Jonathan Stern
Assignment: ***Briefing Paper on the Electronic Signatures in Global and National Commerce Act***
Date: September 18, 2000

BRIEFING PAPER: Background Law of E-Sign

Beginning October 1, 2000, electronic signatures, contracts and other records affecting interstate or foreign commerce will become valid and enforceable under the Electronic Signatures in Global and National Commerce Act ("E-Sign"). Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, §107(a). E-Sign is significant for electronic commerce and commerce generally since it provides equal legal validity for electronic and paper-based agreements. § 101(a)(2). In addition, E-Sign assuages the fears of many Web-site providers by formally legalizing web-based "click wrap" agreements.

E-Sign was motivated by the recognition that electronic commerce is developing at a rapid pace and that public confidence and trust in the integrity of conducting online commerce had to be preserved. Congress' zeal to enact e-commerce legislation that provides for electronic contracting is well founded. According to one study, for instance, it is expected that by 2004 the United States will transact online sales reaching $3.2 trillion. That is about half of all expected on-line sales for that year. Meanwhile, it is expected that this year's revenues will generate about $490 billion in U.S. online purchases. *The Forrester Brief,* at http://www.forrester.com/ER/research/brief.

In developing E-Sign, the drafters of the legislation worked to ensure that the legislation adhered to five elementary principles:

1) Ensuring consumer consent to the replacement of paper notices with electronic notices;
2) Ensuring that electronic records are accurate, and relevant parties can retain and access them;
3) Enhancing legal certainty for electronic signatures and records that avoids unnecessary litigation by authorizing regulators to provide interpretive guidance;
4) Avoiding unintended consequences in areas outside the scope of the bill by providing clear federal regulatory authority for records not covered by the bill's 'consumer' protections; and
5) Avoiding facilitating predatory or unlawful practices." 146 Cong. Rec. S5215-02, S5219 (daily ed. June 15, 2000) (statement of Sen. McCain).

By the time that the act finally passed, this bipartisan effort succeeded in garnering a wide range of supporters including Microsoft, Fannie Mae and the United States Chamber of Commerce.

In providing an overview of the different provisions of E-Sign, the following will analyze the extent to which the above principles have been incorporated into the Act. In so doing, this paper will also assess those scholarly debates surrounding the Act as well as the potential pitfalls which lay ahead.

I. Major Provisions Regarding Electronic Records and Signatures

A. Electronic Signatures and Technology Neutrality

The definition of electronic signature and record is broad. Section 106(5) defines electronic signatures 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." In § 106(4), the "term 'electronic record' means a contract or other record created, generated, sent, communicated, received, or stored by electronic means." Finally, the "term 'electronic' means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities." § 106(2). These definitions inform us that parties can bind themselves contractually by means other

than the traditional ink-and-pen. Beginning this October, a binding contract can be formed from both writing one's name in the body of an e-mail to providing a retinal scan that authenticates a contract and its signator.

E-Sign is intentionally technology neutral and does not promote one technology over another. Proponents of this technology-neutral approach explain that technology is rapidly changing, and since a particular technology could easily become obsolete, it would be unwise to require one. *See, e.g., Allowing Use of Electronic Signature Before the House Commerce Committee's Subcomm. on Telecommunications, Trade and Consumer Protection,* 106th Cong. (June 9, 1999) (statement of Daniel Greenwood, Deputy General Counsel, Information Technology Division Commonwealth of Massachusetts). Daniel Greenwood, Deputy General Counsel, Information Technology Division Commonwealth of Massachusetts, argues that the first digital signature legislation in the world, the 1995 Utah electronic signature statute, already exemplifies outmoded thinking by requiring that public key infrastructure technology be used in creating a digital signature. As a result, much more secure and reliable technology, such as biometrics, is excluded from being used to create an electronic signature.

The critics of the technology neutral approach have been less vocal than their counterparts. However, their critiques demand consideration. Andrew Pincus, General Counsel to the U.S. Dept. of Commerce argues that a technology-neutral approach can conceivably harm the public interest since very large transactions can be consummated through the use of inferior technology. Without a minimum standard for computer security, there is an increased risk that the security of a transaction can be compromised. Detractors also argue that technology neutrality is impossible for the government to

maintain in the event that it is a party to a contract. That is because the government will necessarily have to choose one technology over another in effecting an electronic transaction. You should note, however, that even though technology neutrality would be impossible for an agency to maintain in such a scenario, § 102(b) does explicitly exempt States (not the federal government) from having to maintain technology neutrality.

B. Consumer Protections

Where the original House version of the Act did not include any consumer protections, the Act's final version contains a number of provisions. *See HR 1714, Introduced in the House of Representatives on May 6, 1999.* First, § 101(b)(1) and 101(c)(2) provides that the consumer protection laws of every state will not be preempted. Second, Section 101(c)(1) requires that, whenever a law obligates that a consumer be provided with information in writing, a consumer shall have the option to choose whether to receive those materials electronically. In addition, that consumer must be informed as to the hardware and software requirements to access and retain the electronic records. Since this section only applies to instances where there is an existing writing or record retention requirement, companies that currently provide click-through shopping, such as Amazon.com, will not be obligated to make these disclosures. Finally, §§ 103 (a)-(b) specifically exclude the following from electronic means: probate matters, family-law matters, notices of cancellation of utility services, notices regarding the forfeiture of a primary residence, and notices related to health and safety matters. This is in order to safeguard consumer protection policies that have historically served to

adequately inform consumers of potentially life-changing events or safety issues. *See* 146 Cong. Rec. H4346-07, H4349 (daily ed. June 14, 2000) (statement of Rep. Markey).

While the above provisions do assist in providing consumers with the opportunity to make informed decisions when deciding whether to transact electronically, some groups argue that the protections do not go far enough. The Consumers Union, for instance, has raised concerns that the Act does not indicate which party would shoulder the risk in the event that an electronic signature is stolen or placed in the wrong hands. Unlike credit cards, where federal law limits an individual's loss to fifty dollars, the Act does not provide any explicit protections to the defrauded consumer. The Consumers Union furthers that there is a danger in the fact that the Act does not provide any regulatory provisions to monitor the creators and distributors of electronic signatures. Since there are not any regulatory mechanisms that would help a consumer distinguish a reliable electronic signature distributor from an unreliable one, a consumer could more easily be duped into obtaining an electronic signature that is not properly secure. *See, e.g., "E-Sign on the Dotted Line,"* USBanker, August 1, 2000.

C. Preemption

Perhaps the most contentious issue related to E-Sign is the degree and scope to which it preempts State law. Under § 102(a)(1)-(2), all State laws related to electronic signatures and contracting are preempted unless they constitute an enactment or adoption of the Uniform Electronic Transactions Act ("UETA), *or* they specify alternative procedures that fall within Titles I and II and are technologically neutral. The principle that undergirds this provision is the presumed importance of uniformity among the States.

See, e.g., 146 Cong. Rec. S5215-02 (daily ed. June 15, 2000) (statement of Sen. McCain). It is believed that by requiring States to either adopt UETA or legislation that is significantly, if not entirely, similar to E-Sign, nationwide consensus regarding the legal validity of an electronic contract can be created. As a result, consumers will be able to maintain confidence in contracting online, while companies, not having to worry about meeting contradictory State requirements, will be able to provide services more efficiently. *See, e.g., Electronic Signature: Hearing on H.R. 1714, The "Electronic Signatures in Global and Nation Commerce (E-Sign) Act" Before the House Judiciary Committee's Subcomm. on Courts and Intellectual Property,* 106th Cong. (Sept. 30, 1999) (statement of Howard Coble, Chairman, Subcommittee on Courts and Intellectual Property) and (statement of Thomas C. Quick, President and Chief Operating Officer, Quick & Reilly/Fleet Securities., Inc.).

Opponents of the preemption clauses argue that the Act unnecessarily infringes upon States rights. To begin, since the federal government is responsible in determining whether a State has complied with the statute, it is possible that every contract case involving a question of the validity or legal effect of an electronic signature could contain a federal question. This would result in federal involvement in areas where federal jurisdiction is currently not an issue. *Electronic Signature: Hearing on H.R. 1714, The "Electronic Signatures in Global and Nation Commerce (E-Sign) Act" Before the House Judiciary Committee's Subcomm. on Courts and Intellectual Property,* 106th Cong. (Sept. 30, 1999) (statement of Pamela Mead Sargent, National Conference of Commissioners on Uniform). Second, since E-Sign was motivated by a desire to respond to changing market conditions, preemption should be discouraged. That is because states

are more capable than the federal government in making swift adjustments to shifts in the market. Supporters of E-Sign respond by presenting evidence that the adoption by states of many different laws has indeed disrupted commerce. Hence, they argue, the need for uniformity is immediately pressing precisely because the economic market is moving so rapidly. Moreover, proponents of E-Sign claim that UETA serves to complement state laws while, at the same time, helping to create uniformity among the states. It is noteworthy that this claim has prompted at least one authority to encourage the federal government to create a provision that phases out the federal provisions when the states ultimately obtain near-complete uniformity. *Electronic Signature: Hearing on H.R. 1714, The "Electronic Signatures in Global and Nation Commerce (E-Sign) Act" Before the House Judiciary Committee's Subcomm. on Courts and Intellectual Property,* 106th Cong. (Sept. 30, 1999) (Andy Pincus). Indeed, this proposal makes some sense in light of the existing differences between UETA and E-Sign.

D. Differences Between UETA and E-Sign

UETA is more comprehensive than E-Sign in a number of ways, not all of which are significant. For instance, unlike E-Sign, UETA contains provisions governing the effect of the failure of a party to use an agreed security procedure. UETA, § 10. UETA also deals with the question of when an electronic record is considered sent or received. UETA, § 15. While these sections do have some import, the most important criticism of E-Sign is that UETA discusses the effect of electronic records for evidentiary purposes while E-Sign remains silent.

UETA has two primary sections that discuss the evidentiary value of material that is in electronic form. Section 9 of UETA states that evidence can be used to show that an electronic signature is to be attributed to a person. Meanwhile, § 13 specifies that electronic records cannot be denied admissibility solely because it is in electronic format. *See, e.g.,* Comments to §§ 9 and 13 *in* the final draft version of UETA ; Patricia Brumfield Fry, *Analysis and Perspective: Electronic Authentication*, ELECTRONIC COMMERCE & LAW REPORT, July 12, 2000. While it is certainly useful that UETA explicitly allows electronic records to be used for evidentiary purposes, it is unlikely that E-Sign denies their applicability. That is because, since E-Sign intends to apply the traditional laws of contract to the regime of electronic commerce, there is little reason to expect that its evidentiary worth will be denied.

It is ironic that while proponents of UETA extol its comprehensiveness in relation to E-Sign, it is E-Sign that ultimately provides greater consumer protections. UETA does not require court orders; utility termination; and regulations governing adoption, divorce or other matters of family law to continue to be processed through paper-based writings. E-Sign, however, in an effort to safeguard time-tested consumer protection policies, requires the maintenance of the paper-based form when it involves these life-altering issues. E-Sign, § 103(b).

II. Other Issues That Need to be Addressed

E-Sign contains additional provisions related to: its applicability to federal and state governments; obligations of the Secretary of Commerce to report and promote the Act in the United States and abroad; accessibility of electronic records; and an

amendment to the Child Online Protection Act. I believe that many of these issues can be addressed in footnotes or in the context of the sections described above. In addition, it may also be prudent to include a section which describes the different types of e-signature technologies that are available. I also intend to include, perhaps in a footnote, different perspectives on how risk between consumers and distributors should be spread. Lastly, I had done some preliminary reading on UCITA and its authentication procedures. It seems that UCITA may rub up against E-Sign in some very significant ways. This inconsistency has not yet merited significant scholarly attention.

III. My Unique Contribution

I have been having a tough time finding something to say that has not already been said elsewhere. I am still developing a theory, but I think that I could argue that, contrary to the weight of scholarly opinion, it would be appropriate to include a minimal regulatory scheme into the Act. I would recommend regulations that require a minimum threshold of privacy protection in permitting large transactions. I would also create an accreditation system for providers of electronic signatures.