BUILDING THE LEGAL INFRASTRUCTURE FOR GLOBAL ELECTRONIC COMMERCE: PRIVACY, ELECTRONIC SIGNATURES AND CONSUMER PROTECTION

by

Richard G. Kunkel, J. D. *

The growth in electronic commerce in recent years is staggering. E-commerce revenue has grown from near zero in the mid-1990s to $110 billion dollars in 1999. [1] Industry consulting groups predict a doubling of e-commerce trade every 12 to 18 months, with one projection topping out at $4.6 trillion.[2] What is even more staggering is the potential for e-commerce in the future. To put the sales figures in context, in the first quarter of 2001, retail e-commerce sales were just 0.9 percent of total retail sales.[3] In Europe, less than five percent of Internet uses buy regularly on the Internet.[4]

The great potential of e-commerce is only slowly being realized. One contributing factor in the failure to capitalize on the potential of e-commerce is the lack of a legal infrastructure sufficient to inspire a high degree of confidence in transacting business online, whether in business-to-business (B2B) or business-to-consumer (B2C) transactions.

The ability of the law to respond in a timely way to rapid technological change is frequently tested. In these early years of electronic commerce, traditional physical world approaches to commercial law have been adapted and applied to online business on a case by case basis. In the short run, this adaptation has proven inadequate to provide the legal certainty necessary to foster thriving e-commerce. The United States and the European Union, together with other nations, have begun to take the first legislative steps needed to remove barriers that impede electronic commerce.

This paper will discuss developments in three areas: privacy, electronic signatures and consumer protection. Improvements in the legal framework in these areas are essential to inspire "e-confidence", i.e. the level of trust and legal certainty necessary for businesses and consumers to shift their business transactions from paper based transactions to online transactions. The paper will focus primarily on e-commerce developments in the United States and the European Union. The goal of the paper is not to provide an exhaustive comparison of these statutes, but rather, to bring business law educators up to date on the key developments in these areas.

The Internet is a borderless medium. The ability to easily transact business across jurisdictional borders is one great benefit of electronic commerce. However, the varying legal rules in multiple jurisdictions undermines the legal certainty needed to attract online buyers and sellers. It is becoming clear that the potential of electronic commerce will not be fully realized until at least minimum standards of privacy, electronic contracting and consumer protection are established across the jurisdictional borders of major global markets.

The European Union ("EU") and the United States have taken differing approaches to the problem of harmonizing conflicting laws. In Europe, differences in national laws of Member States impeded the ability to exploit the potential of the digital economy within the European Internal Market. The European Council recognized the need for concerted action and directed the preparation of an *e*Europe Action Plan[5] at the Lisbon European Council held March 23-24, 2000. The Action Plan was approved at the Fiera European Council on June 19-20, 2000.[6]

The Action Plan recognized that Europe trailed the United States in embracing e-commerce, and cited the need for rapid coordinated action by Member States in order to keep abreast with the U.S. and other nations in e-commerce. The goals of the Action Plan were: 1) to remove barriers to free flow of goods and services via electronic transactions in the internal market, and 2) to ensure that Europe was able to participate in shaping the future of electronic commerce rather than merely reacting to developments in the United States and elsewhere. In support of the Action Plan, the Directive on E-Commerce was enacted,[7] near the same time.

Previously the Directive on Distance Contracts[8] and the Directive on Electronic Signatures[9] had been put in place to harmonize legislation on electronic contracting in support e-commerce initiatives.

The United States has taken a more laissez-faire approach to e-commerce issues, particularly at the federal level. The U.S. approach has allowed the market to identify and respond to the major issues through self-regulation. Also, the U.S. states have been allowed to take the initiative on legislation such as the Uniform Computer Information Transactions Act (UCITA) and the Uniform Electronic Transactions Act (UETA). Federal legislation has been narrowly targeted to specific issues such as the Children's Online Privacy Protection Act (COPPA)[10] and the Health Insurance Portability and Accountability Act of 1996[11].

The latest developments in the differing approaches of the U.S. and the European Union are examined in more detail below.

---

* Associate Professor, University of St. Thomas, St. Paul, Minnesota

I. Privacy

Technological advances in the ability to obtain personal and private information, analyze it, and efficiently transmit it to others have made privacy an important consideration almost since the inception of the Internet. On a personal level, individuals need to be assured of the right to control the information collected about themselves, and to be aware of the purposes for which it will be used, how it is to be stored and transmitted to others. The early history of privacy protection on the Internet emphasized this personal right, especially in Europe.

More recently, there is growing awareness of the commercial ramifications of these privacy concerns. On a commercial level, privacy is now understood as an important barrier to confidence in transacting business online. Consumers frequently cite privacy concerns as a serious obstacle to online trading that is not easily overcome. Hence, unless adequate legal protection exists for information to be collected, transmitted and stored securely in e-commerce, the full potential of electronic commerce cannot be realized.

The differences the European and American approaches to e-commerce regulation are most pronounced in the privacy area. In Europe, privacy is considered a fundamental individual right and freedom.[12] Further, Europeans view all personal information as protected, with sensitive data receiving even greater safeguards. To protect privacy, the EU enacted the Directive on Data Privacy,[13] (hereinafter, the "Privacy Directive") which required Member States to enact legislation to implement the Privacy Directive by October 24, 1998. The Directive is a comprehensive regulatory scheme intended to protect individual privacy and to ensure free flow of personal data in the internal market of the EU.[14]

The broad reach of the Privacy Directive applies to all personal data unless used in "purely personal or household activity".[15] Personal data is defined as any information relating to an identified or identifiable natural person.[16] The Privacy Directive seeks to ensure data quality by requiring that all personal data be processed fairly and lawfully; be collected only for specified, explicit and legitimate purposes; is adequate, relevant and not excessive relative to its purpose; is accurate and is kept up to date; and is kept in identifiable form for no longer than necessary.[17]

Data controllers must use appropriate technical and organizational efforts to keep personal data confidential and secure from unauthorized disclosure or access.[18] Each EU member state must establish a supervisory authority to administer and enforce the Privacy Directive.[19] Data controllers must register with the appropriate supervisory authorities before processing begins.[20]

Processing of personal data is permitted only if "legitimate". To be legitimate under Article 7, the unambiguous consent of the data subject is required. There are exceptions for data processing necessary for contracting by the data subject, for legal obligations of the data controller, for protection of a vital interest of the data subject, or the public interest, or is necessary to other legitimate interests of the controller that are not outweighed by the privacy rights of the subject.[21]

Additional restrictions apply to special categories of sensitive data, defined as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning health or sex life.[22]

The Privacy Directive also guarantees the data subjects' rights to notice regarding gathering, maintenance and transfer of any personal data. Before collecting data, the data controller must provide the data subject with the identity of the controller, the intended purpose of the data processing, recipients of the data, notice regarding which items are required and which are voluntary, right of access to the data and the ability to correct the data and other information needed to ensure fair processing under the circumstances.[23] These same rules apply if a data controller obtains the information from a source other than the data subject.[24]

At all times the data subject is guaranteed access to the data held by the controller. When requested by the data subject, controllers must confirm to the subject whether data is being processed, the categories of data and the recipients to whom data are disclosed. This must be done without excessive delay or expense. The

subject also is entitled to seek correction, erasure or blocking of data not complying with the Privacy Directive, both from the controller and any third parties who have received the data.[25]

Data subjects can object to data collection and processing at any time "for compelling legitimate reasons relating to his particular situation". Further, data subjects have the right to block processing at any time and free of charge if it relates to direct marketing.[26]

From an e-commerce perspective, the most controversial part of the Privacy Directive is Article 25, which prohibits transfer of personal data to a third country outside the EU Member States unless the third country ensures an "adequate level of protection".[27] The EU believes its rigorous data protection scheme would be seriously undermined if personal data could freely be transferred to countries lacking sufficient privacy protection, particularly in light of the ease and speed with which data moves in international networks.

The adequacy of a third country's protection is reviewed by an EU Data Protection Working Party[28] (the "Working Party"). For example, the adequacy of privacy protection under Australian[29] and Canadian[30] law have already been scrutinized by the Working Party.

The differences in EU and U.S. privacy policy spring from deep cultural differences in the way Europeans and Americans view privacy. It was immediately clear that legislation to create a comprehensive regulatory scheme with a centralized federal watchdog sufficient to meet the EU's "adequacy" standards would not be politically viable in the U.S. Congress. Thus, under the Privacy Directive, transfers of personal data to the United States by data controllers in an EU Member States likely would be prohibited.

The United States had approximately $350 billion in trade with the EU in 1999. Enforcement of the Privacy Directive threatened to restrict essential data flows in multinational organizations, such as those necessary for transnational bank transactions, credit card transactions and personnel matters. Such restrictions could seriously impede trade between the EU and the U.S. The Clinton Administration began high level-talks with the EU in 1997 to negotiate a "Safe Harbor" for U.S. companies that reflect the U.S. approach to privacy while still meeting the test of "adequacy " in the EU. The Safe Harbor provisions were reviewed by the Working Party [31] and approved as "adequate" by the European Commission on July 26, 2000[32] and were promulgated by the Federal Trade Commission (FTC)[33]

U.S. companies wishing to continue to receive data from data controllers in EU Member States may join the Safe Harbor by complying with its privacy principles. The company must be subject to Federal Trade Commission (FTC) jurisdiction or other recognized federal enforcement bodies to enable government enforcement sanctions. The EU intends to begin enforcement of the Privacy Directive on July 1, 2001.

Participation in the Safe Harbor is completely voluntary. An organization may "opt in" to the Safe Harbor by adopting its applicable privacy requirements, publicly declaring the organization's compliance, and annually self-certifying to the Department of Commerce that they have a self-regulatory privacy program adhering to the requirements.[34] The organization requests to be placed on the Safe Harbor list maintained by the Commerce Department and this constitutes a representation that it follows the Safe Harbor privacy principles. Organizations must notify the Commerce Department if they are no longer in compliance, or if the wish to withdraw from the Safe Harbor.

A second way to enter the Safe Harbor is to join a privacy program administered by another organization such as TRUSTe, BBBOnline, or the program of the Direct Marketing Association.

The Safe Harbor is based on seven key principles: notice, choice, onward transfer, security, data integrity, access and enforcement. These principles approximate the protections given under the Privacy Directive.

Individuals must be notified of the purpose for which information is collected and used, and information not relevant to that purpose may not be collected. Individuals must be notified of the types of third parties to whom data will be disclosed, their rights to limit use and disclosure, and how to contact the organization with inquiries and complaints.[35] All notices must be in clear and conspicuous language, and must be given before collection, (or as soon as practicable afterward) and in all cases before use for another purpose or disclosure to others.

In a clear and conspicuous way, the organization must offer the individual an opportunity to decline to permit ("opt out") their personal information to be disclosed to third parties or to be used for a purpose not related to the purpose for which the data was collected. The means for exercising the choice must readily available and affordable.[36]

For sensitive data (defined as medical or health conditions, sex life, race, ethnicity, political opinions, religious or philosophical beliefs or membership in a union) the information may not be disclosed to a third party or used for an unrelated purpose unless the individual "opts in" by granting permission in an affirmative and explicit way.[37]

Personal information must be relevant to its intended purpose. It may not be processed for another incompatible purpose without consent of the individual. The organization must take reasonable measures to be sure the date is accurate, complete and current.[38] Individuals are guaranteed access to the information, with the right to correct, amend and delete information, unless disproportionately burdensome or expensive to do so or another's rights would be violated. The organization must to reasonable measures to protect personal data from misuse, alteration, destruction, or unauthorized access or disclosure.[39]

Transfers to third parties are subject to the notice, relevance and choice principles. Required notice regarding the third party and the purposes of collection must be given, and the information transferred must be relevant to the original purpose. If the transfer is for incompatible purposes or to an undisclosed third party, then the transfer must be authorized by the individual. However, an organization may make a transfer, without notice, to a third party acting as an agent, provided the transferor confirms that the third party is subject to the Privacy Directive, the Safe Harbor principles or other privacy protection measures of the same level.[40]

Finally, the organization must provide sufficient enforcement mechanisms must be in place that will ensure:

1) internal verification that the Safe Harbor principles are complied with. This may be accomplished by self assessment or third party audits of compliance;
2) independent dispute resolution. This could be provided by organizations such as BBBOnline, TRUSTe, or AICPA WebTrust; and
3) remedies and sanctions available to the third party dispute resolution body that are rigorous enough to ensure compliance, such as publicity, deletion of data, and reversal or correction of errors.[41]

For large organizations dealing with many affiliates, customers and suppliers in the EU, the Safe Harbor program offers real advantages. The adequacy finding by the European Commission is binding on all Member States. For European transferors, verification of a transferee's participation in the Safe Harbor is as simple as checking the list on the Department of Commerce web site. Disputes with European citizens will usually be heard in U.S. courts. In most cases, any requirements in Member States for prior approval of data transfers will be waived or automatically granted.[42] However, the Safe Harbor is limited to transfers outside the EU and does not supplant regulations of Member States applying to data processing within the Member State.

Another way to comply with the Privacy Directive without entering the Safe Harbor program is to enter into private contracts with EU data controllers which incorporate privacy clauses meeting Privacy Directive standards. This approach may be attractive for organizations that receive data from only a limited number of sources in the EU. The privacy principles would need to be applied only to the data received from the EU. This likely would be less expensive to implement than joining the Safe Harbor, which would apply to all data processed in the organization.

On March 27, 2001, the EU issued a draft version of a European Commission decision setting forth proposed Standard Contractual Clauses that could be incorporated into contractual agreements between EU and U.S. parties.[43] The draft decision includes a finding of adequacy for the protection offered by the Standard Contractual Clauses if they are made part of a contractual agreement.

Several issues have arisen which the bring the effectiveness of the Safe Harbor program into question. The Safe Harbor officially opened November 1, 2001 with the Commerce Departments publication of its list of

companies that had signed on to the program. However, as of May 31, 2001, only 48 U.S. companies had joined the list.[44] Many firms have delayed participation in hopes that the rules will be delayed from the July 1, 2001 enforcement date, or be relaxed.[45] Recently, however, the Safe Harbor was boosted by an announcement that Microsoft[46] would join the program. Also, the Direct Marketing Association is allowing its member to join its Safe Harbor seal of approval program free of charge.[47]

The Bush Administration sent a letter to the European Commission expressing concern over the terms of the Standard Contractual Clauses, criticizing them as "unworkable" and "unduly burdensome".[48] However, the EU has refused to further delay any enforcement of the privacy rules due to "U.S. domestic constraints".[49]

Further developments undoubtedly will unfold as the July 1 enforcement date approaches. The EU strategy in enacting the Privacy Directive has made it the de facto minimum standard for privacy in global commerce, and fulfilled the goal of the eEurope Action Plan to have Europe take an prominent role in shaping e-commerce policy. The EU approach has moved privacy to the forefront as a major *commercial* issue, rather than solely a rights and liberties issue. By doing so the EU has rapidly accelerated the growth of attention and resources devoted to privacy among transnational participants in electronic commerce.

II. Electronic Signatures

Both the United States and Europe have acted to address another area of legal uncertainty that impedes e-commerce: the legal effect of writings, notices and signatures online. In U.S. law, each state and the federal government have statutes requiring certain transactions to be evidenced by "writings" and authenticated by "signatures". These sensible requirements of the paper-based world were not easily adapted to the requirements of electronic commerce.

Electronic contracting parties were subject to the risk that the other party could deny the validity or enforceability of an otherwise valid agreement if the electronic contract documents were held not to constitute a proper "writing" or a "signature". In the United States, both federal and state governments tackled the problem. Several states have enacted a version of the Uniform Electronic Transactions Act ("UETA")[50]. At the federal level, Congress enacted the Electronic Signatures in Global and National Commerce Act, more commonly known as "E-Sign".[51] Neither statute requires any one to use or accept electronic records or signatures.

E-Sign's key operative provisions state:

. . . with respect to any transaction in or affecting interstate or foreign commerce --

(1) a signature, contract or other record relating to such transaction may not be denied legal effect, validity or enforceability solely because it is in electronic form; and
(2) a contract relating to such transaction may not be denied legal effect, validity or enforceability solely because an electronic signature of electronic record was used in its formation.[52]

UETA's provisions state:

a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.[53]

Both E-Sign and UETA comprehensively address the issue of enforceability of electronic contracts and signatures. Each statute is an important first step toward greater legal certainty in online commerce. However

plenty of uncertainty remains to undermine confidence in electronic contracting. In fact, the differences between E-Sign and UETA introduce new uncertainty and complexity into electronic contracting.

The first issue concerns the degree to which E-Sign, as a federal statute, preempts operation of UETA enacted in states prior to E-Sign's effective date. Commentators have offered several possible interpretations on the preemption that will have to await judicial interpretation to be resolved.[54] Secondly, E-Sign allows states to modify, limit or supersede E-Sign by enacting UETA or other means, subject to some limitations. Any modifications adopted after E-Sign must specifically refer to E-Sign and must not favor any particular technology by according it any greater legal status or effect.[55]

E-Sign is a minimalist statute drafted with awareness of UETA with hopes of dovetailing with the state statutes. UETA was drafted to more comprehensively deal with issues related to electronic signatures and contracts. Consequently, significant differences exist particularly with regard to consumer protection provisions. E-Sign requires a consumer's electronic consent before electronic contracts, notices and records may be used, while UETA would permit paper consent to electronic notices.[56] Until judicial interpretation of the preemption issues occurs, or a better harmonization of the two statutes is achieved, those in e-commerce will need to be aware of both federal and state legal requirements.

It is important to recognize that E-Sign and UETA are not a panacea for uncertainty in online commerce. There are several remaining items of legal uncertainty that E-Sign and UETA do not remove. While each has broad definitions of what can constitute an electronic signature[57] the issue of authenticity remains. Before accepting an electronic document, one must be sure that the signature was actually supplied by the purported signer, i.e. it is not forged. With respect to contracts, there are further issues about the contractual intent.

UETA provides that a signature will be attributed to a person if it was the act of the person[58]. This can be proved by any relevant evidence such as use of a password. [59] E-Sign is silent on this question. UETA defers to state law on issues such as intent and contract formation.

Both E-Sign and UETA are technologically neutral and do not give greater legal effect or enforceability to digital certificates over other types of electronic transmissions that could constitute a signature. Essentially these statutes leave the level of authenticity protection to the market and the parties to determine in light of the context and significance of the transaction.

A related issue is the integrity of the electronic contract and its signature during transmission. The contracting parties must be sure the record to which their signature is attached or logically associated has not been digitally altered to their detriment. E-Sign does not address this issue. UETA's attribution provision would provide protection from liability since the altered record would not be the act of the person.[60] In addition, if the parties had agreed to use security procedures and one party did not use the procedures agreed, the party conforming to the security procedure can avoid the effects of the changed record.[61] If there is no agreement on security procedures, UETA merely provides that the law of mistake applies to the situation.[62]

On the international level, both the EU and the United Nations have taken action on electronic signatures. The EU has issued a Directive on Electronic Signatures[63] and a Directive on Electronic Commerce.[64] The Electronic Signatures Directive differentiates between a broadly defined "electronic signature" roughly similar to E-Sign and UETA provisions[65] and "advanced electronic signature"[66] which is uniquely linked to, and under the control of, an identified signatory and provides for detection of subsequent alteration of the data. Advanced electronic signatures are given greater legal effect. They satisfy legal requirements for signatures and are admissible evidence *per se*. An ordinary electronic signature may not be denied legal effectiveness or admissibility solely on the grounds that the signature is electronic and did not use advanced signature methods, but their admissibility and effect are not automatic.[67]

The Directive on Electronic Commerce instructs EU Member States to modify their legal requirements to ensure that contracts may be concluded by electronic means, and to remove obstacles that would deny electronic contracts their validity and effectiveness.[68]

The United Nations Commission on International Trade Law (UNCITRAL) has taken a similar tack, but one which favors use of advanced digital signatures technology. An electronic signature is data associated with a message, that may be used to identify the signatory and indicate approval of the information in the message.[69] Such a signature will have legal effect if "an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated in light of all the circumstances, including any relevant agreement. "[70] Thus the validity of the signature will depend on a case-by-case factual finding. This standard only marginally improves the legal certainty regarding the validity of electronic signatures. However, if the electronic signature contains "signature creation data", such as that provided by digital certificates, then the signature is per se considered reliable if the signature creation data is unique to and controlled by the signer and subsequent alterations to the signature or the information are detectable.

With the hurdles of validity and enforceability of electronic contracts largely overcome, the next challenge is to remove obstacles of authenticity and integrity. The legal and technological requirements are largely in place. Now the market must produce and effectively sell digital signature services that are well-known, readily understood and easily implemented by a critical mass of consumers and businesses. The data encryption standards needed to protect the integrity of messages must be sufficient to inspire confidence for even large transactions, and a legal framework to apportion legal liability for cases of interception and alteration of electronic transactions must be developed.

Until then, electronic signatures will have its greatest impact in the following areas:

- Businesses with a high volume of transactions involving electronic signatures so cost savings and performance improvements are meaningful;
- Between parties who already know each other and have easy mechanisms for authentication
- Low value transactions where the cost of potential fraud is sufficiently low as to justify the greater risks of online contracting.[71]

III. Consumer Protection

In the area of consumer protection there is substantial agreement internationally about the essential features of fair trading in electronic commerce. The OECD issued its Guidelines for Consumer Protection in the Context of Electronic Commerce in 2000,[72] and 29 member nations have adopted the Guidelines.[73] The EU enacted its Directive on Distance Contracts in 1997.[74] In the United States, the Federal Trade Commission and the states enforce extensive consumer protection laws.

The multi-jurisdictional nature of the Internet makes enforcement of criminal violations very difficult in the absence of transnational cooperation. However, trade practices authorities in 29 countries have banded together to create the International Marketing Supervision Network (IMSN)[75] to assist in cross-border enforcement.[76] The Federal Trade Commission maintains a website at http://www.econsumer.gov to assist in reporting deceptive trade practices engaged in by foreign companies to the national enforcement agencies in Australia, Canada, Denmark, Finland, Hungary, South Korea, Mexico, New Zealand, Norway, Sweden, Switzerland, United Kingdom, the United States and the OECD.

In addition, the FBI has established the Internet Fraud Complaint Center (IFCC) in cooperation with the National White Collar Crime Center.[77] Recently the FBI announced charges against 90 persons involved in Internet fraud totaling $117 million.[78]

Interstate or international e-commerce presents additional risks of fraud or deceptive trade practices, or even simple non-performance for online consumers. Even though consumers may have a clear legal cause of action against a distant seller, the difficulty and costs of bringing action against a distant seller make the available remedies meaningless and expose online buyers to greater risk. The key to reducing this risk and uncertainty for consumers is private self-regulatory action. Sellers in e-commerce must develop and participate in online dispute settlement mechanisms and codes of conduct in order to increase consumer confidence and business

predictability. This will be necessary to attract more consumers online and to increase the size of transactions they are willing to conduct online with confidence.

The Better Business Bureau's "BBBOnline Reliability Seal" is a trustmark program with 9,800 businesses enrolled and certifying compliance with BBBOnline's Code of Online Business Practices.[79] The program sets standards for online advertising and communications, disclosure of business practices, privacy, security, customer satisfaction and children's privacy.[80] The Better Business Bureau is now developing a joint project with the Federation of European Direct Marketing and Eurochambres, an association of European Chambers of Commerce.[81]

In this area, the law has perhaps done what it can, and e-commerce merchants will have to develop alternative means to improve consumer confidence in electronic transactions across borders. Until this is done, e-confidence may remain low, and e-commerce will not reach its potential.

CONCLUSION

Despite strong growth in the past five years, e-commerce is not anywhere near achieving its full potential. However, recent ongoing global efforts to build the legal infrastructure needed to provide greater legal certainty in the areas of privacy, electronic signatures and consumer protection will greatly aid the development of e-commerce. The significant efforts to harmonize legal regimes in these areas will help to create the e-confidence needed for the potential of e-commerce to be realized in the near future. In addition, online merchants in the private sector will have to work together to create recognizable and trustworthy dispute resolution methods where the jurisdictional limitations of judicial sanctions create obstacles to e-commerce.

ENDNOTES

1 Jonathan Coppel, *E-Commerce: Impacts and Policy Challenges*, O.E.C.D. Economics Department Working Paper No. 252, June 23, 2000, p. 3; ECO/WKP(2000)252. (visited May 15, 2001) <http://www.olis.oecd.org/olis/2000doc.nsf/linkto/eco-wkp(2000)25>

2 *Id.* at p. 7.

3 U.S. Department of Commerce Estimated Quarterly Retail Sales, (visited May 30, 2001) <http://www.census.gov/mrts/www/current.html>

4 e-Europe 2002: Impact and Priorities, Com(2001)140 final at 9, March13, 2001.

e-Europe 2002: An Information Society for All, Action Plan, Lisbon European Council, March 23-24, 2000.

6 e-Europe 2002: An Information Society for All, Action Plan, Fiera European Council, June 19-20, 2000.

7 Council Directive 2000/31/EC of 8 June 2000 on Certain Legal Aspects Of Information Society Services, In Particular Electronic Commerce In The Internal Market, O.J. (L 178).

8 Council Directive 97/7/EC of 20 May 1997 on the Protection Of Consumers In Respect Of Distance Contracts, O.J. (L 144).

9 Council Directive 1999/93/EC of 13 December 1999 on a Community Framework For Electronic Signatures, O.J. (L 013).

10 Children's Online Privacy Protection Act, 15 U.S.C. §6501-6506.

11 Health Insurance Portability and Accountability Act of 1996, 42.U.S.C. §201.

12 European Convention on Human Rights and Fundamental Freedoms, Art. 8; Council Directive 95/46/EC of 24 October 1995, On The Protection Of Individuals With Regard To The Processing Of Personal Data And The Free Movement Of Such Data, Preamble Para. 2 and Para. 3, 1995 O.J. (L 281).

13 *Id.*

14 *Id.* at Preamble, Para 2 and 3. The EU has issued a new guide to its data protection policies. *Data Protection in the European Union*, (visited May 29, 2001) <http://www.europa.eu.int/comm/internal_market/en/media/dataprot/news/guide_en.pdf>

15 *Id.* at Article 3 (2).

16 *Id.* at Article 2.

17 *Id.* at Article 6.

18 *Id.* at Article 16 and 17.

[19] *Id.* at Article 28
[20] *Id.* at Article 18
[21] *Id.* at Article 7
[22] *Id.* at Article 8.
[23] *Id.* at Article 10.
[24] *Id.* at Article 11.
[25] *Id.* at Article 12.
[26] *Id.* at Article 14.
[27] *Id.* at Article 25.
[28] The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data was established in Article 29 of Council Directive 95/46/EC of the European Parliament and European Council of 24 October 1995. O.J. (L 281).
[29] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000, adopted January 26, 2001, WP 40, DG MRKT 5095/00; (visited May 29, 2001) <http://www.europa.eu.int/internal_market/en/media/dataprot/wpdocs/wp40en.pdf>
[30] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 2/2001 on Adequacy of the Canadian Personal Information and Electronic Documents Act, adopted January 26, 2001, WP 39, DG MRKT 5109/00; (visited May 29, 2001) <http://www.europa.eu.int/internal_market/en/media/dataprot/wpdocs/wp39en.pdf>
[31] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 4/2000 on the Level of Protection provided by the "Safe Harbor Principles", adopted May 16, 2000. (visited May 29, 2001) <http://www.europa.eu.int/internal_market/en/media/dataprot/wpdocs/wp32en.pdf>
[32] Commission Decision 2000/520/EC of 26 July 2000 on The Adequacy Of The Protection Provided By The Safe Harbour Privacy Principles And The Related Frequently Asked Questions Issued By The US Department Of Commerce, 2000 O.J. (L 215).
[33] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45665, (2000); Issuance of Safe Harbor Principles and Transmission to European Commission; Procedures and Start Date for Safe Harbor List 65 Fed. Reg.56534 (2000).
[34] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45665, 45670 (2000).
[35] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45665, 45667 (2000).
[36] *Id.* at 45667.
[37] *Id.* at 45668.
[38] *Id.* at 45668.
[39] *Id.* at 45668.
[40] *Id.* at 45668.
[41] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45665, 45668 (2000); *see,* U.S. Department of Commerce, *Safe Harbor Workbook,* pp. 12 and 13 (visited May 31, 2001) <http://www.export.gov/safeharbor/SafeHarbor/SafeHarborWorkbook.html>.
[42] U.S. Department of Commerce, *Safe Harbor Workbook,* p. 6 (visited May 31, 2001) <http://www.export.gov/safeharbor/SafeHarbor/ SafeHarborWorkbook.html>
[43] Draft Version, Commission Decision on Standard Contractual Clauses For The Transfer Of Personal Data To Third Countries Under Article 26(4) Of Directive 95/46/EC, March 27, 2001, (visited May 29, 2001) <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/clausesdecision.pdf>; *see,*Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 1/2001 on the Draft Commission Decision On Standard Contractual Clauses For The Transfer Of Personal Data To Third Countries Under Article 26(4) Of Directive 95/46/EC, WP 38, DG MRKT 5102/00/EN (visited May 29, 2001) <http://www.europa.eu.int/internal_market/en/media/dataprot/wpdocs/wp38en.pdf>
[44] U.S. Department of Commerce, *Safe Harbor List,* (visited May 31, 2001) <http://www.export.gov/safeharbor/SafeHarbor/ SafeHarborWorkbook.html>
[45] *Trade Group Boosts Safe Harbor,* REUTERS, May 22, 2001, (visited May 24, 2001) <http://www.zdnet.com/ecommerce/stories/main/0104752764044.html>
[46] Brandon Mitchener, *Microsoft Plans to Sign Accord on Data Privacy with the EU,* Wall Street Journal, May 16, 2001 at A14, (Visited May 29, 2001) Lori Enos, *Microsoft to Sign EU Privacy Accord,* E-COMMERCE TIMES, May 16, 2001 (Visited May 24, 2001), <http://www.ecommercetimes.com/perl/printer/9572.>
[47] Robert MacMillan, *DMA Group is Go-Between in US/Europe Privacy Morass*, NEWSBYTES, May 22, 2001, (visited May 29, 2001) <http://www.newsbytes.com/
[48] *Bush Team Opposes Proposed Euro Privacy Rules*, THE STANDARD, March 27, 2001 (Visited May 24, 2001), http://www.thestandard.com/article/0,1902,23137,00.html>

[49] Guy De Jonquieres, *EU 'No' to Data Privacy Delay*, THE FINANCIAL TIMES, May 6, 2001, (visited May 24, 2001), <http://news.ft.com/ft.gx.cgw/ ftc?pagename=View&c=Article&cid=FT3M0NO0FMC&l.html>

[50] UNIF. ELECTRONIC TRANSACTIONS ACT.

[51] Electronic Signatures in Global and National Commerce Act, Pub. L No. 106-299, 114 Stat. 464 (2000) (codified as 15 U.S.C. §§ 7001 *et.seq*. [hereinafter, "E-Sign"].

[52] E-Sign, *supra* note 51, § 101 (a).

[53] U.E.T.A.

[54] *See*, Patricia Blumfield Fry, *A Preliminary Analysis of Federal and State Electronic Commerce Laws*, (visited May 29, 2001) <http://www.uetaonline.com/docs/ pfry700.html> , and Margot Saunders and Gail Hillebrand, *E-Sign and UETA: What Should States Do Now?*, CYBERSPACE LAWYER, January 2001 and February 2001 (visited May 29, 2001) <http://www.consumerlaw.org/e_sign.html>

[55] E-Sign, *supra* note 51, §102.

[56] Saunders and Hillebrand, *supra* note zz.

[57] E-Sign, *supra* note 51, § 106 (5) states:."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". UETA's definition is almost identical.

[58] U.E.T.A. § 9

[59] Patricia Blumfield Fry, *A Preliminary Analysis of Federal and State Electronic Commerce Laws*, (visited May 29, 2001) <http://www.uetaonline.com/docs/ pfry700.html>

[60] U.E.T.A. § 9.

[61] U.E.T.A. § 10.

[62] *Id*.

[63] Council Directive 1999/93/EC of 13 December 1999 on a Community Framework For Electronic Signatures, O.J. (L 013).

[64] Council Directive 2000/31/EC of 8 June 2000 on Certain Legal Aspects Of Information Society Services, In Particular Electronic Commerce In The Internal Market, O.J. (L 178).

[65] " '(E)electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication" Council Directive 1999/93/EC of 13 December 1999 on a Community Framework For Electronic Signatures, Art. 2, O.J. (L 013).

[66] *Id*.

[67] *Id.* at Art. 5.

[68] Council Directive 2000/31/EC of 8 June 2000 on Certain Legal Aspects Of Information Society Services, In Particular Electronic Commerce In The Internal Market, Art. 9, O.J. (L 178).

[69] UNCITRAL Draft Model Law on Electronic Signatures, Art. 2 (visited May 29, 2001) <http://www.uncitral.org/english/sessions/und/unc-34/can-493e.pdf>

[70] *Id*. at Art. 6.

[71] Bill Zoellick, *Commentary on the Electronic Signatures in Global and national Commerce Act*, (visited May 29, 2001*)* http://www.fastwater.com/Library/B2BEconomy/DigitalSigs/DigSig/Commentary.php3*; see,* Bill Zoellick, *E-Sign Act Removes Barriers, Doesn't Go Far Enough, BOULDER COUNTY BUSINESS REPORT*, August 25, 2000.

[72] *Guidelines for Consumer Protection in the Context of Electronic Commerce*, O.E.C.D. (2000).

[73] *Electronic Commerce: Selling Internationally – A Guide for Business*, FEDERAL TRADE COMMISSION, March 2000. (Visited May 15, 2001) <http://www.ftc.gov/bcp/ conline/pubs/alerts/ecombalrt.html>

[74] Council Directive 97/7/EC of 20 May 1997 on the Protection Of Consumers In Respect Of Distance Contracts, O.J. (L 144).

[75] The participating countries are: Australia Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovakia, South Korea, Spain, Sweden, Switzerland, United Kingdom, and the United States, along with the European Commission, and the Organization for Economic Co-operation and Development (OECD)

[76] *See*, International Marketing Supervision Network, (Visited May 31, 2001) <http://www.imsnricc.org/>

[77] Internet Fraud Complaint Center

[78] FBI Press Release, May 23, 2001, (visited May 31, 2001) <http://www.fbi.gov/pressrel/ pressrel01/ifcc052301.htm>

[79] *See*, BBBOnline Code of Online Business Practices, (Visited May 31, 2001) <http://www.bbbonline.org/xxx>

[80] *Id.*.

[81] Claire Sabila, *Global E-Commerce Conduct Code in the Works*, E-COMMERCE TIMES, April 23, 2001 (visited May 15, 2001) <http:// www.ecommercetimes.com/perl/ story/9172.html>.