ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

e-Sign Rising

Technology, Privacy, and eCommerce


E-SIGN
RISING
By Dan Puterbaugh

CHEAT SHEET

- ***The beginning.*** Seventeen years ago, the ESIGN ACT confirmed that electronic signatures have the same legal status as wet-ink signatures in the United States. However, since the law's passage, e-signatures have not been fully adopted by either federal or state agencies.
- ***European front.*** The European adopted eIDAS (Regulation (EU) N°910/2014) in 2016 to meet the need for a single e-signature law across its member states.
- ***The paperless movement.*** State legislation in California, following the 1999 Uniform Electronic Transactions Act (UETA), and in Hawaii, following the governor's 2015 State of the State address, affirmed a commitment to electronic signatures in the United States.
- ***Australian advancements.*** In Australia, electronic signature laws fall into three categories: (1) minimalist laws, which allow for broad enforceability with few legal restrictions; (2) two-tier laws, which generally permit e-signatures but provide greater weight to digital signatures; and (3) prescriptive laws, which dictate specific technical methods to electronically sign a document.

For more than 15 years, observers have predicted that electronic signatures were going to replace handwritten signatures. With the advent of recent shifts in the law and policy, they may finally be right.

Electronic signatures have been legal in most major markets for more than 15 years. But due to imprecise drafting or other ambiguities in many of these laws, in-house counsel have faced a dilemma: support the client's desire for business agility or support contract enforceability. While business leaders want their agreements executed speedily so they can beat a competitor to market or recognize revenue sooner, in-house counsel have been forced to put on the brakes while they research the laws of all the jurisdictions that affect the agreement. Historically, one jurisdiction may have had a mature set of electronic signature laws while another may have had no laws at all. Although the US ESIGN Act alleviated much of the pain, varying legislation was still the norm at the state and international levels.

Adding to the confusion was a lack of understanding over the different types of electronic signatures and how regional laws treat each one. All electronic signatures from the leading providers are secure, but some, known as digital signatures in the United States and as advanced electronic signatures in the European Union, carry an extra level of assurance provided by a third party authority known as a certificate authority — which authenticates a signer's identity. In the European Union, there is even a further category of qualified electronic signatures (QES), which are validated by a certificate authority and must be stored on a qualified signature creation device, such as a smart card, USB token, or cloud-based trust service.

Different types of electronic signatures make sense in different types of situations. Most government transactions are low risk and require the security of only a basic electronic signature. Digital signatures and the extra steps they require are best reserved for high-value, high-risk agreements.

However, early laws frequently referenced digital signatures without clarifying the term. This caused many government agencies and lawyers to mistakenly believe they were required to adopt digital signatures to the exclusion of electronic signatures, and laws that were intended to streamline operations instead created inefficiencies and confusion.

Now governments are taking steps to clarify how and when electronic signatures can be used. In the United States, the federal government has updated its information management policy, and around the country, state governments are establishing laws and regulations to encourage their agencies to accept basic electronic signatures. In the European Union, the electronic identification and trust services for electronic transactions (eIDAS) regulation defines a common framework that requires all member states to recognize electronic signatures that meet its standards. In Australia, nearly every document can be signed with an electronic signature that is the legal equivalent to its wet-ink counterpart.

In short, momentum is building in favor of electronic signatures, and many in-house counsel are seeing a tipping point on the horizon. However, as in any era of rapid change, keeping up with developments is challenging. In order to use electronic signatures with confidence, legal professionals should understand the recent legislative progress.

In the United States: Moving from simply legal to promoted

Seventeen years ago, the ESIGN Act confirmed that electronic signatures have the same legal status as wet-ink signatures in the United States. Yet in the years since the law's passage, federal and state agencies have not fully adopted e-signatures despite the demand from commercial enterprises.

This slow uptake didn't go unnoticed by lawmakers. In July 2014, three of the original proponents of the ESIGN Act wrote to US Commerce Secretary Penny Pritzker to express concern about the extent, or lack of extent, to which federal agencies had embraced electronic signatures. The technology was available and the law supported it, yet government agencies continued to rely on wet-ink signatures and paper processes. A shortage of budget and resources got in the way of adopting a technology designed to solve the very problem of budget and resource shortages.

Now, government agencies are under more pressure than ever to make their operations and services more efficient, affordable, and accessible. Constituents want to conduct official business with the same ease and speed they've come to expect in their commercial transactions.

To help the public sector manage information in a more trustworthy and resilient manner, the US Office of Management and Budget (OMB) recently published revisions to the federal government's information management policy, called Circular A-130. Circular A-130 was last updated 16 years ago — when desktop computers were the norm, the first touchscreen phone was brand new, the ESIGN Act was only five months old, and, most important, cybersecurity was not yet a concern.

The earlier version of Circular A-130 did not mention electronic signatures until an appendix was added in 2003; however, the new version categorizes digital signatures as a security measure and specifically advises their acceptance across all executive levels of the government. Electronic signatures are considered so critical to securely streamlining processes, deepening automation, and delivering better service to citizens that Circular A-130 requires their use not only among employees but also among contractors. Enterprises that conduct business with government offices should take heed and be prepared to execute electronic signatures in a technology-neutral manner.

California leads the charge toward streamlining government

At the state level, agency heads are actively seeking technology-based channels to improve their delivery of services. California has frequently led the way by establishing laws to encourage its agencies to accept electronic signatures in order to enhance operational efficiency and the constituent experience. In 1995, a California law made it possible for state agencies to accept digital signatures that complied with a particular set of regulations issued by the US Secretary of State. This law, Section 16.5, was a groundbreaker, coming into existence five years before the federal law known as the ESIGN Act was signed.

As the use of electronic signatures became more popular, California enacted another law. In 1999, the state passed the Uniform Electronic Transactions Act, which decreed that signatures in electronic form, a broader definition than the earlier law, could not be denied legal effect. The following year, 2000, saw the passage of the federal ESIGN Act, which made electronic signatures equivalent to handwritten signatures across the nation.

For lawyers who were eager to see strong legal support for electronic signatures, all of these laws were a good thing — at first glance. However, a lack of cross-referencing left the laws open to ambiguous interpretation. As a result, agencies were uncertain which laws took precedence and exactly what was required. Agencies were confused. As is often the case when the path forward is

unclear, many chose to sidestep the issue and revert to old processes based on handwritten signatures. Adoption of electronic signatures was hobbled rather than helped.

This ambiguity has led to some unusual consequences, as evidenced by a California law that includes language expressly allowing the acceptance of electronic signatures to expedite permitting process for solar-energy systems. This statement would not have been necessary if a clear law was already in place. Likewise, the California cities of Palo Alto and Sacramento noted the confusion and felt compelled to enact ordinances that expressly allow city agencies to accept electronic signatures in support of efforts to increase efficiency. These steps would not have been necessary if the state had one overriding, cross-referenced law that provided agencies with coherent guidance.

> Last year, California legislators took action to clarify the use of electronic signatures with a bill that expressly allows state agencies, cities, and counties to use electronic signatures.

These stopgap measures did not go unnoticed. Last year, California legislators took action to clarify the use of electronic signatures with a bill that expressly allows state agencies, cities, and counties to use electronic signatures. In August 2016, Governor Jerry Brown signed a new law that tied the previous two laws together by defining a digital signature as a type of electronic signature and declaring that California state agencies can accept whichever type of signature is appropriate for a particular transaction. California Secretary of State Alex Padilla said the new law is an important step toward modernizing the government and will help the government “do business better” through streamlined processes and improved efficiencies.

Green Hawaii

In Hawaii, 2015 marked a push toward paperless government. That January, Governor David Ige used his State of the State address to commit to reducing the amount of paper used by the government, and 10 months later, his own office went completely paperless. Departments must submit documents to his office using an electronic routing form template, and signed documents are returned via encrypted email.

The result has been that the time to complete paperwork associated with new hires alone has been reduced by 80 percent. As Todd Nacapuy, chief information officer for the state of Hawaii, noted, “State personnel can sign with just a few clicks, so we can focus on state business and roll out new services faster.” This success has led the state to look for other processes that can be digitized. For example, soon the Hawaii Department of Health will use electronic signatures to manage signed immunization forms for 180,000 students in K-12 schools. Parents and guardians will be able to sign the forms electronically, making it faster and easier to comply with this annual process.

The governor has set the mandatory goal of implementing a secure electronic signature process across all departments. Hawaii’s Department of Human Resources was the first to take up the challenge and shift to electronic signatures for all of its departments, but other agencies are making the move as well and have either implemented electronic signatures or developed plans to do so.

eIDAS and the European Union’s single digital marketplace

In the United States, state governments have struggled to create and interpret electronic signature laws consistently in order to expedite commerce across state lines. On the other side of the Atlantic,

European governments have tangled with similar problems, but with the added complexity of international boundaries and dissimilar cultural expectations.

The European Commission has had directives in place since 1999 to enable the use of electronic signatures, but directives are subject to member state interpretation and implementation. Therefore, the first directive (eSignatures Directive 1999/93/EC) allowed member states to interpret the new law and impose their own restrictions, limitations, and exceptions. The result was a patchwork of differing approaches, with some member states interpreting the directive strictly and others taking a more liberal view. A patchwork of technical standards emerged as well, so real interoperability didn't exist — meaning that an agreement signed and encrypted in one country might or might not be securely tracked to its destination. As technology became more embedded in daily operations of government and enterprise, the inconsistencies of electronic signature laws became a serious impediment to the EU's goal of creating a single European digital market. By 2011, revising the directive became one of the European Commission's top priorities.

As a result, the European Commission adopted eIDAS (Regulation (EU) N°910/2014), which came into effect in July 2016, to meet the need for a single electronic signature law applied uniformly across all member states. While its predecessor was a directive, eIDAS is a regulation and is not subject to interpretation by the member states. It supplies a legal structure for electronic identification, signatures, seals, and documents throughout the European Union.

eIDAS established clear definitions for three types of electronic signatures:

- **Electronic signatures**, which are secure but not authenticated by a third party's digital certificate;
- **Advanced signatures**, which are encrypted and authenticated by a third party (and, as noted, are known as digital signatures in the United States); and,
- **Qualified electronic signatures (QES)**, which are encrypted, authenticated, and stored on a physical device or with a trusted cloud provider.

In addition, in the 1999 directive, cloud-based certificates were not specially recognized; a physical object was needed to use the most secure type of electronic signature. That has changed with eIDAS. Now cloud technology is an accepted component of a secure electronic signature system. This is important because cloud technology is well suited to support interoperability. In practice, that means a user can create an electronic signature with one product, and that signature can be securely tracked and received by someone using a different product.

As a direct result, the European Telecommunications Standards Institute has funded two special task forces (STF) to consider remote signature creation and validation. They are called STF 524 — TSP Signature Validation and STF 525 — TSP Signature Creation. Although these STFs have not yet fully developed their respective standards, those standards are sure to come in the coming weeks and months. They will set the stage for next-gen digital signatures enabled on mobile devices.

Electronic seals

eIDAS recognizes electronic seals. Similar to electronic signatures but only available to purely legal persons such as corporate entities, electronic seals solve the age-old question of whether a particular natural person is an authorized signer for a particular entity. Instead, any use of the entity's electronic seal will be presumed binding on that entity.

Advances in Australia

Australia has historically treated agreements differently from the United States. In Australia, an agreement can be considered binding even when terms are expressed orally, or are in writing but not signed. Nonetheless, in 1999, the Australian government formally recognized the validity of electronic signatures with the Electronic Transactions Act (ETA).

Electronic signature laws fall into three categories: minimalist laws, which allow for broad enforceability with few legal restrictions; two-tier laws, which generally permit the use of e-signatures but provide greater evidentiary weight to digital signatures; and prescriptive laws, which dictate specific technical methods to electronically sign a document.

Australia's ETA is a minimalist law that provides that no transaction will be invalidated because it was completed electronically, which is in line with the nation's historically business-friendly and technology-neutral stance.

Despite this business-friendly approach, a recent case (*Williams Group Australia Pty Ltd v. Crocker* [2016] NSWCA 265) has raised a note of caution among some Australian lawyers. The good news is that most commentators have recognized that this case turned on issues that do not affect the validity of electronic signatures generally. Nonetheless, it has been noted that the business would greatly benefit if laws relating to electronic signatures were harmonized across the country. One group of lawyers is calling for this harmonization to be one of the main agenda items at the next Council of Australian Governments meeting. It's not hard to see how this call for uniform standards could lead to implementation of a comprehensive law like eIDAS in Australia.

A framework for the future

Taken individually, these legislative changes are interesting; taken as a whole, they indicate that a major shift is underway. Electronic signature laws are becoming standardized and liberalized to an extent that makes widespread adoption possible.

Businesses have wanted to use electronic signatures for years, recognizing the efficiency, security, and convenience they provide, and as more business functions shifted to mobile technologies, the clamoring for updated electronic signature laws became even louder. However, enterprises remained hobbled by concerns that an agreement signed electronically in one jurisdiction would not stand up to litigation in another.

Now attorneys have the legal framework necessary to assure their clients on the validity of electronic signatures for use across international markets. Whether a client is in the United States, the European Union, or Australia, and whether business operations are being conducted between private entities or with government agencies, the laws are in place for businesses and governments to safely incorporate electronic signatures in their workflows.

Dan Puterbaugh

Legal Lead

Adobe Sign

Dan Puterbaugh is legal lead for Adobe Sign, Adobe’s electronic signature solution. His writing has appeared on ACCDocket.com, and in Legal IT Insider and CMSWire.