 2019) (unpublished manuscript), https://ssrn.com/abstract=3318883.

> formal requirements of (a) the law which governs the substance of the contract, transaction, record, or signature, (b) the law of either country where a party or its agent is present at the time of contract formation, transaction, record creation, or signature application, or (c) the law that applies at the place of habitual residence of any party to the transaction or contract.

CONCLUSION

As we have seen, transactions, documents, and signatures are separate concepts. Transactions and other legally relevant actions, decisions, and declarations can be recorded in documents and effectuated with signatures. Documents and signatures can be created or copied electronically or in other formats. Transactions, actions, decisions, and declarations, on the other hand, exist in the abstract and independent of the electronic or other form in which they may be documented or signed.

Electronic records and signatures offer governments, companies, and individuals many advantages over ink and paper, including speed, cost savings, convenience, easier search and analysis, cheaper archiving and retrieval, automation of retention and deletion, additional options to protect authenticity and integrity, better evidence and identification, chances of scalability, opportunities to standardize and reduce variety and deviations, and arguably a plus for sustainability (don't print this Article, save a tree). Forgery concerns apply equally to electronic and ink-on-paper signatures, but electronic signature technologies offer additional security measures. A key reason that electronic records and signatures have not been more widely adopted despite significant advantages appears to be legal uncertainty regarding the validity and effectiveness of electronic form under applicable law.

People commonly ask whether electronic signatures are legal. But the more relevant questions to ask are whether electronic signatures are effective and binding, whether they meet statutory form requirements, whether they protect interests as well as handwritten signatures on paper documents, and whether one is required to create, obtain, or retain paper documents with handwritten signatures in addition to electronic records and signatures. To better answer these and other questions, one has to consult not only newer laws specifically regulating electronic signatures and documents, but also older laws prescribing form requirements. Many older laws do not contemplate modern technologies and therefore do not give clear answers as to whether one can satisfy form requirements electronically.

Numerous different form requirements apply in myriad use cases and jurisdictions with respect to particular transactions, documents, and signatures. Legal and political uncertainties hinder adoption of electronic signature products and global harmonization of applicable laws. Existing laws are complex, confusing, and diverse due to historic factors. When electronic signatures, documents, and records were first being widely adopted at the turn of the last century, lawmakers were uncertain regarding the purposes of existing form

requirements, how well electronic records and signatures could satisfy the purposes of form requirements, which technologies and products would be adopted by businesses and consumers, and what legal problems could arise from forgeries. Additionally, lawmakers had reason to be concerned that businesses and consumers would need some time to adapt to new technologies and embrace the binding effect of electronically issued declarations. These considerations may have provided a valid excuse in the mid-1990s for somewhat timid, complex, and consciously incomplete and experimental legislation, but twenty years later, they no longer do. It is time for change.

Lawmakers can and should improve electronic signature laws and harmonize them internationally with:

- clearer default rules favoring electronic form; at a minimum, Congressshould adopt UETA's default rule in ESIGN so it applies in all U.S. states;
- whitelists enumerating transactions that can be given effect with electronic documents and signatures;
- blacklists enumerating transactions that require different forms based on compelling needs; Congress should reconsider, reduce, and render more detailed the existing exceptions in ESIGN and UETA, as Singapore is considering doing, according to a request for public comments in June 2019;
- uniform terminology and simple definitions; and
- clear conflicts of law rules, ideally permissive ones, possibly paired with bilateral or multilateral recognition or adequacy arrangements to drive international harmonization.

At the same time, lawmakers should abandon overly prescriptive regulations that require qualified electronic signatures certified by nationally licensed providers, because they hinder international harmonization, have not been widely adopted in the past, and show little chance or need of being adopted going forward.

***