

FOR EDUCATIONAL USE ONLY

Copr. © West 2000 No Claim to Orig. U.S. Govt. Works

570 PLI/Pat 51

(Cite as: 570 PLI/Pat 51)

Practising Law Institute
Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series
PLI Order No. G0-0090
August/September, 1999

eCommerce: Strategies for Success in the Digital Economy

***51 DOING BUSINESS IN THE DIGITAL ERA: SOME BASIC ISSUES**

Margaret Jane Radin [FNa]
Daniel L. Appelman [FNaa]

Copyright (c) 1999, Practising Law Institute

***53 1. Introduction: Business Legal Infrastructure In The Networked Digital Environment**

Today's business headlines are breathtaking. Digital money, robot purchasing agents, encrypted messages, fear of rampant copying, companies in the red whose stocks go through the roof. In the new world of the networked digital environment, all commerce is or will become electronic in significant ways. In that new world many questions face business decision makers and their counsel.

Some of the questions are economic and strategic. Business decision makers must figure out what business models will work in the new environment. In particular, what changes need to be made in traditional business models to adapt to commerce in the networked electronic world? (And, on the other hand, what kinds of things can be handled as business as usual?) [FN1] Some of the questions are legal and political. Though business models are changing, business decision makers sometimes assume that the legal backdrop for business--for example, the process of entering into and enforcing contracts--is stable and can be taken for granted as it has been in the past. Yet the digital environment is changing the basics of the legal business infrastructure. Making and performing contracts will be different in some respects. So will taxation, intellectual property protection, securities regulation, financial regulation, dispute *54 resolution, and consumer protection, including legal protection of our privacy. All of these legal regimes are in the process of adapting not only to new technological possibilities and new economic models, but also to the global nature of the networked environment.

Business decision makers need to be aware of these changes as they design and implement strategies to stay competitive, as well as strategies to help shape these profound changes to their advantage. The purpose of this article is to provide an overview of the changes that are taking place in the legal business infrastructure. Accordingly, we will consider the basic infrastructure of exchange, contracts and property (patent copyright, and trademark), as well as enforceability (jurisdiction) and one important aspect of regulation (consumer privacy). Before considering these topics, we will consider the pervasive issues of security, authentication, and payment mechanisms.

2. Security and Authentication in the Digital Economy: Why All These Debates About Cryptography?

Encryption protects messages from disclosure and from alteration or corruption. In the digital era, cryptography has become a basic topic for business decision makers, because of the need for security in electronic business transactions. In the digital world, money is a message (a set of 1's and 0's), a signature is a message (a set of 1's and 0's), and so are credit card numbers, copyrighted pictures and music, proprietary computer programs, the "look and feel" of your computer screen, and everything else that drives the world of digital exchange. All of those 1's and 0's are easy to copy in fractions of a second and transmit to the other side of the world. Something is needed to restrict these *55 activities to legitimate transactions if electronic commerce is to be successful. In the digital world, encryption systems are used to enhance the security of **electronic commerce** by addressing these **issues**:

- . Data confidentiality: Given the ease of snooping and copying on a network, firms want to keep their documents private
- . Data integrity: A customer does not want to order a bathmat and receive a bathtub; a bank does not want to sign a digital coin for \$0.10 and have it become a \$1,000,000 bill
- . Identification of parties: A merchant does not want its customer's payment deposited to an account of someone impersonating the merchant; a bank wants to be able to bind a credit card number to its rightful owner
- . Non-repudiation: A merchant does not want its customer to stop payment and deny a transaction after goods have already been delivered
- . Prevention of replay attacks and double spending: A bank does not want a customer who withdraws \$20 or spends \$20 in digital money to be able to replicate the same transaction 10,000 times in a few seconds, then vanish into cyberspace

The legal system has not yet come to terms with cryptography. Because of the ubiquitous need for encryption in the world of digital exchange, the development and marketing of encryption systems is itself an important industry. A large segment of the American business community has begun to protest the U.S. *56 government's restrictions on export of encryption programs, and some have argued that those restrictions impose significant barriers for U.S. companies seeking to do business abroad. [FN2] Though the controversies surrounding export control have made headlines, perhaps more important for the developing infrastructure of digital commerce is the advent of digital signatures.

When public key cryptography is used to ensure confidentiality, to send a message and keep it secret, the sender encrypts a message with the public key of the recipient and the recipient decrypts with his own private key, to which no one else has access. [FN3] Digital signatures also rely on public key cryptography, but digital signatures run the process the other way. In its simplest form, the process starts with the party wishing to sign a message (e.g., a corporate officer signing a contract, or a bank signing a piece of digital money) using its private key to encrypt the message before it is transmitted to a recipient. A recipient then uses the sending party's public key to decrypt the message. Provided that the recipient knows that the public key is really the public key of the sender, then when the key works to decrypt the message, a recipient knows that the sender is the one who sent it (i.e., it is "signed" by the sender). [FN4]

In order for this process to work it is crucial for receiving parties to be able to find out the public key associated with the sending party, and to know for sure that the public key purportedly that of the signing party is really the public key of the sending party, and not that of some interloper bent on forgery. Thus some infrastructure for making public keys readily available and for authenticating them is required. [FN5] The public key infrastructure that has been developing involves firms known as certificate authorities (CA's) who are in the business of vouching for people's public keys by *57 attaching digital certificates to them. [FN6] A digital certificate is the CA's own digital signature. (Who vouches for the CA's digital signature? Another CA. And so on until one reaches a "root" CA.)

The public key infrastructure necessary for commerce in the digital world as it is now constituted, with the concomitant advent of digital signatures to replace "analog" signatures, requires revising the legal ground rules. During the past few years, legislation validating digital signatures at least for some uses has been enacted in the majority of states. [FN7] These laws function, among other things, to enable online contracting by granting legal significance to digital signatures in situations where physical signatures otherwise would be required. Some of the new laws are technology-specific and others are technology neutral. [FN8] Among the questions respecting digital signatures are: Will a receiving party who accepts a deficient digital signature be liable for any losses caused by that signature? What can businesses do to protect themselves against fraudulent digital signatures? Can a receiving party seek indemnity from the CA who guaranteed the defective signature? What levels of proof must a CA require before it issues a certificate? Will a CA be liable to a defrauded party if it fails to require good enough proof? Can a CA disclaim liability? Will a CA be immune from liability if it does require good enough proof? If CA's are immune, will liability be thrown back to the party who mistakenly relied on a certificate?

The importance of encryption in the online environment, and of the issues it raises, should not obscure the fact that encryption is not a security panacea. [FN9] A maxim that bears remembering is that security is only as good as its weakest link. An unbreakable encryption system cannot make up for careless or disloyal employees, improper storage of keys or *58 passwords, and so on. These liability issues are analogous to those of the non-digital world. Still, the advent of digital business is causing companies to have to reevaluate their entire approach to security. And, somewhat analogously to the problems caused by the Y2K "bug," companies or their insurers may face significant liabilities for obsolete security systems or procedures. For example, firms must develop secure storage protocols for their employees' private keys, an urgent item of business because if a key is compromised large liabilities can result.

3. Payment Systems

One form of electronic commerce that can be readily analogized to traditional commerce is retailing of physical goods on the Web, which is similar to catalogue retailing in many respects. [FN10] Instead of telephoning an order from a paper catalogue, the customer can navigate to a retail Web site and buy by clicking a box on a computer screen. How will the customer pay for the goods? To date, consumers have opted overwhelmingly to use credit cards, just as they do for catalogue orders, but other payment mechanisms are being developed. [FN11] Digital checks, for example, work like paper checks: A check is just a particular signed message endorsed by one bank and presented to another bank, giving rise to a settlement of accounts each day; all of these functions can be replicated digitally. [FN12]

Credit card transactions are too expensive to deal with very small payments of the kind that may become widespread if the networked computer becomes a pay-per-view (or pay-per-read or pay-per-quote) screen. A few micropayment systems are in the trial stages now. [FN13] These systems are patented, and give rise to important legal and policy questions about patenting money. [FN14] Varieties of digital *59 cash, most of which are also patented, are also struggling to be born. Although digital cash may offer more consumer privacy than use of credit cards, so far it has not caught on with consumers. [FN15]

In addition, numerous kinds of near-money are also coming into being--digital coupons in return for viewing advertisements, digital scrip for use in playing games online, coupons awarded in customer loyalty programs, and so on. Especially since these can be more freely tradeable than their offline analogues, questions arise regarding to what extent near-money can escape the sort of regulation that banks must comply with. Certainly firms that intend to create coupons, scrip, or rewards programs should think about whether banking-oriented financial regulations are applicable.

When a consumer buys physical goods at a Web site with a credit card, she must transmit some details to

the Web merchant, including the address to which the goods are to be sent, and the credit card details (type of card, card number, billing address, expiration date). Two types of general issues arise: (1) How can a consumer be sure that these details are not being diverted to a fraudulent third party? (2) How can a consumer know what the Web merchant itself is going to do with information about her and her purchases?

In the next section, we will turn to the question about control of consumer information. With respect to worries about theft of credit card details, it is a bit puzzling why diversion of credit card numbers over the Internet worries consumers. There is as much danger of fraudulent credit card use in "real" space as there is in cyberspace, and in any case consumer losses are capped by law at \$50. [FN16] Nevertheless, schemes of secure transmission have been *60 developed in order to transmit card details from the consumer's computer through the network to the Web server (merchant's computer). At present, most Web sites are using SSL (Secure Socket Layer). SSL is a patented program developed by computer scientists at Netscape that uses encryption to transmit the credit card details from buyer to merchant, including digital signatures that verify that the parties are who they say they are. [FN17]

A more ambitious project is SET (Secure Electronic Transactions), which is a protocol--that is a standard or template for programs, not a program itself-- developed by the major card associations (VISA and MasterCard). The SET protocol for the first time integrates the front and back end of a transaction. That is, SET links the communication between the consumer and the merchant (formerly conducted in person, over the telephone, or by transmitting a message from the consumer's computer to the merchant's server) with the credit verification and settlement process between the merchant and the banks (formerly conducted through a separate set of proprietary electronic networks run by the card associations). In this way, the whole process can be accomplished smoothly in one continuous set of standardized messages.

The SET protocol is an elaborate structure of hierarchical chains of certificates and message verification mechanisms at each stage of the sequence (consumer, merchant, acquiring bank, issuing bank). If the SET protocol becomes the worldwide standard, as its sponsors intend, then it will replace SSL and other methods that do not integrate the sequence of events that make up a transaction from purchase to settlement. It is unclear, however, whether SET will become the standard; SET has been criticized for being cumbersome (and therefore relatively *61 slow and expensive), and implementation programs have been delayed.

As development of online commerce proceeds, how these protocols work should become of merely academic interest to most businesses. Most business decision makers do not need to know through what specific programs and mechanisms the banking system accomplishes electronic management of vast amounts of transfers of money; similarly, business decision makers ultimately will not need to know how payment modalities on the Internet work. Our confidence in the banking system's ability to deal with vast amounts of electronic funds transfers, however, rests in part on confidence that government regulation and oversight will keep these systems from breaking down; and if they do break down, that those who deal with banks as customers and depositors will be immune from liability. We are not yet at a similar point for electronic commerce. We do not yet have a stable financial infrastructure in which the risks are all understood and allocated appropriately.

Moreover, the SET protocol only applies to payment; it organizes a transaction only after a customer has finished shopping and wants to buy. A number of large firms such as IBM and SAP are now marketing "solutions" that are designed to integrate all aspects of putting a business online. These "solutions" will then mesh with SET or whatever becomes the payment protocol. At this point it is too soon to tell how liability will play out if these integrated "solutions" prove defective and cause significant losses. Liability may depend to a significant extent on contractual obligations (see below).

4. Consumer Privacy: Is There A Problem? Can TheMarket Take Care Of It?

***62** In the digital world, concerns about consumer privacy and control over private information are very important. As we shall see, firms doing business on the Internet should definitely not assume that consumer information--whether acquired directly from their own customers or indirectly from a marketing firm--belongs to them to use as they wish.

Web servers gather information about customers (what sites they visited, what they purchased, addresses, demographic information, and so on). Information gathered by computers never dies. It can be stored in data bases and amalgamated with other information from other data bases (medical records, health records, financial records). Such repositories of information then become valuable assets, to be sold to marketers and others.

Many people are worried that if this kind of information gathering and marketing goes unchecked, everyone who uses a credit card or browses online will be an open book. "They" will know what books, videos, and pharmaceuticals you bought, what kinds of pictures you are looking at, whether you gamble or play games, whether you have been disciplined by your profession. Especially worrisome is data gathering from children.

Some people do not see this situation as a problem. Let Web sites and other data gatherers disclose exactly what data they are gathering and what they plan to do with it, it is argued, and then let consumers exercise their own choice whether or not to continue with the transaction. If a data gatherer is doing something you consider to violate your privacy, then vote with your feet. In this minimalist approach, questions immediately arise about what constitutes choice to relinquish privacy. Certainly a consumer cannot have chosen to relinquish control of ***63** information if she doesn't even know that a Web site is gathering it and selling it.

Many Web site operators attempt to provide disclosure by having a small link labeled "legalese" or "fine print." If the consumer clicks on this link, it will reveal fine print legalese to the effect that any data submitted can be stored and marketed, and that further use of the site constitutes acceptance of these terms. This probably does not constitute adequate disclosure to justify a finding that consumers voluntarily relinquished their private data; at least, courts or legislatures may have to set guidelines. Thus, the minimalist approach will encourage attempts to regulate what constitutes adequate disclosure and acceptable information practices.

The minimalist approach is not convincing with respect to gathering data from children. Nor is it appealing when applied to services that consumers cannot readily forego, such as medical care. It may be unpersuasive in circumstances in which policy makers think that consumers will systematically undervalue their privacy interests. [FN18] For all of these circumstances where a minimalist approach appears unattractive, the viable policy choices come down to government regulation versus industry self-regulation.

The European Union has taken a strict regulatory approach. Its Data Protection Directive has important consequences for U.S. firms that do business in the EU or process information there or receive information from there. [FN19] Meanwhile, various privacy bills are pending in the U.S. Congress, and the U.S. Federal Trade Commission has been giving a great deal of attention to the issues of online privacy and data control. So far, the FTC has not issued any regulations, but it has issued a report outlining fair information practice principles, leaving open the possibility ***64** that it will hold off on any rulemaking until it can determine whether industry can self-regulate appropriately. [FN20]

Many important Internet sites are promulgating privacy policies in the hope that federal or state regulation can be avoided. [FN21] The World Wide Web Consortium has developed a technical protocol, Platform for Privacy Preference (P3P), for implementing self-enforcing privacy policies for Web sites. [FN22] Businesses have sprung up to provide labels, similar to a Good Housekeeping Seal of Approval, for Web sites that adhere to certain privacy standards. [FN23] Companies entering the world of online business will need to analyze applicable privacy regulations and to make careful decisions about corporate privacy policies and implementation strategies.

Companies seeking to do business online will also need to give thought to consumer protection in other matters. Many existing consumer protection rules directed to fraud and false advertising are applicable to doing business online. [FN24] A particular issue that marketers must closely monitor is the issue of unsolicited commercial e-mail, known as spam. A number of states have enacted anti-spam measures, and federal bills are pending. [FN25] Firms that intend to send out commercial e-mail must evaluate this picture carefully and frequently.

5. The Problem of Jurisdiction in Cyberspace

Rules of property and contract are fundamental to the legal infrastructure for doing business: what do we own and how can we trade it? But these entitlements are useless unless they can be enforced. Rules of property and contract are "local"--that is, varying country by country in the world. *65 Enforcement of each country's rules depends largely upon the connection of firms or transactions with that country. Enforcement, in other words, is in principle a matter of territorial sovereignty. [FN26] Moreover, while the main forms of intellectual property in the U.S. are federal, contract law is state law, as are some important subsidiary kinds of intellectual property, such as misappropriation and right of publicity. Where property in information is concerned, as in many other legal contexts, it matters what state you are suing (or being sued) in.

Though some Internet visionaries have proclaimed that the Internet will so undermine territorial sovereignties as to make them untenable, that is probably visionary overkill. [FN27] The fact remains, however, that it is hard to know where parties and transactions are "located" in the global networked environment, and that means it is hard to know whose law applies and whose courts will take jurisdiction to enforce that law. (The same kinds of questions about location make questions about taxation of online commerce very difficult, but no less urgent. [FN28])

Personal jurisdiction in states in the U.S. depends upon the reach of each state's long-arm statute, as that reach is limited by constitutional standards of due process and fair play. The test most often used is that the defendant must have minimum contacts with a state in order to be haled into court in that state. The question arises whether running a commercial Web site which can be accessed by people in every state subjects the site owner to being sued in every state. Merely posting a Web site has been held not to subject the site owner to jurisdiction. [FN29] On the other hand, posting a Web site with which recipients interact by sending in marketing data has been held to subject the owner to jurisdiction. [FN30]

*66 Many, probably most, commercial Web sites will not be merely passive, but will ask visitors to log in or give demographic data or put their names on customer lists. It appears that many courts will hold this to be enough contact so that a customer can bring suit in the state in which she is located. It appears, that is, that Internet businesses can be sued by customers anywhere. This is especially true if the business has shipped goods to the state in which suit is brought, but it could be true for activities falling short of actual sales as well.

The next question to consider is whether the Web site owner nevertheless could protect itself by placing on

the site a "contract" stating that the customer agrees to sue only in the site owner's preferred state, and/or agrees that the site owner's preferred state law will be the governing law. Choice of forum clauses and choice of law clauses are often found valid in negotiated contracts between commercial entities. From a policy point of view, they are problematic in "contracts" consumers may not even know about. Nevertheless, the U.S. Supreme Court has enforced a forum selection clause in a form ticket against an unknowing consumer. [FN31] Given this state of the law, firms can be expected to try to protect themselves from being sued in all jurisdictions by posting notices that limit jurisdiction and choice of law. They will have to work out with their counsel how best to do this, in light of their business circumstances. Even so, they cannot feel fully confident that taking these measures will protect them until case law addressing these issues has more fully developed.

6. Property in the Networked Environment: Trademarks

***67** By far the most litigation about jurisdiction and about property ownership in cyberspace so far has occurred in cases involving the collision of trademark rights with the registration of domain names. In traditional trademark law, trademark rights only extend to similar products or services which could cause consumers to be confused about the source. In the "real world," Apple Computer, Apple Records, and Apple Bank all coexist; in the online world, there is only one apple.com. Trademark disputes, not involving domain names, that can be resolved by application of traditional trademark principles, have indeed occurred in cyberspace. Playboy, for example, has found occasion to sue a number of Web site operators roughly in its line of products--soft porn images--whose display pages included its trademarks (e.g., Playgirl, the rabbit, etc.). [FN32] These kinds of cases can be resolved, as many trademark cases are in "real" space, by applying the anti-counterfeiting provision in appropriate cases of piracy and otherwise assessing the similarity of the products and the marks and the likelihood of consumer confusion if the marks are allowed to coexist. But so far, the clash between trademark rights and the domain name registration process in the U.S. has resulted in considerable litigation, delay and uncertainty.

NSI, a private company, has to date been the sole registrar of ".com" domain names. In accordance with a system that was begun before the Internet became a commercial modality, NSI has doled out domain names on a first-come first-served basis with no attention to prior trademark rights. U.S. trademark law assigns priority based on the first use of a mark, and even unregistered marks may have priority over registered marks if it can be shown that the unregistered mark was used first. Furthermore, slight variations from a valid trademark, when used in competition with the valid trademark, may cause consumer ***68** confusion in the marketplace and so may infringe the rights of the owner of the original mark. As a non-governmental entity, NSI has no ability or authority to adjudicate who owns a trademark before it doles out a domain name; if Citibank.com is taken but Citibonk.com is not, it will register Citibonk.com to whoever asks for it first. Under its dispute resolution policy, all NSI does is suspend a domain name registration which a claimant can show may conflict with its "first to use" rights as a trademark owner, leaving the parties to await the outcome of an appeal to the courts or to the Patent and Trademark Office. In this situation, speculators have registered domain names corresponding to the trademarks of famous companies, hoping to sell their domain name rights to the trademark owner. At the same time, some legitimate users have had their domain names put on hold at the request of an over-reaching trademark owner.

Trademark law has been evolving away from some of its traditional principles, which stem from the common law of unfair competition, toward a more expansive form of trademark rights. In some instances trademarks are being treated more as "naked" property rights; that is, a right to exclude others from using a mark whether or not it is used to identify goods and whether or not it confuses consumers. [FN33] The right of owners of "famous" marks to enjoin dilution of their marks, which became part of federal law in 1996, [FN34] treats the trademark right more as a property right than as merely a right to have recourse against confusion in the marketplace. [FN35] An owner of a "famous" mark can, with few exceptions, exclude

anyone else from using the mark commercially, no matter what the product or service and without any showing of consumer confusion.

While domain name cases usually do not fit well into traditional trademark principles, they are more readily countenanced under the Dilution Act. Most of the decided *69 cases involving domain names and trademarks involve allegations of dilution. In a typical scenario, A is first to register a particular .com domain name with NSI; then B, a firm whose trademark corresponds to the domain name, seeks to stop A from using the name. In one type of case, A is a speculator who registers domain names hoping to sell them later to firms who might have a demand for them; in another, A is a firm or person legitimately using the name, but B is a larger firm for whom the name corresponds to an established trademark.

Courts have been hostile to domain-name speculators, considering them pirates. Thus, they have been willing to find jurisdiction even if few actual activities of defendant place him in contact with the forum state, [FN36] and willing to take a liberal view of the requirements--that the mark be "famous," that defendant use it "commercially"-- necessary to make out a cause of action for dilution. [FN37] It may be that hostility to speculators in domain name cases has created expansive jurisdictional precedents which will make it easier to sue online businesses in many different places, and also has furthered expansion of the scope of trademark rights. On the other hand, cases in which A is not a speculator (pirate) have been more mixed in outcome. [FN38]

It would have been good advice to firms considering expanding into online business to secure their domain names from NSI several years ago; by now, a few million of them are taken. Nevertheless, as this article is being written, Internet governance is in the process of being handed off to a newly formed oversight body. [FN39] New registries that can compete with NSI and new top level domains that can co-exist with .com will most likely be established. Now may be a good time to secure a domain name.

*70 The foregoing discussion has concerned the conflict between trademark rights and domain name registration procedures in the United States by NSI. NSI registers domain names only in the .com, .net, and .org domains. Most other countries have their own domain registration procedures and grant registrations with country codes as the top level domain (such as .de for Germany, .ca for Canada) rather than .com, .gov, .net, etc. There is currently no procedure for refusing to register a second-level domain name in a particular country because it has already been registered in another country. Thus, identical second-level domain names are being registered by different applicants in different countries, and they are distinguished from one another only through the use of the country code. For example, McDonalds may be registered by one party in the United States as "mcdonalds.com" and by another party in another country as "mcdonalds.de" or "mcdonalds.ca." This would deprive the more famous McDonalds from using its name as a domain name in Germany or Canada, arguably depriving it of trademark rights (though the .com domain is global), and causing confusion in the marketplace in Germany or Canada. To date there is no body of law which would give the trademark owner/U.S. domain name registrant any comfort. The global reach of the Internet argues for a world-wide authority for resolving the conflict between trademarks and domain names in cyberspace. Unfortunately, in some cases resolving the conflict calls for adjudicating trademark rights, and the differing nature of trademark rights in different countries is an obstacle to establishing such a unified authority.

7. More Property in the Networked Environment: Patent

For purposes of the present survey of the legal terrain, the main thing to know about patent is that it is more pervasive *71 in the online world than one might imagine. Encryption schemes are patented, payment mechanisms are patented, and recently the Court of Appeals for the Federal Circuit has said that business methods can be patented. [FN40] At least, many kinds of programs that accomplish crucial business functions in the online world are patented. Many kinds of businesses that were not much concerned with

patents in the past --for example, financial services, retail sales--may now need to be concerned with them.

Questions arise whether the proprietary status of many of these programs will hinder the interoperability necessary for competition. Many of the new patents appear to be drafted broadly and perhaps would be interpreted to conflict with each other if they were put into litigation. Firms often avoid these conflicts either by mutual forbearance or by cross-licensing. Probably there will still be lawsuits brought by those who are in the business of enforcing patents rather than in the business of making and selling products.

8. Still More Property in the Networked Environment: Copyright

During the transition of the Internet to a business modality, copyright was among the first issues understood to be of fundamental importance. Consequently, there has been a great deal of international and national activity dealing with copyright during the past few years, which we will not address here. Because of the ease of copying digital material, and the quality of the copies (indistinguishable from the original), distributors of text, pictures, videos, music, and software feared unchecked rampant copying that could destroy their businesses. These fears eventually culminated in legislation to protect technological copy-*72 protection schemes from those who might disable them. Technological copy protection leads to a self-help regime which we will discuss below.

Copyright protection applies to creative, original works of authorship. Mere facts are not protected by copyright law, and neither are completely unoriginal works. Much of the content posted or transmitted in cyberspace is data rather than computer programs or literary works. Data often consist merely of compilations or collections of facts which are neither creative nor original. There is increasing contention about the extent to which databases can be protected by copyright. Under current U.S. copyright law, many databases are not protected by copyright and can therefore be freely copied. Copyright protection, if it applies at all, will be "thin," covering only the original method of organization but not the facts contained in the compilation of data. [FN41]

As firms put their businesses online, more and more of them will have data compilations that they wish to protect from copying (for example, inventories, marketing information, supplier information). In some cases, the state laws dealing with unfair competition may be invoked to protect a database from copying. There is also a debate whether database owners may use contract restrictions or technological protection to prevent copying even though the copyright law itself gives the owner no proprietary rights in his or her creation. The extent to which these valuable compilations may or may not be protectable property of the compiling firm will have to be evaluated in each case.

No doubt business decision makers realize that it is a copyright violation to put pictures and text belonging to others on a Web site without permission, just as much as it *73 would be to put them in an advertising brochure without permission. Firms in the process of going online should also realize, however, that some characteristic Web practices they may take for granted are at least questionable under copyright law. For one thing, computers make "copies" almost every time they do anything. For this reason browsing through various texts online could be a copyright violation even though browsing through texts in a bookstore isn't. Even though in the physical world the "first sale" doctrine ensures that one may freely pass on to someone else a physical object embodying a copyrighted work (e.g., a book), this right does not readily translate to the online world, because when you send a digital "object" to someone else your computer keeps a copy and makes a copy to pass on. Email messages, like letters, are owned by their authors, so the practice of forwarding e-mails all over the network is prima facie a copyright infringement.

The practice of "framing" one firm's Web site inside another's for the purpose of displaying advertising may create an unauthorized derivative work. The practice of "linking" --Web page design that allows

viewers to click on a link, a piece of text or graphic, and be transported to another Web page--may be construed to violate reproduction rights or distribution rights of the copyright holder in the material that is linked to. It may be argued by linkers, at least, if not by framers, that the practice is so characteristic of the Web that it is appropriate to assume that anyone who maintains a Web page has impliedly granted permission to link to it. But may such implied permission be disclaimed simply by placing on the page a notice that permission to link to it is not granted? So far there are no clear legal answers either to the question of whether implied license exists to link to Web pages, or to the question whether such an implied license, if it exists, can be readily disclaimed by notice on the Web page.

*74 If the defense of implied license is up in the air, so is the traditional defense of "fair use." In copyright law some uses that would otherwise be infringement may be found to be fair use. Might this defense apply to Web practices such as linking or framing? The Copyright Act sets forth a list of nonexclusive factors to be considered, [FN42] including what kind of material was taken, and how much of it, but courts have generally said that the most important factor is whether or not the copying interfered with the owner's market by supplanting a portion of the demand for the copyrighted material. [FN43] In the digital world, where transaction costs are dramatically lower, many items that owners could not formerly charge for may now be charged for (for example, extracting micropayments for the right to quote a few sentences from an article). Thus, if economics is all there is to fair use, there will be far fewer findings of fair use in the digital world. The issue is deeply disputed among policy makers and legal scholars; businesses that wish to make use of small portions of others' material should stay tuned to this debate.

9. Contract: Policing the Bargain

Whereas copyright in the digital world has received a great deal of attention, it is contract law that may turn out to be the more important. It has always been possible for some firms to structure intellectual property by contract, primarily by provisions in licenses. As commerce of all kinds becomes digitized, however, contractual alterations of intellectual property rules become feasible for more and more firms and transactions. Many firms in the digital environment are contracting around established rules of intellectual property. (By "contracting around established rules," we mean treating those intellectual property rules as default rules that only govern the transaction unless the *75 parties enter into an agreement to be bound by different rules of their own choice.)

The practice of contracting around intellectual property rules forces business decision makers as well as policy makers to consider to what extent the established rules of intellectual property are variable by contract, as well as who--whose legal system--will decide that question. It also forces policy makers to consider what kinds of contracts will be valid and enforceable, and whose law will decide that question. [FN44]

Consider first to what extent intellectual property rules can be varied by contract. The question implicates important background issues:

(A) Pre-emption: When does the U.S. federal intellectual property regime trump contracts otherwise enforceable under state law? Pre-emption is a complicated area of legal doctrine, in which patents and copyrights are treated differently. Clearly a state cannot declare that patents have a shorter term in California than in other states, but there are large grey areas. One court thought that contracts are not subject to pre-emption because contracts only bind the immediate parties, but this reasoning may be shaky in the online world, and so far the decision has not become a rule for other courts. [FN45]

(B) Freedom of contract: In the networked digital environment, some people argue that no law is needed other than the invisible hand produced through myriads of contracts. We must bear in mind, however, that

it is a fallacy to think that contract can flourish without a background law that shapes and bounds it. [FN46] No one would have any certainty in trading without a system of background rules against force, fraud, and things off limits *76 to trade (such as human beings). These rules are complex and controversial in developed legal systems, extending to concepts of unconscionability, contracts in restraint of trade or contrary to public policy, etc. The issues of who will define and enforce these limits in the networked digital environment, and how they relate to contracting out of intellectual property rules, have yet to be addressed meaningfully.

(C) The role of the public domain in the economic justification of intellectual property: In the traditional justification most often invoked in U.S. law, the body of intellectual property law is treated as being the result of a giant economic cost-benefit analysis. Rights are granted to creators--so it is routinely argued--solely to the extent necessary to achieve the correct incentive structure to draw forth the optimal amount of new information and invention. Schemes of contracts that create property-like protections for things that are otherwise not copyrightable or patentable threaten to upset the incentive structure by diminishing the public domain needed by future creators. The same argument applies to contractual attempts to limit exemptions or defenses, such as the applicability of the "fair use" doctrine or the "first sale" doctrine. Right now the validity of such contractual limitations is unclear.

Turning to the issue of validity, the networked digital environment has indeed foregrounded some difficult issues.

(A) "Click-through": Is "click-through" going to be a valid method of contract formation? What issues will be important to validity? Possibilities include:

- . whether or not the recipient had a meaningful opportunity to view the terms;
- *77 . whether or not the terms were presented in big enough print or clear enough language;
- . whether or not the recipient manifested assent; and
- . whether the manifestation of assent occurred prior to the transaction.

"Click-through" contracts are to some extent analogous with "shrinkwrap" contracts, the validity of which is still in doubt. [FN47]

(B) Machine-made contract: To what extent can computers substitute for people in assenting to contractual provisions? A main issue here is at what point legal enforceability should depend upon the presence of a human being in the transaction. It will no doubt be efficient and unproblematic for repetitive tasks, such as ordering supplies from the same supplier under the same terms, to be accomplished by machine. One could require, though, for example, that the machine should be programmed to let out a warning beep to alert a human being if the terms change. A different and important context for asking this question has to do with situations in which one's personal computer automatically enters into "contracts" with various Web sites. Will the terms accepted by your computer be binding on you? This is an area whose legal implications are only beginning to be explored.

(C) Adhesion contracts and market failure: Standard form contracts that are uniform throughout an industry, often called adhesion contracts because of their take-it-or-leave-it quality, begin to look like a property scheme designed by private companies instead of by the government. Economic thought about uniform adhesion contracts is that they are neither good nor bad in the abstract but must be evaluated in context. Contract terms in an industry might be uniform *78 because the package of terms won out in a free market; in that case, consumers simply have voted with their dollars to buy an item with one set of warranties and exclusions and not some other set. On the other hand, contract terms might be uniform because of they are imposed by firms with market power (by monopolization or collusion). To the extent that judges accept this economic view of standard form contracts, their validity depends upon market circumstances, so they cannot be declared either valid or invalid on a wholesale basis. Companies wishing

to use standard form contracts should consider the market context and what the contract aims to accomplish.

(D) "Running" contracts: So far we have talked about contract validity as between the immediate parties. But we must also consider contracts that purport to "run" to successors of immediate parties, i.e. contracts imposed by a transferor that attempt to bind all future transferees (contracts that "run with" an information "object"). Such contracts are important in the networked digital environment. For example, Netscape released its browser software under the General Public License promulgated by the Free Software Foundation, and this license also governs Linux and other software. [FN48] Its important feature is a "running" provision that any user in the chain of distribution must make public the source code for any improvements developed by the user. This example is a narrowing of copyright--in fact the license is known as "copyleft"--but the same technique can be used to broaden copyright, for example to foreclose a fair use defense for all users in a chain of distribution.

To what extent running standard-form contracts will be enforceable is an important issue, particularly for considering the legal status of the operations of the new generation of sophisticated copy protection and *79 management systems, sometimes known as trusted systems. [FN49] Firms that promulgate contracts that purport to be binding on successors to the initial buyer will need to consider whether they are in fact enforceable against successors. Firms that are buyers removed in the distribution chain from the originator of a contract will need to consider whether they are bound by it.

10. New Generation Copy Protection: Technological Self-Help

Sophisticated rights-management programs can be programmed to prevent delivery of a piece of content until payment is received and credited, to prevent all copying of a piece of content or the making of more than n copies, to prevent printing a copy or more than n copies, to prevent reading it more than once or more than n times, to destroy the content if the user attempts to do something prohibited, and so on. Many of the visions of self-ordering in the information context -- the envisioned shift from fixed rules of property to rules variable by contract, for example -- rest on the assumption that all of the details of these contracts will be rendered self-enforcing through the use of technological rights management systems.

Self-enforcement is not the same as enforcement by a court. Technological management systems are a species of technological self-help. In this they are unlike legal contracts. They are more like sending over a committee of one's friends to intimidate a storekeeper into paying a debt than they are like relying on legal enforcement of contract. With the advent of these systems, technology has (at least temporarily) outrun the law.

People are betting different ways on whether and when the law will catch up. Legal support for trusted systems has *80 been enacted, in the form of the provisions of the Digital Millennium Copyright Act aimed at preventing disablement of copy protection and management systems. These provisions are aimed not only at pirates themselves, but also at those who produce and use technologies that might be used for piracy. [FN50]

At present, many businesses are concerned that technologies produced for a legitimate purpose may be attacked as being possibly usable by pirates.

So far the law has not dealt with the other side of the picture--the question whether there should be limits on the operations of copy protection and management systems. For example, can such systems be used to lock up indefinitely information which is not covered by intellectual property rights or is covered only for a limited time? Can such systems be used in lieu of contracts that courts might have found unenforceable?

These issues remain open. Business decision makers have the opportunity to shape the legal infrastructure in which they must compete and survive in the future.

FNa. Margaret Jane Radin is William Benjamin Scott & Luna M. Scott Professor of Law, Stanford Law School, Co-Director of Stanford's Law, Science, and Technology Program, and Of Counsel to Heller Ehrman White & McAuliffe.

FNaa. Daniel L. Appelman is a Shareholder, Heller Ehrman White & McAuliffe, Silicon Valley Office, and Chair of the firm's Electronic Commerce Practice Group.

FN1. An ever-broadening array of different kinds of businesses is developing in the electronic marketplace. Sometimes the middleman is being eliminated (as in direct retail sales on the Web by Dell Computer); sometimes a new middleman is being created (as in book brokering by amazon.com). New conglomerates and spheres of influence are in the process of forming (for example, AT&T acquires TCI, which has acquired @Home, which intends to acquire Excite). It is too soon to tell how all this will sort out economically. We can note, at least, a range of different business types with significant electronic aspects, to keep in mind as we take a look at some basic legal questions.

- . sales of physical goods: for example, amazon.com., Compaq, cdnow . auctions: for example, priceline.com, eBay
- . advertising: for example Yahoo!, NetCenter, Excite
- . subscriptions, pay-per-view, pay-per-play: for example, Wall St. Journal online, Consumer Reports
- . sales of services: for example, securities trading sites such as eSwab, etrade
- . business to business trading: for example, financial EDI, extranets
- . outsourcing and integration: for example, IBM's total "solutions" for e-commerce
- . infrastructure: for example, ISP's, payment mechanisms such as MilliCent, security systems such as RSA, pipelines such as @Home and the telephone companies

FN2. The crypto debate, which includes the issue of key escrow as well as the issue of export controls, can be followed at the site maintained by the Center for Democracy and Technology, <http://www.cdt.org/crypto/>.

FN3. For an explanation of public key cryptography, including an explanation of digital signatures, see RSA's crypto FAQ, <http://www.rsa.com/rsalabs/newfaq/>.

FN4. In practice an extra step is added to minimize the amount of public key encryption and decryption necessary: a one-way mathematical function known as a hash function is applied to the message to give a unique short bit-string (hash value). The integrity of the message can be verified if it hashes to the same result when a receiving party's computer reapplies the hash function. If the parties only need to guarantee the integrity of the message, but do not need to keep it secret and do not need to verify the identity of the sender, then the message can be sent in the clear (unencrypted) with the hash result, and the receiving party can reapply the same hash function and check to see if she obtains the same hash result.

If the parties also need to verify the identity of the sender, the sender can use his public key to encrypt the hash value of the message and append this short encrypted bit-string to the message before sending. Then the receiving party can decrypt the hash value with the sending party's public key and then apply the hash function to the message to see if they match; if they do, the receiving party knows the message came from the party whose public key he has applied. This is the most common form of digital signature.

Finally, if the parties need to keep the message secret, they can avoid using public key encryption

for the entire message by using what is known as a digital envelope. In this procedure, the sending party uses traditional encryption requiring a shared key (for example DES) to encrypt the message, then uses public key encryption to encrypt the necessary shared key and send it to the other party. Thus, in practice, often the receiving party will use the sending party's public key to decrypt a hash value which serves as a digital signature and also to decrypt a shared key which will be used to decrypt the message.

FN5. See Michael Fromkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OREGON L. REV. 49 (1996), available online at <http://personal.law.miami.edu/~froomkin/articles/trusted.htm>.

FN6. See, e.g., Verisign, at <http://www.verisign.com>.

FN7. A useful catalogue of digital signature legislation is at the website of the Chicago firm of McBride Baker & Coles, http://www.mbc.com/ds_sum.html.

FN8. For example, the Utah Digital Signature Act (1996), available at <http://www.commerce.state.ut.us/web/commerce/digsig/act.htm>, assumes that public key cryptography requiring a particular infrastructure will be used. Professor Jane Kaufman Winn argues that more technology-neutral legislation will have a better chance of remaining effective as technology evolves. See Jane Kaufman Winn, *Couriers Without Luggage: Negotiable Instruments and Digital Signatures*, 49 SOUTH CAROLINA L. REV. 739 (1998), available online at <http://www.law.sc.edu/sclr/WINN.HTM>.

FN9. For a good overview of network security issues, see Special Report: Computer Security and the Internet, in *SCIENTIFIC AMERICAN* October 1998 pp. 98- 117.

FN10. They are different in many respects too: presenting a Web page to a consumer costs a lot less than producing and mailing a catalogue; the Web page can be automatically tailored to the consumer and can be continually updated to reflect new items and delete those that are out of stock; and integrated merchant software packages can automatically re-order from suppliers when necessary, take care of shipping, and more.

FN11. See Robert D. Fram, Margaret Jane Radin, and Thomas P. Brown, *Altered States: Electronic Commerce and Owning the Means of Value Exchange*, *STLR* (Stanford Technology Law Law Review), <http://stlr.stanford.edu>, forthcoming 1999 (hereafter "Altered States").

FN12. The Financial Services Technology Consortium, a group consisting of prominent banks, financial services providers, and technology companies, has developed a digital check project consisting of hardware and software to perform the same functions as those of paper checks. In the pilot phase, the first digital check was processed in June 1998; it is estimated that digital checks will be in widespread use in another two years. For more information, see <http://www.echeck.org/>.

FN13. See, e.g., the MilliCent system developed by Digital Equipment Corporation, <http://www.millicent.digital.com/> (Compaq, which now owns Digital, aims to find a partner to help bring MilliCent to market and states that it should be offered to the public in 1999). See also, IBM Micro Payments (formerly known as Mini-Pay), <http://www.hrl.il.ibm.com/mpay/>.

FN14. These issues are explored in *Altered States*, cited in note 11, *supra*.

FN15. DigiCash, whose eCash is based on David Chaum's pioneering patents, recently filed for Chapter 11 reorganization, see <http://www.digicash.com/>. CyberCash recently abandoned its CyberCoin digital cash product, see <http://www.cybercash.com/cybercash/services/cybercoin.html>.

FN16. Truth in Lending Act, Regulation Z; see 15 U.S.C. 1601-1666j, 12 C.F.R. part 226.

FN17. For information on SSL, see <http://home.netscape.com/newsref/ref/128bit.html>.

FN18. For example, if consumers can receive a free checking account by clicking in a box that allows the bank to disseminate their financial data however it wishes, consumers may undervalue their privacy interests when they click on the box, perhaps because they cannot imagine what the harm will be like until they later suffer injury from the bank's practice. Those who accept this argument will make the analogy to legal regimes that do not permit tenants to waive the implied warranty of habitability in return for lower rent, and do not permit consumers to waive strict products liability in tort in exchange for a lower price on a product.

FN19. For information on the European Directive on Data Protection, see PETER P. SWIRE AND ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE AND THE EUROPEAN PRIVACY DIRECTIVE, THE BROOKINGS INSTITUTE 1998.

FN20. See Federal Trade Commission, Privacy Online: A Report To Congress (June 1998), available at <http://www.ftc.gov/reports/privacy3/toc.htm>.

FN21. See, e.g., <http://www.yahoo.com/info/privacy/>.

FN22. See <http://www.w3org/p3p/nutshell.html>.

FN23. See, e.g., TrustE, http://www.truste.org/about/about_truste.html.

FN24. See Federal Trade Commission, Rules Of The Road For Internet Advertising (outlining applicable laws), available at <http://www.ftc.gov/bcp/online/pubs/buspubs/ruleroad.htm>.

FN25. For An Overview Of Current U.S. Statutes And Pending Bills, see the Web Site of John Marshall Law School, <http://host1.jmls.edu/cyber/statutes/email/state.html>.

FN26. Enforcement of the basic rules enabling commerce depends upon personal and subject matter jurisdiction, based upon territorial sovereignty, and also upon whose law will be applied, based upon choice of law rules that also rest on territorial sovereignty.

FN27. See Margaret Jane Radin And R. Polk Wagner, The Myth Of Private Ordering: Rediscovering Legal Realism In Cyberspace, ____ CHI.-KENT L. J. ____ (forthcoming 1999)(hereafter "The Myth Of Private Ordering").

FN28. See "Selected Tax Policy Implications of Global Electronic Commerce", U.S. Treasury Department (Nov. 1996), available at <http://www.ustreas.gov/taxpolicy/internet.html>.

FN29. Bensusan Restaurant Corp. v. King, 126 F.3d 25 (2d Cir. 1997); Cybersell v. Cybersell, 130 F.3d 414 (9th Cir. 1997); CFOS 2 GO, Inc. v. CFO 2 GO, Inc., 1998 U.S. Dist. Lexis 8886 (N.D. Cal. June 5, 1998); Green v. William Mason & Co., 996 F. Supp. 394, 399 (D.N.J. 1998).

FN30. Zippo Manuf. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998).

FN31. Carnival Cruise Lines v. Shute, 499 U.S. 585 (1991).

FN32. See, e.g., Playboy Enterprises, Inc. v. Universal Tel-A-Talk, 1998 U.S. Dist. LEXIS 17282; Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc., 939 F. Supp. 1032 (S.D.N.Y. 1996).

FN33. See, e.g., Boston Professional Hockey Assoc., Inc. v. Dallas Cap & Emblem Mfg., Inc., 510 F.2d 1004, 1010-11 (1975), where defendant was selling National Hockey League logos, unattached to a product (such as a hat or sweatshirt). Although the court recognized that the case was difficult under traditional trademark law because a reproduction of the trademark itself was being sold, unattached to other goods or services, the court concluded that trademark law should protect the trademark itself: "Although our decision here may slightly tilt the trademark laws from the purpose of protecting the public to the protection of the business interests of plaintiffs, we think that the two become ... intermeshed" *Id.* at 1011.

FN34. The Federal Anti-Dilution Act of 1995, which became law in 1996, is section 43(c) of the Lanham Trademark Act, 17 U.S.C. 1125(c).

FN35. The trial court stated in *Panavision Int'l v. Toeppen*, 945 F. Supp. 1296, 1301 (C.D. Cal. 1996), *aff'd* 141 F.3d 1316 (9th Cir. 1998): "Whereas traditional trademark law sought primarily to protect consumers, dilution laws place more emphasis on protecting the investment of the trademark owners."

FN36. See *Panavision Int'l v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998).

FN37. See *Intermatic v. Toeppen*, 947 F. Supp. 1227 (N.D. Ill. 1996).

FN38. See, e.g., *Gateway 2000 v. Gateway.com*, 1997 U.S. Dist. Lexis 2144 (E.D. N.C. 1997); *Interstellar Starship Services, Ltd. v. Epix, Inc.*, 983 F. Supp. 1331; *Albert v. Spencer*, 1998 U.S. Dist. LEXIS 12700.

FN39. See the Clinton Administration's White Paper, National Telecommunications & Information Administration, Management of Internet Names and Addresses (June 5, 1998); proposed rule, 15 C.F.R. chapter xxiii (Recommendations of the Dept. of Commerce National Telecommunications and Information Administration), available at <http://www.ntia.doc.gov/ntiahome/domainname/022098fedreg.htm>. See also Jeri Clausing, Planning the Internet's Final Privatization, *New York Times*, Oct. 5, 1998.

FN40. See *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*, 149 F.3d 1368 (1998).

FN41. The notion of "thin" copyright, as well as the requirement of originality and the concomitant difficulty in protecting collections of facts, is set forth in an important decision of the U.S. Supreme Court, *Feist Publications v. Rural Telephone Service*, 499 U.S. 340 (1991).

FN42. See section 107 of the Copyright Act, 17 U.S.C. 107.

FN43. See, e.g., *American Geophysical Union v. Texaco, Inc.*, 60 F.3d 913 (2d Cir. 1994).

FN44. The proposed Uniform Computer Information Transactions Act, successor to the proposed Article 2B of the Uniform Commercial Code, if enacted into law by the various states, would decide a number of important open questions regarding contract validity.

FN45. *ProCD v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996).

FN46. See Radin and Wagner, *The Myth of Private Ordering*, *supra* note 27.

FN47. The proposed Uniform Computer Information Transactions Act, successor to the proposed Article 2B of the Uniform Commercial Code, if enacted into law by the various states, would validate most "shrink-wrap" contracts.

FN48. See <http://www.linux.org/info/gnu.html>.

FN49. See, e.g., Mark Gimbel, *Some Thoughts on the Implications of Trusted Systems for Intellectual Property Law*, 50 *STAN. L. REV.* 1671 (1998).

FN50. The Act creates a new chapter 12 in U.S.C. Title 17. For the policy arguments about why such provisions are needed, see the House Commerce Committee report on the Digital Millennium Act (H.R. Rep. No. 105-551, part 1), which is available at <http://thomas.loc.gov/cp105/cp105query.html>. Cf. the report released in mid-1998 by the Copyright Office suggesting that legislation is not advisable, available at <http://lcweb.loc.gov/copyright/reports/>.

END OF DOCUMENT