Jonathan Stern
Box 845
Outline of Argument

Outline for Essay on the *Electronic Signatures in Global and National Commerce Act*

This paper will describe the factors that led to the enactment of E-Sign and will carefully address the wisdom of a technology neutral approach to electronic signatures. More specifically, this paper will attempt to demonstrate that technology-neutrality can have potentially disastrous effects on the user of an electronic signature since the legislation will permit unsafe transactions to take place while not explicitly stating who will shoulder the risk in the event that an electronic signature is stolen or placed in the wrong hands. In turn, I will analyze the most commonly discussed alternatives to technology neutrality, namely, technology-specific legislation and a regulatory scheme similar to the one that exist between credit card holders and credit card companies.

In assessing various methods to allocate risk, I will show that none of the various consumer protection schemes properly shield the consumer from liability in the event of theft or other non-negligent acts. To this end, I will also address consumer-related issues such as: what happens if the electronic signator does not realize that he has entered into a contract, and who will be liable in the event that an individual's signature is stolen or intercepted (the CA will most likely bear the risk although they could contract with the signator to allocate the risk differently). Ultimately, I hope to provide some clarity as to whether it is proper to permit an e-mail to create a binding contract in an environment where it is easy for hackers to steal signatures and difficult to objectively prove the (in)validity of an appropriated signature.

I. Background

This section provides a brief summary of E-Sign and discusses its relationship to the e-commerce boom and to state-sponsored electronic signature legislation. This section also highlights key provisions and describes the spectrum of electronic signature technology. *See* Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229; 146 Cong. Rec. S5215-02 (daily ed. June 15, 2000); *The Forrester Brief*, at http://www.forrestor.com/ER/research/brief; Thomas J. Smedinghoff & Ruth Hill Bro, *Moving With Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce*, 600 PLI/PAT 507 (2000); 16 different statements at Congressional hearings.

A. The Formation of E-Sign

Introduction of the importance of electronic signature law in the expansion of electronic commerce. Description of state-sponsored legislation and comparison to the objectives of the federal statute.

B. Major Issues

Pinpoint key issues related to E-Sign and the debates that have surrounded them.

1. Differences Between UETA and E-Sign

Summarize key differences between the two including UETA provisions that allow electronic signatures to be used for evidentiary purposes and E-Signs exclusion of specific utilities from falling under E-Sign.

2. Preemption

Describe how E-Sign preempts almost all states (with exception to consumer provisions) that do not adopt UETA and explain the debate over whether it is appropriate for the federal government to do so.

3. Consumer Protections

Discussion of the many consumer protections that are provided for in E-Sign. Explain how click-through shopping will be affected by the law. Present critiques of E-Sign in failing to adequately protect the consumer.

4. Technology Neutrality

Present E-Signs' approach to technology neutrality and compare to other state and international laws. Create the architecture for the debate as to whether technology-neutrality is a good thing.

II. Variety and Gradations of Electronic Signatures

Summarize the variety of devices that will constitute an electronic signature. Provide a description of the usefulness of different methods. *See* Adam White Scoville, *Clear Signatures, Obscure Signs*, 17 CARDOZO ARTS & ENT. LJ 345 (1999).

A. Shared Secrets Method

Examples include personal identification numbers, credit card numbers, and passwords. They provide the minimum level of security and authenticity of signature or record.

B. Biometric Means of Identification

Examples include fingerprints, retinal patterns, face scans, and voice recognition.

C. Digital Signatures

Best example is the Public Key Infrastructure that includes the use of certification authorities. This method provides the best assurance that the electronic record was signed by the party whose digital signature is attached and the electronic contract was not altered after it was signed.

III. Analysis: Spreading Risk Among Consumers and Distributors

Analyze three most relevant methods to allocate risk in the event of fraud; a breach in security; uncertainties regarding whether a contract has been formed. Debate the pros and cons of each method. *See* Amelia H. Boss, *Searching for Security in the Law of Electronic Commerce,* 588 PLI/PAT 401 (1999); Benjamin Wright, *Eggs in Baskets: Distributing the Risks of Electronic Signatures*, 452 PLI/PAT 63 (1996); Daniel J. Greenwood, *Risk and Trust Management Techniques for an "Open But Bounded" Public Key Infrastructure*, 38 JURIMETRICS J. 277 (1998), Michael J. Osty & Michael J. Pulcanio, *The Liability of Certification Authorities to Relying Third Parties*, 17 J. MARSHALL J. COMPUTER & INFO. L. 961 (1999); Philip S. Corwin, *Electronic Authentication: The Emerging Federal Role*, 38 JURIMETRICS J. 261 (1998); Henry H. Perritt, Jr., *Legal and Technological Infrastructures for Electronic Payment Systems,* 22 RUTGERS COMPUTER & TECH. L.J. (1996); Daniel J. Greenwood & Ray A. Campbell, *Electronic Commerce Legislation: From Written on Paper and Ink to Electronic Records and Online Authentication*, 53 BUS. LAW. 307 (1997); Jane Kauffman Winn, *Couriers Without Luggage: Negotiable Instruments and Digital Signatures*, 49 S.C. L. REV. 739 (1998); Jane Kauffman Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177 (1998); C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*, 34 SAN DIEGO L. REV. 1225 (1997); C. Bradford Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 SAN DIEGO L. REV. 1143 (1996)

A. Technology Neutrality

Evaluate E-Signs' promotion of technology neutrality. Argue that this proposal, more than any other, is most likely to shift an inordinate amount of risk on the individual providing the signature. Show how the open-ended nature can result in accidentally entering into a contract and that it might be against public policy to permit large transactions to be conducted through technologically inferior means. Demonstrate inadequacies of tort law to cover all possible situations.

B. Technology Specific

Acknowledge the danger in being tied into technology that might become obsolete. Explain that, depending on the technology selected, risk can be evenly or it can be disproportionately spread. Describe biometrics in maintaining the ceremony of contract formation. Illustrate how risk will probably be shifted towards the signator although the likelihood of fraud may be small. Focus on the merits of certain closed and open PKI and CA schemes in protecting the electronic signator and the recipient. Present PKI as a potentially effective way of dealing with fraud, security breaches and ensuring that the parties are aware that a contract has been formed.

C. Credit Card Model

Provide overview of how the credit card industry developed in the 1920s into the industry that it is today. Show that the $50 cap has been in the best interests of the consumer, banks and credit card companies. Explain the model's applicability to electronic signatures. Note that unless this model is coupled with something that is technology-specific this model will not work since it is premised on the fact that there is a modicum of uniformity in credit cards/electronic signatures and that risk can therefore be calculated.

IV Conclusion