



**An Early Scorecard – Comparing Electronic Signatures  
Legislation in the US and European Union**

**Josh Bell  
Ruben Gomez  
Paul Hodge  
Viktor Mayer-Schönberger**

2002

RPP-2002-03

**Regulatory Policy Program**

**Center for Business and Government**  
John F. Kennedy School of Government  
79 John F. Kennedy Street, Weil Hall  
Cambridge, MA 02138

## **Citation**

This paper may be cited as: Bell, Josh, Ruben Gomez, Paul Hodge and Viktor Mayer-Schönberger. 2002. “An Early Scorecard – Comparing Electronic Signatures Legislation in the US and European Union.” Regulatory Policy Program Working Paper RPP-2002-03. Cambridge, MA: Center for Business and Government, John F. Kennedy School of Government, Harvard University. Comments may be directed to the authors at John F. Kennedy School of Government, Harvard University, 79 JFK Street, Cambridge, MA 02138; Email [joshbell@post.harvard.edu](mailto:joshbell@post.harvard.edu) and [Ruben\\_Gomez@ksg01@harvard.edu](mailto:Ruben_Gomez@ksg01@harvard.edu) and [Paul\\_Hodge@ksg.harvard.edu](mailto:Paul_Hodge@ksg.harvard.edu) and [Viktor\\_MS@harvard.edu](mailto:Viktor_MS@harvard.edu).

## **Regulatory Policy Program**

The Regulatory Policy Program at the Center for Business and Government provides an environment in which to develop and test leading ideas on regulation and regulatory institutions. RPP’s research aims to improve the global society and economy by understanding the impacts of regulation and creating better decisions about the design and implementation of regulatory strategies around the world. RPP’s efforts are organized around the following three core areas: regulation, markets, and deregulation; regulatory instruments; and regulatory institutions and policymaking.

The views expressed in this paper are those of the authors and do not imply endorsement by the Regulatory Policy Program, the Center for Business and Government, the John F. Kennedy School of Government, or Harvard University.

## **For Further Information**

Further information on the Regulatory Policy Program can be obtained from the program’s director, Jennifer Nash, Center for Business and Government, John F. Kennedy School of Government, 79 JFK Street, Cambridge, MA 02138, telephone (617) 384-7325, telefax (617) 496-0063, Email [jennifer\\_nash@ksg.harvard.edu](mailto:jennifer_nash@ksg.harvard.edu).

**An Early Scorecard -  
Comparing Electronic Signatures Legislation in the US and the European Union**

**Josh Bell, Ruben Gomez, Paul Hodge, and Viktor Mayer-Schönberger<sup>1</sup>**

While its cryptic wizardry remains little understood by the average citizen, electronic signatures have been dubbed a cornerstone of the information economy. Over the last two years legislatures on both sides of the Atlantic have rushed to enact electronic signature statutes to provide appropriate legal frameworks for their use.

In this essay we compare the United States ESIGN Act with the European Union Electronic Signatures Directive and provide a brief assessment of where the two sides “got it right” as legislative drivers of enhanced electronic signature use and acceptance. This brief assessment cannot substitute for a full-fledged and in-depth analysis, but we are confident it offers a helpful first overview.

**A. The background:**

On December 13, 1999, the Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures was enacted after substantial deliberations both on the EU level as well as within the member states.<sup>2</sup> The Directive's aim is to "facilitate the use of electronic signatures and to contribute to their

---

<sup>1</sup> Josh Bell (joshbell@post.harvard.edu) is the Michael von Clemm Fellow at Harvard University. Ruben Gomez (Ruben\_Gomez@ksg01.harvard.edu) is a June 2001 graduate of the John F. Kennedy School of Government with a Master in Public Policy. Paul Hodge (Paul\_Hodge@ksg.harvard.edu) is a research fellow at Harvard's Kennedy School of Government. Viktor Mayer-Schönberger (Viktor\_MS@harvard.edu) is on the Kennedy School faculty.

<sup>2</sup> Official Journal L 13, 12 of January 19, 2000.

legal recognition."<sup>3</sup> It establishes a legal framework for electronic signatures "in order to ensure the proper functioning of the internal market".<sup>4</sup> The Directive comprises twenty-eight recitals, 15 articles and four appendices. It requires implementation legislation on the national level to commence before July 19, 2001 and mandates the European Commission to review the Directive by July 19, 2003.

Roughly six months later, on June 30, 2000, President Clinton signed into law its American counterpart, the Electronic Signatures in Global and National Commerce Act<sup>5</sup> (ESIGN).<sup>6</sup> ESIGN is a "first-of-its-kind" in the United States, establishing a uniform federal law for electronic signatures, contracts, records and notices. It comprises seven articles (§ 7001-7006 and 7021). Most of the provisions of ESIGN became effective October 1, 2000, with certain provisions relating to record retention of electronic records having taken effect on March 1, 2001, and electronic records of student and other loans, insured by the United States Government, on June 30, 2001.

In essence then, both statutes have the same aim: to enhance the acceptance and use of electronic signatures by giving legal effect to electronically signed documents.

## **B. The scorecard:**

In the following analysis, we compare the two acts in their scope, area of application, treatment of liability, formal structure, infrastructural setup, and handling of the ancillary issue of confidentiality. We conclude our comparison with an overall assessment of the utility and usefulness of each statute to achieve their stated goals for enhancing the acceptance and use of electronic signatures.

### 1. Scope

---

<sup>3</sup> Article 1

<sup>4</sup> Id.

<sup>5</sup> Codified as 15 U.S.C. § 7001 (2001) et seq.

<sup>6</sup> The US statute clearly wins the contest for most preferable acronym.

While the two statutes share the same general aim, they differ very substantially in scope.

ESIGN's scope is twofold. Its primary aim is to give legal recognition to documents electronically signed. To this end it stipulates a non-discrimination "rule of validity"<sup>7</sup> mandating that legal effect, validity or enforceability of a signature, document or transaction may not be denied "solely because it is in electronic form". Despite its restrictive name ("electronic signatures" act), ESIGN extends its scope by providing a legislative framework for providing electronic records to consumers<sup>8</sup> and to the government<sup>9</sup>. As such ESIGN is not just an electronic signatures act, but also regulates the acceptance of electronic records in business-consumer and citizen-government<sup>10</sup> interactions.

The EU Directive provides a more comprehensive regulatory framework. It gives legal recognition to documents electronically signed, but it does much more. It envisions the growth of a complex network of competing and complimentary public key infrastructures (PKIs) providing electronic certificates to customers that, in turn, can be used by these customers to electronically sign documents.

Just looking at the scope one can discern the very different approach of ESIGN and the Directive. The Directive is based on a complex and mature conception of how electronic signatures are created and in general terms what organizational structure is needed. ESIGN is much narrower - and wider at the same time. It is narrower as it plainly mandates the acceptance of electronic signatures and leaves the rest to the markets to set up. It is wider as it incorporates not just rules for electronic signatures but also for the acceptance of electronic records.

## 2. Area of application

---

<sup>7</sup> 15 U.S.C. § 7001 (a)

<sup>8</sup> 15 U.S.C. § 7001 (c).

<sup>9</sup> 15 U.S.C. § 7004.

<sup>10</sup> "Citizen" here is to be understood broadly to include businesses and other entities.

Ideally, to advance electronic signatures, their use should be possible in a large variety of circumstances. This belief is reflected in the language of the statutes. The core of both statutes - the rule giving legal recognition to electronically signed documents - is broadly applicable to a vast spectrum of documents and transactions. In practice, this commitment severely constrains the applicability of both statutes'.

ESIGN's largest constraint in applicability is its solely addressing business-to-consumer transactions. Any transaction governed by the Uniform Commercial Code (other than sections 1-107, 1-206 and Articles 2 and 2A) is not subject to ESIGN's general "rule of validity". While this does not preclude contractual partners in the B2B sector from using electronic signatures, it leaves it to the parties to agree on their validity. Electronic signatures are to be generally accepted in consumer markets only. In a less controversial move, ESIGN excludes wills and similar acts along with documents and transactions governed by family law. In a setback to electronic government, court documents are also excluded from ESIGN. Finally, and more troubling from a business perspective, specific consumer protection rules exclude "cancellation or termination of utility services", documents relating to the use of a primary residence of an individual, cancellation of life insurance, product recalls and accompanying documents required when transporting or handling hazardous material. Continental European lawyers may shiver when reading this casuistic laundry list of exceptions to ESIGN, but American jurists are familiar with the legislative compromises necessary to assure swift congressional passage.

At a glance, Article 5 of the EU Directive, providing legal recognition of electronic signatures, is clearer and more broadly applicable. It covers all transactions from B2C to B2B and does not provide exceptions for specific transactional types. A closer look, however, reveals that the devil is - as usual - in the details.

Article Five contains two parts. The first part mandates that *advanced* electronic signatures are legally equivalent to a hand-written signature and admissible as evidence in legal proceedings. However, these advanced electronic signatures must be "based on a qualified certificate" and "created by a secure-signature-creation device". The second part stipulates that electronic signatures are "not denied legal effectiveness and admissibility as evidence [...] solely on the grounds that [it] is in electronic form."

Only a closer look reveals that the EU Directive envisions two different kinds of electronic signatures: a simple electronic signature and an "advanced" electronic signature using "qualified certificates"<sup>11</sup> and "secure-signature-creation-devices."<sup>12</sup> A "qualified" certificate, however, can only be provided by a special "certification-service-provider"<sup>13</sup>, who fulfills the requirements of the Directive's Annex II. The Directive links these two types of signatures with two classes of legal recognition. Simple electronic signatures cannot be denied legal recognition just because they are electronic. But they need not be accepted either. The advanced electronic signatures based on qualified certificates issued by special service providers, however, are to be legally recognized. Not surprisingly, everyone is better off using the "advanced" signatures.

Even with advanced signatures, loopholes ensure that legal recognition is not always assured. Advanced signatures are only considered equivalent to hand-written signatures. If a statute requires more than a hand-written signature - for example, a signature in the presence of a notary public- the advanced electronic signature is not legally recognized. The significance of this provision cannot be understated. In most European nations several kinds of transactions require more than a hand-written signature. Wills have to be hand-written or signed by witnesses. Real estate can only be sold and corporations

---

<sup>11</sup> A "qualified certificate" is a certificate (in the words of the Directive "an electronic attestation which links signature-verification data to a person and confirms the identity of that person) that meets the requirements of the Directive's Annex I and is provided by a certification-service-provider; see Article 2 (10).

<sup>12</sup> These are signature-creation devices, which meet the requirements of the Directive's Annex III; see Article 2 (6).

<sup>13</sup> Article 2 (10).

formed in the presence of a notary public or at the courts. This diminishes the applicability of the EU Directive even when using "advanced" electronic signatures.

### 3. Liability provisions

To advance the use of electronic signatures, regulatory frameworks must clarify the non-trivial fundamental liability issues involved. What happens if something goes wrong and an electronic signature becomes compromised? Who is liable if someone appropriates my electronic signature device by breaking into it?

The EU Directive's Article Six provides detailed liability rules. But these only apply to "qualified certificates". Certificate issuers are liable to anyone who reasonably relies on the certificate. The burden is on the provider of such certificates to prove that he has not acted negligently. However, by assigning a liability "ceiling" to individual certificates, providers may cap their monetary responsibility for any liability claims connected to the issued certificate. Article Six, however, is silent on the liability of anybody else, including providers of "simple" electronic certificates. Here, once again, the EU's two-track approach is visible. The regulated providers of certificates for "advanced" electronic signatures face a stricter level of liability, but may limit the amount of their exposure. The providers of simple electronic signatures are held accountable in accordance with national liability rules.

In contrast, E-SIGN leaves the issue of liability untouched. The only exception to this rule – an odd one - limits the liability of insurance agents and brokers<sup>14</sup>

Ultimately, in leaving liability questions unresolved, neither statute provides a framework particularly conducive to advancing the use of electronic signatures. The Directive mandates an awkward two-track approach. With varying national liability rules, it creates an uneven playing field for electronic signature service providers in Europe.

---

<sup>14</sup> U.S.C § 7001 (j): insurance agents' and brokers' liability when contracting with another party by means of an electronic signature is limited.

Alternatively, E-SIGN does not even address the issue, except in a politically motivated exception for the insurance industry. This result is not surprising. Structuring a liability regime that gives sufficient incentives, both for consumers to use electronic signatures and for companies to provide the necessary services, is a complex undertaking given the zero-sum relationship of companies and consumers. Still, despite its predictable difficulties, the resulting disregard for outstanding liability concerns is disappointing.

#### 4. Formal structure:

Both statutes try to advance electronic signature use by providing a nascent regulatory framework. Their impact, however, depends on whether the statutes are formally enforceable and applicable.

E-SIGN is a federal statute. It explicitly preempts state law<sup>15</sup> but states have two ways to overcome this general federal preemption. Firstly, by adopting, without amendments, the Uniform Electronic Transactions Act as recommended by the National Conference of Commissioners on Uniform State Laws. Secondly, by adopting technology neutral legislation consistent with E-SIGN. State and federal agencies can create regulations interpreting E-SIGN provisions, but such regulatory activity is limited to protect E-SIGN's original purpose to facilitate the expansion of electronic commerce.

The EU Directive is a European Union-level legal instrument. It directs member states to pass national laws implementing the Directive's rules. This is to accommodate different legal cultures and frameworks, as the Directive includes a number of provisions that member states "may" but do not have to implement. The disadvantage is that such flexibility creates differing national electronic signature frameworks, stifling the Directive's explicit goal of a "coherent legal framework"<sup>16</sup> across the European Union. Implementation of the Directive must commence by July 19, 2001. If a member state has not implemented by then, the Directive must be applied immediately, superseding any

---

<sup>15</sup> 15 U.S.C. § 7002.

<sup>16</sup> Recital 20.

efforts by the responsible member state government to impose a customized national framework of its own.

In the past, implementation flexibility has greatly assisted the European Union's efforts to harmonize European regional differences while still allowing member states to retain the distinct elements of their national legal cultures. The critical challenge remains striking the right balance between stringency and flexibility. The EU strongly emphasizes the necessity of building trust and reliability in electronic signatures. Furthermore, its two-track approach for simple and advanced signatures already reflects a compromise among member states.<sup>17</sup> Still, the Directive contains wording permitting substantial added discretion when extraordinary flexibility is needed for its implementation. For these reasons, when assessing the statute's value, one might argue that the Directive grants too much formal flexibility, insufficient for ensuring the necessary conditions for harmonization across Europe. Conceptually, at least, the American approach through federal preemption may be the better solution since it creates a more cohesive - and hence more predictable - legal framework.

## 5. Infrastructural Setup

ESIGN envisions the market building the necessary infrastructure for electronic signatures and does not foresee an immediate need for further regulating this growth.

The EU Directive takes a nearly opposite view. The European legislators thought it insufficient to give electronically signed documents plain legal recognition. If sensitive and important electronically signed documents become useless because a certificate provider has become hacked and compromised, or insolvent and unable to maintain security, consumers would not only be exposed to substantial risk but also lose faith in electronic signatures. The Directive's tight framework for regulated service providers aims at minimizing such risks.

---

<sup>17</sup> The British wanted a self-regulating approach similar to ESIGN, Germany and France argued for strict regulatory oversight. The two-track approach is the resulting compromise.

## 6. Ancillary issue of encryption

Both ESIGN and the EU Directive aim at advancing the use of electronic signatures to guarantee the authenticity of electronic documents. Neither mentions another important need in electronic commerce and communication: the need for confidentiality.

This is less surprising with ESIGN than with the EU Directive. ESIGN is almost singularly focused on legal recognition of electronic signatures.<sup>18</sup> However, the Directive aims for more. In addition to rules of recognition it provides a developed electronic signatures framework. Most experts see it leading to the build-up of (national and international) public key infrastructures (PKIs). But PKIs, by definition, can also be used to provide the secure encryption needed for ensuring confidentiality. In spite of this, the Directive avoids the issue of confidentiality and encryption.

The reason is less rational than expected and more pragmatic than is desirable. To avoid delays caused by policy debates on the use of encryption, the European Union designed a legal framework that permits creation of a versatile infrastructure without resolving confidentiality concerns, hence crippling its prospects by not addressing these important concerns explicitly. This is like building a multi-lane highway to only use one lane. While intended to ease encryption use by avoiding protracted policy debates, this compromise is significantly less ingenious than the American approach of leaving everything to the market.

### **C. The results:**

We have now looked at six specific dimensions of electronic signature legislation and evaluated how the US and the European Union legislation fared in each.

---

<sup>18</sup> Although it is important to keep in mind that ESIGN's electronic records provision touch on electronic record storage and retrieval and should have triggered confidentiality concerns.

These six dimensions reflect our assessment of their relative importance. To be sure, the list is incomplete and the selection subjective. It is not meant to provide more than a first comparison of the two statutes and to assess the relative merits of the solutions they incorporate.

Below is the computed scorecard, base on a scale from ● (worst) to ●●●●● (best).

	ESIGN	EU Directive
Scope	●●●○○	●●●●○
Area of Application	●●○○○	●●●●○
Liability	●○○○○	●●●○○
Formal structure	●●●●○	●●○○○
Infrastructural Setup	●○○○○	●●●○○
Encryption	●●○○○	●○○○○

Weighing each dimension equally, the EU Directive clearly "wins", 17 to 13 (on a benchmark scale of 0 to 30). Despite its numerous shortcomings, from a legislative perspective, the Directive undoubtedly emerges as the more sophisticated, innovative and creative governmental driver of electronic signature use and acceptance.

Still, we are doubtful that it will be able to realize the grand expectations it embodies. The biggest hurdle to the acceptance of electronic signatures is its reluctant use by a skeptical public. The legal frameworks are designed to put electronic signatures on equal footing with hand-written signatures. The EU Directive takes an added step by providing a regulatory framework that addresses users' concerns. But the PKIs it foresees still need to be developed by commercial enterprises. PKIs need to be viewed as a viable business model before investors back such ventures. The secure and reliable PKI for "advanced" signatures the EU Directive envisions may provide more benefits to the users and hence a stronger incentive for them to use it. But they are also more costly to construct. So far,

electronic signatures have fared badly in the market place. Even during the “irrational exuberance” of the year 2000 the European Union did not experience a wild rush of market entrants seizing on potential PKI business opportunities offered by PKIs. In Germany, one of the few European nations with national electronic signature statutes, only a small number of companies provide PKI services. In Austria, whose July 1999 electronic signature act was the first to "implement" the EU Directive, not a single provider of "qualified certificates" for advanced signatures has been admitted.

Its initial euphoria was short-lived and the market remains reluctant to investing in complex electronic signature infrastructure. This does not come as a surprise. The B2C market is thriving without the need for electronic signatures. Credit cards provide sufficient proof of authenticity of customer identities and transactions. They offer a means of guaranteed payment, and - to some extent - even dispute resolution services. The B2B market, long thought to provide most of the fuel for electronic signatures, has not offered much of a boost either. Why?

- B2B markets have evolved more slowly than predicted.
- The burst of the "dotcom bubble" forced many B2B marketplaces into bankruptcy.
- Within the B2B markets the ones focused on long-term contracts and relationships don't need electronic signatures. The business partners "know" each other, especially when the exchange is financed by large players.
- B2B spot markets, composed of short-term, cyclical, on-off business contracts, cover only a small fraction of the market.

In sum, the B2B market provides substantially fewer economic incentives for the PKI build-up than originally expected. The irony is that confidentiality and security of communication over the Internet, true needs of current B2C and B2B ecommerce, were left out of both E-SIGN and the EU Directive.

Perhaps the EU Directive aspires to do too much. In the long run, despite its legal shortcomings, the United States' E-SIGN may turn out to be the better solution. Brief, crisp, deliberately generic and unimposing (despite its ambitious name), it casts a very

narrow focus without embracing any expectations for stimulating or creating a secondary service market. Sadly, its most important and lasting advantage might be what legal analysts consider its biggest weakness: that it does not prescribe anything structurally, and that it can be easily replaced or abolished.