

Corporate Policies for Electronic Commerce
delivered at the HICCS Conference Jan 10, 1997
Nashville, Tennessee

Richard W. Oliver
Owen Graduate School of Management
Vanderbilt University, Nashville, Tennessee

Abstract

This paper proposes an approach to developing corporate policies for electronic commerce. The Internet and related public-private networks, such as EDI and Intranets are growing rapidly as a medium for commercial enterprises to transact business and develop relationships both internally and externally. While there is no body of law or commercial precedent governing such activity on the Internet, this paper argues that corporations would be well advised to construct policies for their individual approach to electronic commerce. The paper offers a schema for developing such policies.

1. INTRODUCTION

Scenes from somewhere in cyberspace:

XYZ Retail, a large, successful, traditional retailer with stores across the country, decides to set up a presence on the Internet. The company hires Joe Pearl to be the company's Webmaster. Joe also has his own server and website at home on which he has posted an extensive array of adult content. Wishing wider availability of his material, Joe adds a link from the XYZ site to his own site. It takes several months for XYZ to discover the adult material (it has been a joke on the Internet for some time, but none of XYZ's executives are Internet users so they are unaware of the situation). The situation surfaces when several shareholders raise the issue at the company's annual meeting. Reporters covering the otherwise boring annual meeting give the story national exposure. XYZ shuts down the site and immediately dismisses Joe. Joe files suit against the company claiming he did not know that it was against company policy to do what he did. Unfortunately, neither the XYZ Employee Manual nor their Code of Conduct Policy addresses the issue for which Joe was dismissed.

o*

Betty Ark, an employee of a major global corporation resides in Kansas and routinely downloads information from a company server in a foreign country. One day Betty notices that the company's employees in that country have received sensitive cost information about a competitor. While the laws in that country are silent on the acquisition and use of such competitive information, it is clearly not useable in the U.S. Betty nonetheless takes the information and uses it in structuring a bid the company is making later that day for a contract with the U.S. government. The competitor, also bidding on the contract, recognizes that its security has been breached and institutes a suit. Several other countries are added as parties to the suit as the data passed through lines in their areas of jurisdiction.

oo*

ABC Company decides to set up a presence on the Internet, but lacking any internal skills, hires NET Services, Inc. to construct and manage its website. ABC decides to "do it right", and commits significant dollars to NET to develop a unique approach. ABC's intellectual property is quite exciting but the Website graphics and approach developed by NET is truly outstanding and generates considerable traffic. NET decides to use the same approach for its other clients; but ABC

tells them they cannot. NET goes ahead anyway. ABC takes them to court only to find that NET, not ABC owns the Website, just as a photographer owns the images photographed, even if paid to take them.

The marketing department of a highly regarded public firm, MNA Corp., decides to advertise on one of the Internet's commercial search engines. As part of its payment, it negotiates with the search engine operator to fink all generic requests for certain types of information directly to their website, thus by-passing any potential competitor information available on the Internet. Competitors find out about the practice and demand that it stop. MNA cancels its deal with the search engine operator and publicly apologizes to its competitors. While the competitor accepts the apology, the Federal Trade Commission decides to look into the case for possible violations of antitrust laws as an illegal restraint of trade.

Frank Cap, an extremely valuable engineer for SOFIFEC a small start-up software company, routinely posts false or misleading information about a competitor's products in an Internet newsgroup discussing the competitor's product. Ray Clark, the Vice President of marketing for SOFTEC must decide what to do, as the company has taken a very public stand on the integrity of commerce on the Internet.

Ruth and Bill are dedicated, and some would say dangerous, members of a right wing paramilitary group. Ruth, a skilled computer technician works for TRA Corp. Ruth often works late and during those times she routinely and anonymously sends news bulletins and political commentary (written by Bill) to people at TRA and elsewhere via the Internet using TRAs e-mail system. Often, Ruth will "spam" various company e-mail systems, filling them with various messages and requests for donations to their cause. After many months, Ruth's identity is discovered and she is fired. She sues TRA on the grounds they have abridged her rights to free speech.

Economists tend to view corporations as a complex set of transactions that occur both internally, among employees, and externally, between the firm and its many constituencies, customers, suppliers, governments, etc. Business executives on the other hand, while recognizing that transactions are at the heart of corporate endeavors, often describe those transactions, particularly ongoing ones, in terms of a set of relationships. Of course most of the transactions and relationships by which business is conducted occurs within a given set of laws and regulations established by the various levels of governments in the geographically-defined jurisdictions in which those businesses operate. (While this paper is focused primarily on business corporations, much of the discussion is applicable to governments, professional firms and organizations, nonprofits and the like.)

In electronic network environments, such as the Internet, two problems arise in this context. First, the networks tend to span many geographic areas with varying laws and regulations. Second, there are today, no set of rules to govern activity within those networked environments. While the small community of early Internet users had a set of conventions on the use of the Internet, those conventions have largely fallen into disuse as the number of Internet users has grown so dramatically. No set of rules has arisen to take the place of those early conventions, and, in particular, no set of rules exist today to guide the use of the Internet for electronic commerce.[I] No comprehensive legal framework yet exists to regulate electronic commerce, but some legal precedents are finding their way of other areas and are being applied to various aspects of Internet activities. Many crimes that can be committed on the Internet are already covered under various

statutes. For detailed discussion of the legal issues surrounding electronic commerce see [2] and [3].

Even in situations of clearly defined legal parameters, businesses have a large number of options in the ways in which they might execute transactions and nurture relationships. An important function of senior management in organizations, then, is to determine the precise way in which to conduct their business. Business executives have a number of tools at their disposal to ensure the proper conduct of those transactions and relationships, including organizational structures, job descriptions, corporate goal setting, compensation programs, and information systems to name just a few.

One of the most important tools that companies, large and small, use to ensure the orderly, efficient, coordinated and ethical conduct of both transactions and relationships, is a set of corporate policies. Although policies are (or should be) updated periodically, they tend to transcend individual managers as they are often in place for many years and span the careers of several executives responsible for a particular set of relationships and transactions. These policies are typically the result of years of accumulated experience with business practices in a wide range of corporate activities, and can range from hiring practices, to sales practices, to manufacturing practices. A good set of corporate policies cover the most important aspects of a firm's operations and spell out for employees, and others, how the firm wishes to conduct its business.

While these corporate policies can be either formal or informal, most are, hopefully, written and widely communicated, at least within the firm. Prior to internal computer networks, corporate policies were most often committed to paper, placed in a "manual", and available in only a few centralized locations. Today, many corporate policies are now finding their way to corporate -computer servers which provide employees fast and easy access to the policies. Many companies today require new employees to review all policies relevant to their work assignment, and sign a statement that they have read and understand them.

Most corporate policies are developed to ensure the orderly conduct of business in order that the firm survive and prosper from an economic point of view. In addition, companies often write policies to ensure that their affairs are conducted not only in a strictly legal, but also in an ethical manner. In terms of policies that address the ethical conduct of transactions and relationships, some companies even require the signing of an annual statement of understanding and compliance by all employees. These ethics policies are variously referred to as a "Code of Corporate Conduct", "Corporate Ethic Statements", and the like. These policy guides are also often circulated widely among the firm's external constituencies.

With the explosive growth of the Internet as a means for both corporate transactions and relationships, corporations would be well advised to add policies for electronic commerce to those existing sets of corporate policies and, as with ethical policies, to widely disseminate them to internal and external constituencies. A study by the Conference Board found that only some 26 percent of US firms had a policy on electronic commerce, although 40 percent had such policies under consideration. Unlike ethics policies which tend to be widely circulated, these electronic commerce policies have not, as yet, received much public attention.

And, as the whole subject of electronic commerce is relatively embryonic, and the economic, legal, moral, and ethical issues regarding the Internet are only now emerging (and perhaps just the tip of the iceberg is showing). Much work on this subject can be expected over the next few years. There has been much discussion of certain aspects of Internet activity such as privacy, pornography (or more broadly on rights of publication and access), security and intellectual property rights. There was even an attempt by Congress to legislate certain content on the Internet, but it was overturned by the courts. Stepping into the void, the U. S. Federal Trade Commission recently issued a plea for a set of voluntary rules for electronic commerce.(4) While the outcome of these debates and

legislative efforts will have a far reaching effect on businesses, they will clearly take considerable time to resolve, and will likely take many different forms around the world. The issues such as privacy and security of external transactions have dominated the public debate, and some thoughtful discussion has emerged from the academy on topics such as information ownership.(5) As yet, however, there has been very little attention to issues regarding transactions, communication and relationships internal to the firm.

In light of these uncertainties, businesses themselves must begin to craft policies that will guides corporate transactions and relationships. Unfortunately, little work currently exists on this topic. In fact, no academic articles or professional papers on the subject of corporate policies for electronic commerce had been published at the time this paper was written. Writing an actual set of corporate policies to cover all companies and all situations would be nearly impossible, and well beyond the focus of this paper. However, this paper is an attempt to begin the dialogue by suggesting a tentative set of areas or situations for which corporate polices for electronic commerce should be enacted.

The short vignettes at the beginning of the paper were presented to help illustrate potential problems for corporations in the conduct of electronic commerce. While fictional, they are loosely based on actual situations, but have been disguised to protect the identity of the parties involved, and simplified to highlight the electronic commerce policies at issue.

2. THE CONTEXT FOR ELECTRONIC COMMERCE POLICIES

With the substantial growth in the routine business use of networked-enabled computing environments the ability to create and exchange information and to conduct corporate transactions is increasing at a rapid rate. As information exchange is also at the heart of development and maintenance of corporate relationships, the same might be said about the ability of computernetworked environments to speed and support corporate relationship building and maintenance, both internal and external to the firm.

In some corporations, the Internet, and the electronic commerce that it makes possible, is viewed simply as an extension of existing business practices, operations and systems of an organization. In others, it is seen as the opportunity to alter the very nature of traditional internal and businesscustomer communications, transactions and relationships. With either approach, corporations need to formulate and communicate acceptable use policies that address the issues extant with electronic commerce. In some cases, simply extending the existing corporate conduct policy and ethics manuals to include "digital communication" may suffice. In other cases, new policies will need to be created. Electronic commerce policies should define how a corporation (or any organization for that matter) is going to use and allow use of their computing resources. These policies need to provide both internal and external users with rights and responsibilities for using the corporation's information and computing resources. In conjunction with acceptable use policies internally, firms need to spell out the level of enforcement, from simple reprimands to dismissal. While this is particularly important internally, with the growth of extranets (allowing outsiders to use defined parts of a companies internal networks), it is also important for external users as well. Firms may wish to add these new policies in existing policy collections, or as in the case of ethics policies, highlight them in a set of documents that receive wide circulation, and even, perhaps, periodic review by employees who are required to sign statements of acknowledgment.

As the vignettes at the beginning serve to illustrate, many of the "rules of engagement" 'of electronic commerce are now just evolving. While many areas are already emerged, others surely have not. How then to construct a set of policies which will cover all known and yet undiscovered areas of concern? While no set of policies can cover issues that have not surfaced, a disciplined approach to writing policies could conceivably address most issues.

3. APPROACHES FOR DEVELOPING ELECTRONIC COMMERCE POLICIES

There are a number of ways of approaching the

formulation of such a set of corporate policies for electronic commerce. One way would be to examine each step of the value creation process of the firm, using a value chain analysis.(6) This would include an examination of all the primary infrastructure functions (finance, human resources, purchasing, etc.) and the inbound and outbound logistics, operations, marketing and sales functions of the firm. While such an approach might be useful, it could miss important considerations such as the internal use of e-mail. Another approach might involve an examination, and written policy to address, every transaction, internal and external, in which a firm engages. Such an exhaustive approach would likely tax the resources of even the most well-resourced and intentioned firm. And, like the value chain approach, it offers no guarantee that all transactions will be discovered and dealt with. Further, neither approach offers protection against new value creating activities, transactions or the development of relationships that are not addressed in the policies. Thus, a more generalized approach to setting corporate policies for electronic commerce seems most appropriate until the field begins to mature, and there is a common body of legislative, regulatory, litigation, commercial practice and academic literature to support a more specific and detailed set of policies.

4. GENERAL SCHEMA FOR DEVELOPING A CORPORATE ELECTRONIC COMMERCE POLICY

Perhaps then, a more valuable, albeit general approach, involves developing a set of corporate policies around relationships with six key constituencies: employees (including employee organizations such as unions), customers (including distributors, consumers and payers), suppliers, governments, other key stakeholders (shareholders, environmental and civic groups, etc.) and competitors. Against these, the four primary areas of electronic commerce "space" could be matrixed. These activity "spaces" include intranets (internal), extranet (external/private), websites and the Internet. Those companies heavily involved in private networks, such as EDI, may wish to add it as a fifth "space". *See Exhibit 1.*

5. FOUR AREAS OF CORPORATE "ELECTRONIC SPACE"

A very brief examination, from a policy perspective, of each of the four primary areas of corporate "electronic space" seems in order. In each area there are specific considerations that overlap across the other areas of concern. For instance, access levels across all computing resources, both internal and external, need to be considered in terms of current and future business policy development. Within each quadrant, however, specific areas of concern can be identified.

Intranet

This is a critical "space" for firms to develop policy, and one of the key areas of concern is data access. A policy must be developed to guide employees as to what constitutes public information, both intra-firm and extra-firm, as well as what mechanism and location for storage will be implemented. In most organizations, the information needs and requirements increase as you move higher up in the organization. The issues surrounding information access across various levels of the organization and between different business departments and business units obviously needs to be outlined.

Most intranets are firm specific computing resources that enable e-mail and information sharing. However, the ability to transmit information outside of the firms' network may also exist. A corporate electronic commerce policy must address the fact that transmission of sensitive or proprietary information via electronic communication is to be proscribed and controlled. In addition, steps must be taken to insure secure transmission of intra--company communication to protect the firm against future liability. E-mail correspondence is a simple but potentially problematic communication tool. The ability to transmit sensitive or proprietary information both inside and

outside the firm needs to be considered. Some companies are already addressing this issue by building disclaimers into the headers of all e-mail transmissions. Questions of ownership of internal e-mail should also be dealt with.

The intranet may also allow access to the Internet and web. This creates another area for the firm to consider in any policy formation. There needs to be definitions of personal and professional differentiation of access and use of the Internet. While it may be acceptable to look up a recent stock price, the abuse of personal information search and retrieval needs to be addressed. Similarly, while the previous situation may be acceptable on company time, the use of company computers and time for downloading less appropriate material, such as adult images, or "spamming" should be addressed. Copyright infringement issues regarding placement of licensed software on public directories need to be expanded to include downloading any material off of the Internet.

In some firms, many of the above policies may already be in place, but as companies move traditional back office functions such as payroll and purchasing to the intranet, and marketing programs find their way to corporate websites, new policy guidelines must be put in place. For example, if the marketing department uses the website as an advertising medium, a corporate policy needs to guide the creation, approval, and release of information to the website. Other business functions such as finance, research and development, and human resources may use the intranet or website for information dissemination, yet this is new ground for most companies and policies must define and describe acceptable use.

Extranet

While no formal definition exists, the extranet can be thought of as the digital "space" that exists between the firm's internal intranet and the public Internet. Many firms are granting rights of access to well defined internal portions of their computing and data resources for customers, suppliers and others constituents. This allows customers for instance, to order goods, schedule service calls, provide customer service information, etc. The value to firms using such extranets is that they can offer highly response service at reduced costs, as customers do most of the work. Issues surrounding privacy of the stored and displayed files are analogous to the intranet considerations. However, the level of access that is granted for one set of constituents, highly valued customers or stockholders, may be significantly different than for others such as members of the Board of Directors. Additionally, the privacy of electronic transmissions and personal records of employees is something that must be addressed in relation to the access available to each of these stakeholders.

In terms of strategic business partners and suppliers, issues may arise concerning "digital gratuities" (e.g., otherwise secure information) and influence. For example, policies need to outline acceptable business practices surrounding increased supplier access or information in exchange for better pricing. These issues extend down the supply chain; thus, firms need to determine to what extent they are going to monitor and enforce security along the extranet.

Website

Perhaps the most important "space" for a firm engaged in electronic commerce is the website, and its **design, creating and use are critical from** a policy perspective. For instance, while some firms **are able to locate internally the necessary personnel** to implement the technical aspects of the website, much of the design, presentation, and layout aspects of the website may be outsourced. However, this outsourcing is analogous to a photographer hired to take a picture for a brochure or corporate publication. The firm "owns" the brochure but unless specifically compensated for the original work, the photographer owns the rights to the actual photographs and negatives. Thus, ownership of the design of website becomes a key issue for the company. In addition, due to the ease of copying and downloading information via the Internet, firms need to think about copyright considerations

that surround their website. While there is to date no clear guidelines, some lawyers have suggested that copyrighting each and every page that is accessible at the firms' site may be prudent. Additionally, due to the ability to access information outside the website, firms need to consider disclaimers that advise users of this situation and disavow firm responsibility for the content outside their website.

Once a website is in place and operational, firms need to consider data access -- both internal and external. While the website provides information, that information typically exists in the form of files stored on internal computers. The ability to "drill down" beyond the web front-end and access directories and files that may contain other sensitive or "non-public" information must be secure. Often, widely dispersed personnel representing diverse business units, functions and organizational levels have ability to access and post information. Thus, corporate policy guidelines are a necessity to ensure consistency of approach and protection of privacy, security, etc.

The corporate website is still evolving as an electronic commerce "space". For those firms that can offer a service or product directly over the Internet, the website serves as a perpetual storefront or salesperson. In other firms, the website provides an information dissemination and retrieval frontend, analogous to existing corporate communication departments. In either case the website now serves as a direct market research mechanism and questions surrounding who owns the "information transaction" data will surely arise.

In addition, from a policy perspective, the website needs to be examined along each of the other important relationship categories. For example, which employees will have access to and the ability to change information on the site? Which departments or units of the firm will have the right to "space" on the corporate website? Who will control the "look and feel" of various departments or units, or foreign subsidiaries be permitted on the site? Will prices be posted, and if so, will all units and subsidiaries post prices?

Also, if the website and by extension the extranet are going to serve as a transaction vehicle or for information disclosure, the issues surrounding the implementation of price discounting need to be addressed. This requires a determination of the type of transactions occurring and the variety of displays required along the extranet resources. For example, a new or small volume customer might not be permitted to "view" the same website or extranet servers as a larger volume, more established customer. In such a scenario, the firm needs to consider restraint of trade and other applicable commercial laws.

Internet

The Internet itself is one of the most important areas of consideration for corporate policies. Every one of the key relationship areas will need to be examined for policy development. For example, employee access and use of the Internet while on the job needs careful attention. Will employees be granted access to the Internet, or only certain classes of employees? How much time will employees be allowed to spend on the Internet? Will the time and actual use of the Internet by employees be monitored and documented? Will such information be used in determination of compensation and promotions? Will employees be restricted solely to business use of the Internet, or will they be permitted to do personal things, such as shopping, on the Internet? If so, how much of such activity will be permitted? If abused, what will the penalties be? If an employee accesses pornographic material and leaves it on a computer screen in view of others, will that constitute sexual harassment, and be cause for dismissal?

A study by Gordon & Guckson, P.C. recently reported in Network World, suggests that few firms (30%) have policies regarding employee access to certain parts the Internet. Of those that do have such policies, only 13 percent cover access within certain hours, 39 percent specify certain employees, 41 percent spell out the type of information, and 52 percent detail the type of

information. The study goes on to reveal that other items covered by corporate "computer" policy include such things as e-mail use, company trade secrets, home or remote access and third party software.(5)

If product comparisons are made on your website and available to the general public via the Internet, the firm needs to insure the most recent comparable competitive products are shown. Failure to do so may expose the firm to defamation or wrongful advertising suits from competitors. This reasoning also implies that firms need to take a proactive approach to monitoring competitor websites to insure firm products are displayed in a correct and accurate fashion. This is not a trivial consideration given that the ease of instantaneously broadcasting inaccurate information to thousands of individuals. Firms should also create policies that direct employees responsible for electronic commerce activities to "log", document and store records of website content and other digital material consistent with firm policies for paper record storage. A firm establishing some form of extranet for suppliers, business partners, customers, etc., must ensure that it is not violating any restraint of trade laws. Competitors may take exception to being prevented from accessing the same relevant information to which others have access. Finally, firms need to be sensitive to what lawyers refer to as the "battle of forms"; the documentation, disclosures and disclaimers that accompany paper transactions of firms. Policy guidelines could ensure that employees use the "digital counterparts" of such legal protections.

4. CONCLUSION

It was beyond the scope of this paper to attempt to cover all the potential corporate policy areas of concern as firms begin to transact business and build relationships in electronic environments. It has argued that no policy could cover all the current and future issues that might need to be addressed in such a policy, but instead, proposed an approach that matrixed the most important areas of electronic "space" against the key constituencies with whom the firm develops and maintains relationships. Through this matrix the most important policy areas should emerge. More effort will be needed as new policy concerns develop in this dynamic environment.

REFERENCES

- [1] Spar, D. & Bussgang, J. J., Ruling the Net. Harvard Business Review, May-June 1996, p 125133.
- [2] Cavazos, Edward A., "The Legal Risks of Setting Up Shop in Cyberspace," Journal of Organizational Computing and Electronic Commerce, Vol. 6, No. 1, pp. 51-60, 1996
- [3] Rose, Lance., Netlaw. Your Rights in an Online World, Berkeley California: Osborne McGrawHill, 1995.
- [4] Teinowitz, I. FTC chairman seeking voluntary Web rules. Advertising Age. June 10, 1996. p.42
- [5] Branscomb, Anne Wells. Who owns Information? Basic Books, 1995.
- [6] Porter, M., Competitive Advantage, New York: Free Press, 1985
- [7] Network World. Court restores 'Net freedom. Vol. 13, Number 25. June 17, 1996.

EXHIBIT I

Intranet	Electronic Commerce Space				
	Extranet	Website	Internet		
Key Constituent Relation- ships	Employees	access	access	access	access
		equity	acceptable	acceptable	acceptable
	Customers	use	use	use	use
		privacy		privacy	
	Govern- ments		access	access	access
			equity	equity	equity
			security	security	security
			access	access	access
	Suppliers		privacy	privacy	privacy
			security	security	security
Stake- holders		property	property	property	
		rights	rights	rights	
Competitors		access	access	access	
		equity	equity	equity	
		access	access	access	
		privacy	privacy	privacy	
				equity	
				fairness	
				property	
				rights	