ASSOCIATION OF AMERICAN LAW SCHOOLS 2001 ANNUAL MEETING: SECTION ON LAW AND COMPUTERS

JANUARY 5, 2001—SAN FRANCISCO, CALIFORNIA

SAVING ROSENCRANTZ AND GUILDENSTERN IN A VIRTUAL WORLD? A COMPARATIVE LOOK AT RECENT GLOBAL ELECTRONIC SIGNATURE LEGISLATION

Susanna Frederick Fischer[*]

MICHAEL MEURER:

Thank you very much. Our final speaker is Susanna Fischer. She is a professor at Catholic University. She previously served as a law lecturer at the London Guildhall University. She teaches and researches in the areas of cyberlaw, comparative law, and intellectual property law. She practiced in these fields in London and New York as a member of both the English and New York bars.

SUSANNA FISCHER:

I. INTRODUCTION

Good afternoon, everyone! I am honored to wrap up this session on such interesting and cutting-edge legal issues. I will focus today on recent global legislative initiatives designed to establish a legal framework supporting electronic signatures. As many governments worldwide increasingly seek to encourage the growth of e-commerce, the enactment of such legislation has become a priority. Proponents of electronic signature legislation undoubtedly share the views of one of the sponsors of the recent United States E-Sign

[*] Susanna Frederick Fischer is an assistant professor of law at the Columbus School of Law of The Catholic University of America in Washington, D.C. Professor Fischer can be contacted at fischer@law.edu.

legislation,[1] former Senator Spencer Abraham, who has opined that electronic signature legislation "literally suppl[ies] the pavement for the e-commerce lane of the information superhighway."[2]

The year 2000 was a banner year for electronic signature legislation worldwide. More countries enacted electronic signature legislation in 2000 than had done so in the previous five years (the first five years of such legislation).[3] I am going to take a comparative look at this legislation. Because e-commerce is so inherently global, I think that a comparative approach is particularly important.

The most striking feature of the various electronic signature laws enacted to date around the world is their lack of uniformity of approach. This is interesting in that every jurisdiction enacting such laws shares the same fundamental goal as E-Sign: to encourage the development of e-commerce by affording at least some electronic signatures an equivalent legal status to handwritten pen and ink signatures.[4] However, there is a lack of consensus as to how best to achieve this goal. As a result, we have what Dutch commentator Simone van der Hof has termed "a veritable Tower of Babel."[5]

Here is an overview of what I am going to say about this Tower of Babel situation. There are three primary legislative models for the regulation of electronic signatures. The first model is known as the "mandatory" or "prescriptive" approach, because it mandates one particular technology, namely digital signatures based on public key cryptography. The second model is the complete opposite: it is a minimalist approach that is completely technology-neutral. The third model is a hybrid of the first two. This hybrid model is expressed to be technology-neutral, but gives certain technologies the benefit of helpful legal presumptions.

These three models reveal a fundamental philosophical difference in approach as to the appropriate role of government in establishing security and trust in electronic signatures. I will suggest that this Tower of Babel situation is less than ideal for fostering e-commerce, especially when combined with a dearth of technological standards for electronic signatures. Policymakers need to remove their national blinders. I will argue that their failure to do so is likely to result in barriers to global e-commerce as well as a widening digital divide.

Before examining the three legislative models in greater detail, I will sketch out a little essential background, both as to the legal functions of electronic signatures and as to electronic signature technology.

---

[1] *See* Electronic Signatures in Global and National Commerce Act of 2000, 15 U.S.C.S. § 7001 (Supp. 2001).

[2] 146 CONG. REC. S5223 (daily ed. June 15, 2000) (statement of Sen. Abraham).

[3] *See generally* SIMONE VAN DER HOF, DIGITAL SIGNATURE LAW SURVEY, *available at* <http://rechten.kub.nl/simone/ds-lawsu.htm>.

[4] *See generally id. See also* David M. Nadler & Valerie M. Furman, *Landmark Electronic Signatures Legislation Becomes Effective,* COMPUTER & ONLINE INDUS. LIT. REP., Jan. 3, 2001, at 13, *available at* LEXIS, 2dary Library, Combined Legal Newsletters File.

[5] *See* B.P. Aalberts & S. van der Hof, *Digital Signature Blindness: Analysis of Legislative Approaches Toward Electronic Authentication* § 1.2, 7 THE EDI LAW REVIEW 1-55 (2000), *available at* <http://rechten.kub.nl/simone/ds-fr.htm>.

II. BACKGROUND

A. The Legal Functions of Electronic Signatures

Electronic signatures must serve the same essential functions as handwritten signatures, namely (i) *authentication*; (ii) *integrity*; and (iii) *non-repudiation*.[6] Authentication means ensuring that a party to a transaction is who she purports to be.[7] Integrity means ensuring that a communication has not been altered in the course of transmission.[8] And finally, non-repudiation means ensuring that a party cannot later go back on the transaction should a dispute arise.[9]

One of the most famous illustrations of a signature that failed in these essential purposes can be found in William Shakespeare's *Hamlet*.[10] Towards the end of the play, in Act V, Scene II, Hamlet delivers this confession:

> I had my father's signet in my purse,
> Which was the model of that Danish seal;
> Folded the writ up in form of th'other,
> Subscribed it, gave 't impression, plac'd it safely,
> The changeling never known.[11]

Hamlet is describing one of the most famous forgeries in English literature. Hamlet's evil uncle, Claudius, the King of Denmark, has exiled Hamlet to England, accompanied by two messengers, Rosencrantz and Guildenstern, who are unfaithful friends to Hamlet.[12] These messengers bear a letter from Claudius, sealed with the royal seal, demanding that Hamlet be executed on his arrival in England.[13] The crafty Hamlet replaces this letter with a forged letter, which he seals with a likeness of Claudius' seal.[14] The forged letter orders that the messengers be killed.[15] Hamlet's forgery is not detected, and Rosencrantz and Guildenstern unknowingly deliver their own death sentences.[16]

Poetic justice for Hamlet's false friends? Some literary critics may think

---

[6] *See* David Taylor & Felix A. Ortiz, *Encryption-Hindering the Hackers: Some Technical and Legal Issues*, *in* FOURTH ANNUAL INTERNET LAW INST. 2000, at 743, 746 (PLI Patents, Copyrights, Trademarks & Literary Prop. Handbook Series No. GO-00D6, 2000).

[7] *See* Thomas J. Smedinghoff & Ruth Hill Bro, *Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce,* 17 J. MARSHALL J. COMPUTER & INFO. L. 723, 745 (1999).

[8] *See* John F. Delaney & M. Lorrane Ford, *The Law of the Internet: A Summary of US Internet Caselaw and Legal Developments*, *in* REPRESENTING THE NEW MEDIA COMPANY, at 31, 290 (PLI Patents, Copyrights, Trademarks & Literary Prop. Handbook Series No. GO-00JH, 2001).

[9] *See* Smedinghoff & Bro, *supra* note 7, at 746.

[10] *See generally* WILLIAM SHAKESPEARE, HAMLET; *see also* Bill Zoellick, *Wide Use of Electronic Signatures Awaits Market Decisions About Their Risks and Benefits,* N.Y.STATE BAR ASS'N J., Nov/Dec. 2000, at 10, 12, 14, *available at* <http://www.nysba.org/media/barjournal/nov00/zoellick.html>.

[11] SHAKESPEARE, *supra* note 10, act 5, sc. 2.

[12] *See id.* act. 4, sc. 3.

[13] *See id.* act. 5, sc. 2.

[14] *See id.*

[15] *See id.*

[16] *See id.*

so,[17] but most ethical lawyers and business people will find this successful forgery disturbing. The seal (or signature) failed to serve at least two of its essential purposes: (i) *authentication* (that is, ensuring that the letter was *really* sent by its purported sender, Claudius); and (ii) *integrity* (that is, that the letter sent by Claudius was not changed in the course of delivery). The play does not deal with the issue of non-repudiation, but it seems quite clear that Claudius would not be willing to accept responsibility for the forged order that resulted in the deaths of Rosencrantz and Guildenstern.

Forged signatures were nothing new in Shakespeare's day. The Old Testament describes the notorious Jezebel writing letters in her husband Ahab's name and sealing them with his seal.[18] Unlike Hamlet, Jezebel did not do this to betray her husband, but rather to ensure an illicit gain of a vineyard.[19] Sadly, human nature does not appear to have improved significantly over time, and the problem of forged signatures and broken promises persist, even in this bright new era of e-commerce and technological change.

B. Electronic Signature Technology

We have moved from the seals and signet rings of Hamlet and Jezebel to the widespread use of handwritten signatures. More recently, new electronic signature technologies have been developing.

The first major electronic signature technology, generally known as "digital signatures," is based on advances in cryptography in the mid-1970s, specifically the birth of public key cryptography.[20] Public key cryptography is based on the revolutionary notion of two separate keys, one to encrypt a message and one to decrypt it.[21] One key, the public key, is made generally available, while the other key, the private key, is kept secret by its holder.[22] The two keys are mathematically related so that a message encrypted with one key can only be decrypted with the other key.[23] It is statistically impossible, even for a computer, to deduce the identity of the private key from the public key.[24]

If King Claudius had public key encryption at his disposal, and he wanted to send a message to the English Queen instructing her to kill Hamlet on his arrival in England, Claudius would encrypt his message with the English Queen's public key. The message could thus only be decrypted with the

---

[17] *See, e.g.,* Lois Simpson, *A Study of Rosencrantz and Guildenstern from Shakespeare's Hamlet,* Dec. 13, 1999, *available at* <http://www.hamlet.org/l_simpson.html>.

[18] *See* 1 *Kings* 21:8.

[19] *See* 1 *Kings* 21:7, 14-15.

[20] *See* Taylor & Ortiz, *supra* note 6 at 747-48. *See also* W. Diffie, *The First Ten Years of Public-Key Cryptograpy,* 78 PROCEEDINGS OF THE IEEE 560-77 (1988) (providing an excellent history of the development of public key cryptography by its discoverer).

[21] *See* RSA LABORATORIES, RSA LABORATORIES' FREQUENTLY ASKED QUESTIONS ABOUT TODAY'S CRYPTOGRAPHY, VERSION 4.1 § 2-1-1 (2000), *available at* <http://www.rsasecurity.com/rsalabs/faq/2-1-1.html>.

[22] *See id.*

[23] *See id.*

[24] *See* R. Jason Richards, *The Utah Digital Signature Act as "Model" Legislation: A Critical Analysis*, 17 J. MARSHALL J. COMPUTER & INFO. L. 873, 880-81 (1999).

English Queen's private key. Even if Hamlet had access to the Queen's public key, Hamlet could not read Claudius' message, and Rosencrantz and Guildenstern would have been saved.

Digital signatures use a public key infrastructure ("PKI"), in a slightly different way. They also rely on another mathematical algorithm known as a "hash function."[25] This compresses a message into a more concise version, known as the "message digest."[26] If the underlying message is changed at all, the message digest would change too.[27]

To create a digital signature for Claudius' letter to the English Queen, Claudius would first create a message digest of his letter. Claudius then encrypts the message digest with his private key—a reversal of the plain vanilla encryption scenario previously discussed. Claudius next sends *both* the encrypted message digest and the message to the English Queen. The English Queen then uses Claudius' public key to decrypt the message digest. If successful, the Queen knows that the letter was sent by Claudius, as the holder of his private key. The Queen then uses the same hash function used by Claudius to create a message digest of the letter she received from Claudius. She compares the two message digests. If there are differences, she should beware! Differences indicate that Claudius' letter was changed in the course of delivery.[28]

One problem: how does the Queen know that Claudius really holds the private key? This is a particular problem if Claudius has not personally delivered the public key to the Queen. Even if he did, the private key could be stolen or lost. A solution to this problem is to rely on a trustworthy third party to certify that a particular person is associated with a particular public key, and that that person holds the related private key.[29] This third party is generally known as a Certification Authority ("CA"). If informed by a private key holder that his or her private key has been lost or stolen, a CA can revoke the certificate for that key.[30]

Public key cryptography is not the only electronic signature technology in existence today. Companies are racing to develop other types of electronic signature technology, most prominently biometric technologies based on an individual's unique physiological or behavioral traits, such as iris scans or dynamic signature analysis.[31] As this technology has been developing, but before any particular technology has really taken off in the marketplace, a

---

[25] *See* W. Everett Lupton, Comment, *The Digital Signature: Your Identity by the Numbers,* 6 RICH. J.L. & TECH. 10, § 11 (1999), *available at* <http://www.richmond.edu/jolt/v6i2/note2.html> (describing "hashing" as "the process of creating a string of characters, also called a digest, by mapping from the full plain-text message (i.e., the use of an algorithm)").

[26] *See id.*

[27] *See id.*

[28] *See id.* at § 12.

[29] *See* Michael J. Osty & Michael J. Pulcanio, *The Liability of Certification Authorities to Relying Third Parties*, 17 J. MARSHALL J. COMPUTER & INFO L. 961, 964-65 (1999).

[30] *See* Lupton, *supra* note 25, at § 18.

[31] *See, e.g.,* THE BIOMETRIC CONSORTIUM WEB PAGE, *available at* <http://www.biometrics.org>.

growing number of jurisdictions have enacted legislation to regulate electronic signatures.

III. A COMPARATIVE LOOK AT ELECTRONIC SIGNATURES LAWS TO DATE

It took some time for a significant number of jurisdictions to enact electronic signature legislation. The earliest countries to adopt such legislation, namely Germany (1997), Italy (1997), Malaysia (1997), and Russia (1995), endorsed the prescriptive approach mandating specific technology, namely PKI.[32] These countries were strongly influenced by the prescriptive approach taken by the State of Utah in its pioneering Digital Signature Act of 1995.[33]

A. Prescriptive Legislation

The prescriptive model is founded on the argument that PKI is the only mature technology that could provide adequate security to e-commerce transactions. Proponents of prescriptive legislation contend that legal certainty is key to stimulating widespread public trust in electronic signatures.[34] Critics, on the other hand, argue that by giving legal recognition only to one type of technology, technological improvements may be stymied.[35]

Besides its endorsement of PKI technology, another typical attribute of prescriptive legislation is that it sets out an elaborate legal framework defining the rights and liabilities of the parties to an electronic transaction, including trusted third party CAs.[36] Critics of the prescriptive approach argue that prescriptive legislation overly limits the liability of CAs and imposes excessive liability risk on consumers.[37] Typical prescriptive laws, such as Malaysia's Digital Signature Act of 1997, provide that if a private key is lost or stolen due to the key holder's failure to exercise reasonable care, she will bear unlimited liability for consequential loss or damage.[38] The policy reason for this is to insulate CAs from liability where the CA could not be expected to prevent such harm or insure against it.

B. The Hybrid Model

As these critics became more vociferous, some jurisdictions, starting with Singapore in 1998, began to move toward a more market-driven legislative

---

[32] *See* Amelia H. Boss, *The Internet and the Law: Searching for Security in the Law of Electronic Commerce,* 23 NOVA L. REV. 583, 602-03, 606 (1999).

[33] *See* Utah Digital Signature Act of 1995, UTAH CODE ANN. §§ 46-3-101 to –504 (1998 & Supp. 2000).

[34] *See* Boss, *supra* note 32, at 598.

[35] *See, e.g.,* REPORT OF EXPERT GROUP TO THE ATTORNEY GENERAL OF AUSTRALIA, ELECTRONIC COMMERCE: BUILDING THE LEGAL FRAMEWORK, Executive Summary (1998), *available at* <http://www.law.gov.au/aghome/advisory/eceg/ecegreport.html>.

[36] *See, e.g.*, Utah Digital Signature Act of 1995, UTAH CODE ANN. §§ 46-3-301 to –310 (1998 & Supp. 2000).

[37] *See, e.g.,* C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws in the Electronic Commerce Marketplace,* 34 SAN DIEGO L. REV. 1225, 1233-37 (1997).

[38] *See* Digital Signature Act, 1997, § 61 (Malay.), *available at* <http://www.cca.gov/my/sign61.htm>.

model. Singapore's Electronic Transactions Act of 1998 was heavily based on the United Nations Commission on International Trade Law ("UNCITRAL") Model Law on Electronic Commerce ("MLEC"), adopted in 1996.[39] The UNCITRAL MLEC took a technology-neutral approach.[40] This also influenced other countries adopting legislation around this time such as Bermuda (1999).[41] The Singaporean law is an example of the "hybrid" or "two-tier" approach. This hybrid approach was also endorsed by the European Union Parliament/Council Directive on a Community Framework for Electronic Signatures ("E.U. Signatures Directive").[42] This directive came into force early in 2000, and must be implemented by Member States by July of 2001.[43]

The hybrid approach is founded on a policy of limited technological neutrality, typically providing, as does the E.U. Signatures Directive, that an electronic signature may not be denied legal effectiveness or admissibility solely because it is electronic.[44] However, certain favored technologies are afforded special presumptions, such as a presumption of authenticity if the electronic signature is verified by a qualified certificate meeting certain requirements.[45] Although these so-called "advanced electronic signatures" are not expressly required to be created with a particular technology, the only existing technology that appears to meet the requirements laid down by hybrid legislation like the E.U. Signatures Directive, is PKI.

Hybrid legislation typically includes some rules on the rights and duties of parties to an electronic transaction. For example, the E.U. Signatures Directive requires Member States to ensure, at minimum, that CAs are liable in damages for harm caused to someone reasonably relying on a qualified certificate for the accuracy of the information in it, unless the CA did not act negligently.[46] However, CAs must be permitted to limit their liability by specifying limitations on the use of a qualified certificate, or the value of a transaction in which it may be used.[47]

Proponents of hybrid schemes contend that they are preferable to other legislative models because they are more flexible and adaptable to new technological developments, but they also ensure a level of legal certainty that

---

[39] *See* Electronc Transactions Act, 1998 (Sing.), *available at* <http://www.lawnet.com.sg/freeaccess/ETA.htm>.

See generally UNCITRAL Model Law on Electronic Commerce, U.N. Comm'n on Int'l Trade Law, 29th Sess., U.N. Doc. Supplement No. 17 (A/51/17), Annex I (1996), *available at* <http://www.uncitral.org/english/texts/electcom/ml-ec.htm>. *See also* G.A. Res. 51/162, U.N. GAOR, 51st Sess., U.N. Doc. A/RES/51/162 (1996) (endorsing UNCITRAL Model Law).

[40] *See UNCITRAL Model Law, supra* note 40 at Guide to Enactment § I.A.6.

[41] *See* Electronic Transactions Act, 1999 (Berm.), *available at* <http://legal.06.free.bm>.

[42] *See* European Parliament and Council Directive 1999/93, 2000 O.J. (L 13) 12, *available at* <http://www.fs.dk/uk/acts/eu/esign-uk.htm>.

[43] *See id*. art. 13, § 1.

[44] *See id.* art. 5, § 2.

[45] *See id*. art. 5, § 1.

[46] *See id*. art. 6.

[47] *See id*. art. 6, § 4.

is necessary to build and maintain sufficient public trust in electronic signatures.[48] But critics of hybrid legislation argue that this approach does not permit sufficient breathing room for market forces, overprotects certain technologies at the expense of innovation, and amounts to excessive government regulation.[49]

C. Minimalist Legislation

The criticism referred to above influenced the development of the third legislative model, the "minimalist" approach. This market-worshipping approach has proved particularly popular in common law jurisdictions. E-Sign endorses a minimalist approach,[50] as does the Uniform Electronic Transactions Act ("UETA").[51] Australia and the United Kingdom have also recently enacted minimalist legislation.[52] New Zealand is currently considering pending legislation that is very similar to Australia's.[53]

Minimalist legislation is wholly technology-neutral. For example, E-Sign provides that no electronic signatures of whatever type may be denied legal effect, validity, or enforceability simply because it is in electronic form.[54] No special presumptions are given to PKI, or any other particular technology. Moreover, no special rights or duties for parties to electronic signature creation or verification are set out in minimalist legislation.

Proponents of minimalist legislation argue that the market should determine what technology will succeed.[55] Also, they contend, a minimalist approach encourages the use of more than just one type of technology. Different technologies may be preferable for different purposes. But critics contend that the minimalist approach is hopelessly vague and creates too much legal uncertainty. They fear that failure to endorse PKI may deny it sufficient support to allow it to thrive.

D. The Explosion of Legislation in 2000

In 2000, there was an explosion of electronic signature legislation in many

---

[48] *See* INTERNET LAW & POLICY FORUM, SURVEY OF INT'L ELECTRONIC AND DIGITAL SIGNATURE INITIATIVES I(B)(2), *available at* (last modified Sept. 24, 1999) <http://www.ilpf.org/digsig/survey.htm>.

[49] *See id.*

[50] *See* Electronic Signatures in Global and National Commerce Act of 2000, 15 U.S.C.S. § 7001 (Supp. 2001).

[51] *See generally* UNIF. ELECTRONIC TRANSACTIONS ACT (1999), *available at* <http://www.law.upenn.edu/bll/ulc/ulc.htm>.

[52] *See* Electronic Transactions Act, 1999 § 10 (Austl.), *available at* <http://law.gov.au/publications/ecommerce/interim3.html>; Electronic Communications Act, 2000, c. 7, § 7 (Eng.) *available at* <http://www.hmso.gov.uk/acts/acts2000/ 20000007.htm>.

[53] *See* Electronic Transactions Bill, 2000, (N.Z.), Jan. 18, 2001, *available at* <http://www.med.govt.nz/irdev/elcom/transactions/bill>.

[54] *See* 15 U.S.C.S. § 7001(a).

[55] *See, e.g.,* REPORT OF EXPERT GROUP TO THE ATTORNEY GENERAL OF AUSTRALIA, ELECTRONIC COMMERCE: BUILDING THE LEGAL FRAMEWORK, Executive Summary (1998), *available at* <http://www.law.gov.au/aghome/advisory/eceg/ecegreport.html>.

parts of the world.[56] Some of this legislation is prescriptive, such as in India, Hong Kong, Estonia, and Peru. Some is minimalist, such as Australia, Gibraltar, and Japan. And some, including much of the European legislation, is hybrid, including Austria, Finland, France, Ireland, Luxembourg, Slovenia, and Sweden. The Tower of Babel is clearly still under construction.

IV. CONCLUSION

I close with a few observations on the Tower of Babel of global electronic signature laws. First, it is extremely important for Americans not to lose sight of the fact that the minimalist approach we adopted in E-Sign (which was designed to reconcile our own American Tower of Babel of state electronic signature laws) has not been universally embraced worldwide. As in the area of privacy laws, we now find ourselves on something of a collision course with Europe, as well as some other civil law jurisdictions. Many civil lawyers are concerned that the American minimalist approach cannot be reconciled with the civil law's approach to contract formalities, which generally includes far more stringent requirements than in common law jurisdictions.

Sadly, the global initiatives promoting greater harmonization of laws have really been a case of two little too late. UNCITRAL's Working Group on Electronic Commerce recently finalized a draft Model Law on Electronic Signatures ("MLES"), which is expected to be adopted without major change by the full Commission in June of 2001.[57] But the MLES is not expected to have much effect on existing legislation. Many business entities lost confidence in the MLES due to the persistence of its adherence to a prescriptive approach mandating PKI. Although this approach has finally been abandoned, it seems unlikely that these business interests will now endorse the MLES.

Finally, it should be emphasized that too much of the world is simply uninvolved in the Tower of Babel. To my knowledge, no African country has yet enacted electronic signature legislation. In the Middle East, only Israel has electronic signature legislation.[58] In my view, it is crucial for global stability and social justice for the First World to bridge the digital divide and enable the Third World to participate to a greater extent in e-commerce. If this does not happen, we will risk becoming a world even more divided between the greedy haves and the resentful have-nots.

Thank you.

QUESTION & ANSWER SESSION:

MICHAEL MEURER:

Questions? In the back.

---

[56] *See generally* SIMONE VAN DER HOF, DIGITAL SIGNATURE LAW SURVEY, *supra* note 3.

[57] *See generally* UNCITRAL, *Recent documents of UNCITRAL and its Working Groups, Working Group on Electronic Commerce,* Mar. 2001, *available at* <http://www.uncitral.org/english/sessions/wg_ec>.

[58] *See* VAN DER HOF, DIGITAL SIGNATURE LAW SURVEY, *supra* note 3 (noting that the Israeli Knesset passed the Electronic Signature Act in March, 2001).

QUESTION:

A question for Professor Litman. What are your thoughts about the apparent disconnect between what you describe as the . . . view of the . . . government and then all of the polling data of the United States population, which suggests that a large number of people in the United States would be considered old-timers who actually would prefer to have legislation that protects their privacy and that, in addition, they actually do not engage in e-commerce because of the fear of privacy invasions?

JESSICA LITMAN:

I mean that is, I think, the typical collective action problem. The people who influence the government, in crucial respect, are people who make a business of influencing the government rather than necessarily the aggregate majorities. And, so, I think that privacy is nothing special along those lines.

AUDIENCE:

Hi, I was hoping to make—

JANE WINN:

The question for those listening on tape was: The American public seems deeply concerned about information privacy rights even if our government is disinterested, hence Professor Litman's response, which is this is another example of breakdown of democratic processes. As a commercial law professor, those of you who are not commercial law professors would not know, we are all amateur economic historians and there is an interesting feature of United States economic history that I think is relevant here. I would suggest that American consumers have already made a Faustian bargain that most people are not fully conscious of, that in the United States most consumers expect to be able to purchase whatever they want, whenever they want, because they have access to credit; and that's a very significant characteristic of American markets that is not true once you leave the United States generally.

Outside the United States, consumers still have savings! Think of that. The reason that American consumers have access to credit at levels that is unparalleled anywhere else in the civilized world, is because the institution of credit reporting grew up in the United States over a hundred years ago. In the United States, this is an aspect of economic democracy, which is not as pernicious as some that Professor Litman pointed out—the idea that large numbers of working people could borrow money and repay it as a self-amortizing loan out of their current income is a distinctly American economic institution.[1] Unsecured lending to consumers on the scale that it exists in the US is not feasible unless you have information about people's creditworthiness. The institution of collecting information about consumers is based on community merchants' associations; and it is only in the last twenty-five years or so that what were historically community-based credit bureaus

---

[1] For a history of consumer credit in the US, *see* Lendol Calder, Financing the American Dream: A Cultural History of Consumer Credit (1999).

have aggregated into the three big credit reporting services that we know today. What has happened is that Americans were accustomed to having a certain amount of information collected about them and retained about them and reused about them because in the context it *was* favorable. There was a quid pro quo that was favorable. And the institutional transformation has changed all those calculations.

So, you know, when they do these surveys and they say, like, "How do you feel about having, you know, corporations collect all this information about you and sell it?" and everyone says, like, "Oh, that's really horrible." But if you ask, "Do you feel so strongly about your privacy rights that you would be willing to pay cash for your purchases?" At that point, we have got something to negotiate because US consumers really are willing to give up some privacy if they get something in return, such as for better terms or credit. This is a big cultural difference between the US and Europe, where there is less dependence on consumer credit. The decision in Europe to have categorical information privacy rights is politically feasible because merchants in European countries do not have the institutions that we do of collecting information about consumers for credit and marketing purposes, so they are not giving anything up by recognizing strong privacy rights. Perhaps European merchants are starting to adopt U.S.-style marketing practices, but in general, they do not have them today. There is not somebody whose ox is being gored. In Europe they can pass strong privacy laws because the lobbyists are not resisting as forcefully as they are in the United States.

MICHAEL MEURER:

Can you pass that down, please? We have got a great question here and three answers from our panelists.

ELLIOT MAXWELL:

I do not believe that the United States government has been indifferent to this question of privacy. The Administration over the last four years has vigorously supported privacy legislation, with respect to financial services and with respect to medical privacy. It has strongly advocated a position that unless there were wide and deep implementation of the OECD principles on privacy that it might support legislation; and, in fact, the FTC has supported legislation. If one looks at the pattern of behavior within the e-commerce community over the last three years, there have been very positive changes in behavior with regard to privacy. And, so, to describe the government as indifferent seems to me dead wrong.

Now, the question is whether a system of privacy legislation akin to the European Privacy Directive is either desirable or, if desirable, politically feasible, is a different question. But the characterization of indifference is absolutely inappropriate I think we can debate the best way to implement the principles of notice, choice, redress, security, and the like. So, I would much rather engage on those issues rather than whether the government is indifferent.

JESSICA LITMAN:

I did not say indifferent to privacy, I said uninterested in regulating this;

and—

ELLIOT MAXWELL:

If one reads the thousands and thousands of pages of comments on medical privacy, for example, and one looks at the progress of those rules, I do not think it would be fair to say that the government has not been interested in regulations that enhance privacy protection. The Administration has taken the position that certain kinds of information are more sensitive than others and should be treated differently. It has looked to a range of actions, including self-regulation, regulation and laws, as well as technological solutions and increased education.

MICHAEL MEURER:

We'll finish this off with one more question.

QUESTION:

Actually, a reaction.

MICHAEL MUERER:

Maybe two reactions, then.

QUESTION:

I'm sorry?

MICHAEL MEURER:

One question or two reactions.

QUESTION:

Joel Reidenberg with Fordham University. I guess it is a reaction. I would agree with Elliot that the United States government has not been indifferent. I think it is a gross overstatement to say that the United States government has pushed any kind of reasonable level of fair information practice regulation in the United States. We can look, yes, there have been a couple of successes, like the HIPA regulations that have come out in the last couple of days, but if you look at areas like financial services privacy, I mean, in particular, Gramm-Leach-Bliley, as a fair information practices statute, it is mediocre at best. I think Jane's example of credit reporting is a particularly apt one because that is the one area in American law where we in fact have a very powerful privacy statute called the Fair Credit Reporting Act. If you look back to 1970 when it was enacted, the growth of the consumer credit industry in the United States has been attributed to the fact that we have *had* strong privacy protection in that field. I certainly do not see that anywhere that has come out.

ELLIOT MAXWELL:

I just want to note that the Administration did not support the final version of Gramm-Leach-Bliley and, in fact, worked actively to try to strengthen it. And so to characterize that legislation as one the Administration supported

when the Administration at the time of passage said that it would seek introduction of new legislation in the following Congress because of its lack of satisfaction with the protections in that legislation is hardly a fair characterization of the Administration's position.

JESSICA LITMAN:

Again, Elliot, I did not mean to impugn your Administration or the Commerce Department or President Clinton when I talked about the government writ large.

MICHAEL MEURER:

Thirty seconds. Thirty seconds, please.

ELLIOT MAXWELL:

There has been, and will continue to be, a very important debate about privacy in the Administration and in the Congress. I am very comfortable in saying that the Clinton-Gore Administration was not satisfied with Gramm-Leach-Bliley and has not been satisfied with how deeply and broadly the OECD principles have been adopted. I think we all have lots of hard work to do in getting better privacy protection and in determining the appropriate means to accomplish that.

MICHAEL MEURER:

Okay, I am sorry. We are going to have to cut this off and move to the business meeting. That ends the e-commerce section. Thanks very much to the panelists.