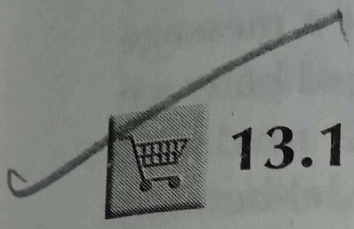
Legal Issues



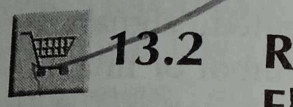
13.1 Legal Issues

The world is used to conducting business and commerce on signed paper documents. Two millennia of commerce has been based on the written document with its value 'authorised' by the signature of a duly authorised officer. The current legal practice has paper documents and signatures affixed thereon as a foundation. Electronic documents and messages, without the familiar signatures and marks, have changed the scene and trade wants to be assured that the electronic world is safe. The e-commerce system must, therefore, offer at least the same level of reliability as that which obtains in the paper world, notwithstanding the significant differences between the concepts embodied in electronic messages and paper documents. It is well known that frauds do take place in the traditional paper-based commercial transactions. Signatures can be forged, paper documents can be tampered with, and even the most secure marks, impressions, emblems and seals can be forged. But then these are known, and trade as well as the legal community know how to deal with these problems. Companies set aside funds to take care of losses due to such frauds. For example, credit card companies do know that a small percentage of transactions is fraudulent in nature. The world is 'comfortable' with these problems, since they have been there for as long as we have been trading.

The electronic world, on the other hand, exposes us to issues which were hitherto unknown, since they are directly the outcome of creating documents electronically, transmitting them over worldwide computer communication networks. Trading partners exchange documents electronically. They need to convince themselves that such documents are authentic when received over networks, and that their authentication can be established in case of dispute. Transactions may be electronic, but the key concepts of admissibility of evidence and evidential value of electronic documents, which are central to the law, remain the same. There must be a way to prove that a message existed, that it was sent, was received, was not changed between sending and receiving, and that it could not be read and interpreted by any third party intercepting it or deliberately receiving it. The security of an electronic message, a legal requirement, thus gets directly linked to the technical methods for security of computers and networks. From the legal angle, there is a further complication because the electronic message is independent of the actual medium used for storage of transmission. The message can be stored on a floppy, disk, or an optical disk. Likewise, it may be transmitted over a local area network, a Virtual Private Network (VPN), or the Internet. The physical medium could be coaxial cable, radio link, optical fibre or a satellite communication channel.

The legal issues of e-commerce have generated tremendous interest among technologists, traders and legal experts. Many of the early e-commerce experiments, and even production systems went into operation without any legal interchange agreement between trading partners, or between networks and their customers. No laws for e-commerce existed in India too. When the Indian Customs EDI System (ICES) project got off the ground in 1995, it was without any e-commerce/EDI law, or even a proper interchange agreement. Since then, much has been achieved. The Indian Parliament passed the Information Technology Act in 2000, the details of which are given in Chapter 16. Technologists and users alike have shown confidence in e-commerce, though electronic messaging technology gives rise

to many legal questions and issues. As early as 1991, Benjamin Wright,[1] a Texas-based US attorney, expressed confidence in his book, *The Law of Electronic Commerce* that 'if implemented intelligently, electronic communication can confidently be used for legal transactions'. He rejected 'the attitude that technology deserves suspicion'.



13.2 Risks: Paper Document versus Electronic Document

The risks that afflict the traditional signing of a paper document are many. There is no standard method for signing in ink: signatures could be in created in any manner—strange, non-decipherable scribble, changed signatures with every transaction. Moreover, it is seldom compared against specimens for authenticity. But then this is accepted since we feel confident that signatures are there, though they may have been forged. There is no guarantee that any given ink signature can be verified by forensic science. Given a reasonable sample of specimen signatures, science can offer a probable, well-informed opinion on the authenticity of signatures in question. The originator may repudiate his own signatures on a document in an attempt to disown a transaction. The receiver may raise any number of objections. Moreover, some pages of a document may not have been signed, or may have been altered after the signed document was created. There are therefore myriad risks associated with a paper document, and these risks are distributed across a number of acts performed by various players in a commercial transaction. These include:

- The style of signing by the originator
- The secret choice of the originator to change his signature
- The content of the signed document
- The facts external to the document, but in historical context to it

- Competence of experts who opine on the authenticity of signatures, and pages of document
- The views of courts on the issues in case of a dispute.

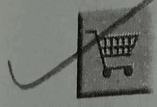
It is clear that risks abound in the authentication of paper documents. The paper world has legally enforced documents, through the evidence of a 'document', a 'writing', and a 'signature'. In the electronic equivalent, it amounts to the following: 'writing' requires that a record is created, 'signature' reflects the desire for a 'legal and ritualistic symbol of finality, assent, and authenticity.' In e-commerce, there is concern that in the absence of proper controls, it is relatively easy to change an electronic record. Proper controls need to be enforced in e-commerce transactions. For example, business software used for e-commerce may be restricted to authorised users only and all uses of the same including unsuccessful attempts should get automatically logged in an audit log. Message confirmation, record making and control standards have emerged. These have been discussed in the chapters on Security Issues and PKI. Some of the techniques for ensuring integrity of messages during communication include:

- A professionally operated network supported by disaster recovery methods
- Communication protocols, network control and management software
- Data checking and preservation techniques
- Cryptography
- Use of Auditors

Since message authentication is linked to technical methods in that one has to prove to a court the source and integrity of a message, the security issues of e-commerce are intimately related to legal issues. Authenticity, integrity, confidentiality, and non-repudiation of origin and receipt of electronic transactions conducted over networks, are essential for authenticating electronic messages in case of a dispute. Authenticity may be the key to a legal dispute. Before evidence of an electronic message is admitted in a trial, a number of objections can be raised on the grounds of authenticity. According to Wright, the

principles of evidence law developed around paper documents are valid in e-commerce transactions, resulting in issues which arise as follows:

"In the classic trial, one party, the 'proponent,' seeks to 'admit' a bit of evidence (such as a record of an invoice) to prove a point that matters in the trial. Typically the proponent must 'lay a foundation for the evidence to show its admissibility under evidence law (or the rules of evidence). The other party, the 'opponent,' may object if there is a basis for doing so under the law. If the judge allows the admission, the 'trier of fact' (normally the jury but sometimes the judge) may consider the evidence in deciding the case. A trier of fact generally decides a case only on the basis of evidence that is admitted."



13.3 Technology for Authenticating Electronic Document

Techniques have been developed which can 'authenticate' e-commerce transactions with a degree of certainty which is the same or more than that obtainable with paper documents. Cryptography and digital signatures are the pillars of this technology. In fact, a digital signature is much more reliable than a handwritten signature since it is not subject to the originator's will or intention to deliberately change his own signature. The use of Trusted Third Parties (TTPs) is essential for non-repudiation services. They perform the role of an independent witness, similar to the function of a notary public.

Cryptography techniques, based on symmetric and asymmetric methods of generating keys which are used to transform the message to encrypt it, have been discussed in Chapter 14. A cryptographic check value is a way of preserving the integrity of the message data. The sender binds his unique identifier onto a message in such a way that the message cannot be forged by the receiver, and cannot be denied by the owner of the secret key. A combination of public and private

cryptographic keys supports digital signatures. It is the independent certifying authorities that are expected to hold the public keys of all users, while the users would hold the public keys of the certifying authorities that they are connected to. Some certifying authorities, the unconditionally trusted ones, would actually generate the key pairs for digital signatures, and distribute them safely. Others would issue the certificate of the public keys that they hold in their register.

The state of Utah in USA, was one of the earliest to adopt a Digital Signature Act, which is known as the Utah code. This Act envisaged the global use of public key cryptography based on government licensed CAs. This concept was implemented in the Indian Information Technology Act, 2000, which is discussed in Chapter 16. The originator of a document has to keep his private key secret. In e-commerce transactions, it is the private key that becomes the object of fraud. The risk is completely shifted to the private key and concentrated there. As opposed to this, biometric technology implemented around some part of human beings distribute such risks. Biometrics measure individuals' unique physical or behavioural characteristics to recognise or authenticate their identity. Some of the technologies that are:

- Physical biometrics such as fingerprints, hand or palm geometry, retina, iris, or facial characteristics
- Behavioural biometrics including signature, voice (which also has a physical component), keystroke pattern, and gait.

The Organisation for Economic Co-operation and Development (OECD) recommended on March 27, 1997, that member countries should establish new, or amend the existing policies, methods, measures, practices and procedures to reflect and take into account the principles concerning cryptography policy set forth in the OECD Guidelines for Cryptography Policy. These guidelines are reproduced in Appendix 8.

13.4 Laws for E-Commerce

As discussed, the legal requirement is to establish the authenticity of an electronic message or document. This includes integrity, confidentiality and non-repudiation of origin and receipt of electronic document in case of dispute. The UNCITRAL Model EDI/e-commerce Law defines an electronic data message as follows:

> "2(a) Data message means information generated, stored or communicated by electronic, optical or analogous means including but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy."

The law proposes legal recognition of data messages, and defines 'writing' and 'signature', and their admissibility and evidential value. The model law as adopted by the UNO is reproduced in Appendix 3. Individual countries were advised to enact this law with suitable modifications that may be necessary in the national context. Rules and guidelines also need to be framed for those maintaining electronic records, providing network services, Internet service providers, electronic notaries, Trusted Third Parties (TTPs), Certifying Authorities, etc. to take care of general record keeping and control requirements, confidentiality and control of data, privacy controls, access of business software and use of digital signatures.

The Electronic Transactions Act (ETA) enacted by the Singapore Government in July 1998 sought to "create an environment of trust, predictability and certainty" to provide a conducive framework for electronic transactions and the electronic formation of contracts. The ETA addressed issues of electronic records and signatures, liability of network service providers, electronic contracts, digital signatures and the role of certification authorities. Additionally, the Computer Misuse Act and the Privacy code were proposed to be suitably adopted to protect computer systems and consumer data.

13.5 Legal Issues for Internet Commerce

Internet commerce raises legal issues through the provision of the following services:

- Online marketing
- Online retailing: ordering of products and services
- Financial services such as banking and trading in securities
- Online publishing
- Exchange of electronic messages and documents EDI, electronic filing, remote employee access, electronic transactions
- Online contract formation

Trade and commerce over the Internet generate several legal issues[3,4], which are discussed below.

13.5.1 TradeMarks and Domain Names

Domain names have traditionally been assigned by the InterNic Registry in the USA. The .com domain used by commercial entities uniquely identifies them in cyberspace. The latter is worldwide since the Internet, like a river, is not confined to the geographical boundaries of a country. This advantage poses a problem too. A company takes a domain name from the Registry in its name. Unlike the traditional commercial world where different companies may have the same trademark in different products or services, in cyberspace, only one name can be assigned as Name.com. Thus the company which registers its name first for the domain name, eliminates all others from using that name in cyberspace. As one would expect, this has led to legal battles. It has been argued in courts in the USA and the

UK that a domain name functions as a trademark. Therefore, a person or a company not entitled to the trademark, but using it as a domain name is guilty of trademark infringement.

The infringement of trademarks by the use of domain names is essentially on two grounds: that of confusion, and that of dilution. In the US, the Lanhan Act, 1984 defines a trademark as "any word name, symbol, or device or any combination used or intended to be used to indicate the source of the goods". Liability for infringement, when the infringer uses a mark that may be confused with the trademark of another, whether deliberately or through negligence, when seen to be used in the context of similar goods or services, is strictly on the infringer. The celebrated case of Maritz Inc. vs. Cybergold Inc. considered the issue of trademark confusion with domain names. The former was using unregistered 'GoldMail' with its GoldMail service on the Internet, with the URL *goldmail.com*. Cybergold, on the other hand, was developing a similar Internet service with the domain name *cybermail.com*. The issues debated included the matter of confusion between the marks 'GoldMail' and 'CyberMail', and the likelihood of confusion among appreciable number of buyers.

The trademark dilution issue came up in *Hasbro Inc.* vs. *Internet Entertainment Group Inc.* The court was convinced that Hasbro had been producing a game, Candy Land, for young children for several years and that 94 percent of the mothers were aware of this game. Internet Entertainment Group, on the other hand registered a domain name *candyland.com* at which site they featured pornographic materials. The court granted an injunction preventing the latter from using the domain, and ruled that rightfully belonged to Hasbro.