***297**

IDEA: The Journal of Law and Technology
1991

TRADE SECRETS AND TELECOMMUNICATIONS: THE PROBLEMS WITH LOCAL AREA NETWORKS

Scott M. Alter [na]

PREFACE

The volume of information communicated by electronic means has increased dramatically over the past few decades. Some of this information may be considered a trade secret by its owners. Where this is the case, the manner in which the information is communicated and transferred can have a profound effect on whether a court will conclude that the information is legally a trade secret.

Various devices have contributed greatly to this increase in electronic communications. One such device, the Local Area Network (LAN), is particularly well suited to efficiently communicate information. Where this communicated information is considered a trade secret, the blessing of efficiency which LANs offer can become a curse when attempting to maintain the trade secret status of the information. In view of this, possible legal ramifications need to be assessed before allowing trade secret information to be used on a LAN.

At present, there is no case law which addresses trade secret issues as they apply to information used on a LAN. Therefore, inferences and analogies between the facts of these cases and conditions on a LAN environment must be made in order to predict how courts might rule in this situation. These inferences and analogies should be made and analyzed partly on the basis of opinions of technical commentators regarding LAN security in general.

This article addresses the issues noted above by first discussing LAN technology generally. Some basic concepts of trade secret law are then *298 examined, followed by a discussion of representative case law. Specific precautionary measures particular to LANs are examined in light of this case law. Finally, the above-noted concepts are discussed from a licensing perspective.

Any number of audiences could find value in this article, although it was written with two groups in mind. The first group consists of Corporate and de facto Corporate Counsel who may have a modest technical background. The technical discussions in this article allow members of this group to understand the basics of LAN technology, so that the legal ramifications of using trade secret information on a LAN can be better appreciated.

The second group consists of software developers or owners of proprietary computer-related information who may have little knowledge of trade secret law. The legal discussions in this article allow this group to realize the possible consequences of using their information on a LAN. These legal discussions may also benefit the Corporate and de facto Corporate Counsel if they have had little experience with trade secret law.

While the following discussion focuses on LANs in conjunction with trade secrets, it should be understood that some of the issues addressed have broader implications with regard to electronic communications generally.

INTRODUCTION

Local Area Networks used for sharing and disseminating information such as raw data and computer programs have become an increasingly common sight in today's work place. "LAN sales are expected to rise from 932,000 units in 1990 to 2.6 million in 1994, . . ." [n1] This increasing popularity of LANs [n2] will naturally result in an increase in the amount of information disseminated amongst various types of computers and other devices attached to LANs.

*299 The issue of security of information used on LANs has been a hot topic since their inception [n3] and nearly every commercial LAN system has some form of security. [n4] Nonetheless, security is still a major concern for most organizations that are considering a LAN. [n5] As one commentator observed, " u nless suitable access controls (and possibly data encryption) is imposed upon the LAN environment, serious problems with industrial espionage may develop." [n6]

Compared to information stored on other computer systems, sensitive information used on LANs is particularly vulnerable largely due to a LAN's ability to disseminate information. As one commentator has noted, "[m]any of the security problems and solutions in the LAN environment parallel those in the minicomputer and mainframe world. The LAN adds to these some unique problems of its own. The most formidable challenge is the way LANs distribute information." [n7]

The precise degree of vulnerability of information on a LAN will depend on such factors as the setting in which the LAN is used and on the configuration of the LAN itself. Any vulnerability due to these factors is increased further by the fact that many are unaware or unwilling to acknowledge the full extent to which security problems can exist on a LAN. [n8]

*300 The added security concerns which LANs have introduced have caused some commentators to suggest avoiding using LANs for sensitive information. [n9] However, the obvious convenience and advantages which have made LANs so popular suggest that, as a practical matter, companies will continue to use LANs to distribute all kinds of information, including that which might be considered "sensitive." Where this is the case, the owner of such information should take additional precautions so that the information will not become prey to persons such as disgruntled emplo yees or corporate spies.

The issue of using and disseminating sensitive information becomes more complex if this information is considered a trade secret. One of the factors courts consider in determining if information is a valid trade secret is whether the information was treated as a "secret." More specifically, courts ask whether or not reasonable measures or "reasonable precautions" were taken to protect the secrecy of the information. If a court finds that reasonable precautions were not taken, then it will find that no trade secret exists. [n10] If no trade secret exists, an alleged trade secret owner cannot collect damages for misappropriation of the information. [n11]

Since reasonable precautions must be taken to maintain the secrecy of a trade secret and since LANs can create a vulnerable environment for sensitive information, an unsuspecting trade secret owner could unwittingly allow information to be used on a LAN in a way that might be considered inconsistent with maintaining reasonable precautions. Thus, before trade secret information is used on a particular LAN, the potential legal consequences must be assessed. Such an assessment must take into account the configuration and type of devices attached to the LAN, who will have access to the trade secret information and the physical security measures in place to protect the LAN. In addition, where it is anticipated that trade secret information will be licensed to another, the owner of the trade secret needs to make sure that the licensee maintains reasonable precautions in its treatment of the licensed trade secret information.

*301 I. LAN Technology

A local area network typically consists of two or more computers usually linked together by metal or fiber optic cables [n12] so that information can be shared between computers. LANs also typically allow resources such as printers or modems to be shared among the computers attached to the LAN. [n13] This sharing of information and resources avoids duplication of such items, while enhancing access speed and integrity of information.

The information used within a LAN can consist of computer programs or data. For the purposes of this discussion, a computer program refers to executable information which is actually used to directly control the Central Processing Unit of a computer. [n14] Any information which is not a computer program is considered data. [n15]

While the word "local" in "local area network" seems to suggest a very geographically limited network of computers, the definition of this term is subject to much interpretation. One commentator has observed that "[a] local area network must be local in geographic scope, although the term 'local' might mean anything from a single office or a large building to a multi-building educational or industrial campus." [n16] Thus, by some definitions, a "LAN" could be spread out over a large area. In any event, LANs are to be distinguished from wide area networks (WANs). A WAN typically consists of large, often widely spread out computers (or "nodes") such as mainframes, which are interconnected. Processing control of the WAN is centralized in each of these nodes. [n17]

A LAN can be configured so that one or more of its constituent computers are dedicated solely to storing and distributing information for *302 the remaining computers. Such dedicated computers are referred to as servers. [n18] The remaining computers (referred to as workstations) are able to send and receive information to and from a server. This type of LAN configuration is referred to as server-based.

Alternatively, LANs can be configured so that all of the computers which compose the LAN are peers. This type of LAN is often referred to as a peer- based LAN. These LANs enable the computers composing the LAN to send and receive information to and from each other, thus making each computer both a potential server and workstation. For the sake of simplicity, computers composing a peer-based LAN will be referred to as workstations in this discussion.

While microcomputers (also known as personal computers) are frequently the type of computer used on a LAN, [n19] LANs can also comprise other, larger types of computers as well. [n20] The ability to use a variety of different types of computers on a single LAN gives it a flexibility not found in homogeneous computer systems.

A LAN operating system (that is, the computer program which allows the LAN to function as a LAN) typically allows a workstation to logically access a server's permanent storage devices (e.g., hard disks, optical disks, etc.) and peripheral devices (e.g., printers, modems, etc.) as though those resources were physically a part of the workstation itself. When a user on a workstation executes a computer program or requests data residing on a server, that computer program or data is actually copied from some permanent storage device of the server and is "loaded" into what is called the main memory or random access memory (RAM) of *303 the workstation. [n21] In this way, the workstation has an actual copy of that computer program or data at its disposal. This aspect is one of the important distinctions between LANs and other multi-user computer systems such as mainframes.

A workstation's ability to store and process information, coupled with the general ability of a LAN to disseminate information among various devices, gives the LAN some distinctive advantages over other types of computer environments. [n22] However, these advantages may create some disadvantages when it comes to computer security. For example, the fact that a computer program and data can be loaded into the

RAM of the workstation means that this information can be copied more easily onto a permanent storage device within the workstation and removed therefrom. Also, the fact that many LANs use information access methods allowing information destined for one workstation to potentially be "listened to" by some or all other workstations can make it easier for an unauthorized person to access sensitive information. [n23]

In addition to allowing for the dissemination of information among the various components of a LAN, LANs can by accessed by remote workstations or other devices over telephone lines through the use of modems. Further, individual LANs can be interconnected by direct wiring or over telephone lines. Where two LANsof the same or similar technology (i.e., communications protocol) are connected together, the connection mechanism is generally known as a bridge; where two LANs of different architectures are connected together, the connection mechanism is generally known as a gateway. [n24] Such mechanisms *304 increase the communication and information disseminating potential of LAN technology, but they also can heighten the security risk to information used on a LAN.

In addition to the use of bridges and gateways, the trend toward standardization of LAN protocols will result in greater harmonization of communications, or "connectivity." [n25] In the late 1970's, the International Standards Organization (ISO) published a model for Open Systems Interconnection (OSI). The goal of this model was to increase the ease with which different vendors' devices can be interconnected to each other via such means as bridges or gateways. [n26]

Although total connectivity among the LAN devices of various vendors may not presently exist, OSI has already been used as a basis for the development of some widely-used protocols. [n27] Also, other widely-used protocols have developed independently of OSI. [n28] The emergence of these protocols will serve to further increase the information dissemination potential of LANs.

For all the reasons indicated above, more and more information will be transmitted between various LAN-related devices. While enhanced LAN communication will benefit the computer industry in many ways, it will also increase the potential for unauthorized access of information. [n29] The implications of this information being considered a trade secret are discussed below.

*305 II. Trade Secret Law

To understand the legal ramifications of using trade secret information on a LAN, one must first understand what a trade secret is and how it must be maintained. Also, one should understand the scope of trade secret protection in comparison with other forms of intellectual property protection. An understanding of these topics can assist the owner of trade secret information in avoiding pitfalls which could otherwise lead to forfeiture of the trade secret. In addition, it can also assist the owner in benefiting fully from the advantages that trade secret protection can offer. A brief comparison of trade secrets with other forms of intellectual property is discussed first below.

Trade secret protection has traditionally been an important method for protecting information such as software-related information. [n30] Copyright and, more recently, patent protection are also now used to protect software-related information. [n31] Although copyright and patent protection have some significant advantages over trade secret protection, [n32] trade secret protection has the advantage that, by definition, the information is not known to the public. Other advantages of trade secret protection include the broader scope of subject matter that can be *306 protected [n33] and the unlimited duration of that protection. The duration of a utility patent is 17 years (see 35 U.S.C. Section 154). [n34]

Maintaining information as a trade secret does not preclude the use of other forms of intellectual property protection. For example, copyright and trade secret protection are compatible. [n35] In contrast, patent protection and trade secret protection are mutually exclusive. [n36] However, in situations where secrecy can be given up for broader protection and where the trade secret information is patentable, [n37] then patent protection should be a serious consideration. [n38]

*307 Regarding the definition of a trade secret, it is first noted that trade secret law is derived from common law, and governed by the individual states. This is unlike patent and copyright protection which are both governed by Federal laws. [n39]

At present, most states provide laws modeled in accordance with either the Restatement of Torts (Restatement) [n40] or the Uniform Trade Secrets Act (UTSA). [n41] Both of these "models" are only proposals for states (in the case of the UTSA) [n42] or for the courts themselves (in the case of the Restatement) to adopt at their discretion. The UTSA is the newer of these two similar [n43] models and has been gaining in popularity. At the time of this writing, the UTSA has been ratified by 33 states. [n44]

When litigation centers around a trade secret, two related issues are typically analyzed. The first is whether a trade secret exists (that is, whether the subject matter constitutes a valid trade secret). The second is whether the trade secret has been misappropriated (that is, improperly *308 procured). The concept of the "existence" of a trade secret is analogous to the concepts of validity and copyrightability in patent and copyright law, respectively. The concept of misappropriation is analogous to the concepts of patent and copyright infringement.

Regarding the first issue of whether a trade secret exists, there are several circumstantial factors relating to the subject matter which must be present for it to be considered a trade secret. These factors are derived from portions of the Restatement and the UTSA. They include the type of subject matter at issue, [n45] whether the owner derives economic value from its maintained secrecy [n46] and whether the subject matter is readily ascertainable (that is, whether it really is a secret and not in the public domain). [n47] While these factors are part of what characterizes a trade secret, defining a trade secret precisely is difficult. [n48]

An additional factor related to the concept of "secrecy" has particular relevance to information used on a LAN. This factor is that the information must be the subject of ongoing efforts to maintain secrecy. In other words, "reasonable efforts" or "reasonable precautions" must continually *309 be taken to ensure that the subject matter remains a secret. If reasonable precautions are not taken, then, according to both the Restatement and the UTSA, the subject matter is not a "trade secret." [n49] This proposition is followed by the courts. [n50] Thus, maintaining a trade secret hinges in part on how the subject matter is continually treated.

The requirement of maintaining "reasonable precautions" is particularly relevant to trade secret information used on LANs, largely because of the dissemination capabilities of these devices. These dissemination capabilities may place such information used on a LAN in a particularly vulnerable position. This then raises a question as to whether trade secret information used on a LAN runs counter to the requirement of maintaining reasonable precautions. If the answer to this question is "yes," then the consequences will affect the above-noted second issue of "misappropriation."

Misappropriation of a trade secret involves the ability to obtain remedies against a wrongdoer for stealing or "misappropriating" the trade secret. [n51] A finding of misappropriation is determined based upon *310 whether the trade secret was procured by "improper means," [n52] or whether there was some "duty" not to disclose the trade secret. [n53] It is this ability to obtain remedies based upon misappropriation that makes trade secret protection of any worth.

Under both the Restatement and the UTSA, a finding of misappropriation pre-supposes that a trade secret exists. [n54] Thus, if any of the above-noted factors which define a trade secret are not present, then there can be no misappropriation (since there is no trade secret). [n55] For example, where reasonable precautions are not taken to protect the secrecy of information used on a LAN, then there can be no misappropriation. Where there is no misappropriation, there are no available remedies stemming from trade secret protection.

One can now understand why it is important for owners of trade secret information used on a LAN to take reasonable precautions to keep their information secret. However, a question remains regarding how much "precaution" is considered "reasonable." Another question is whether the specific characteristics of a LAN affect the amount and types of precautions that are necessary. These questions are addressed below.

*311 III. The Relationship Between Reasonable Precautions and Trade Secret Information Used On A LAN

Courts have generally followed the principle that taking "reasonable precautions" to maintain the secrecy of trade secret information does not entail doing everything possible to safeguard the information. This is illustrated by the celebrated case of E.I. Dupont De Nemours & Co. v. Christopher. [n56] In this case, the defendants were hired to take aerial photographs of a DuPont manufacturing facility which was under construction and which did not yet have a roof. In discussing the issue of precautions required to protect the trade secrets within the facility, the court stated that "perhaps ordinary fences and roofs must be built to shut incursive eyes, but we need not require the discoverer of a trade secret to guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available." [n57]

Rather than require absolute secrecy and extensive precautionary measures, the practice generally followed is that reasonable precautions under the circumstances must be maintained. [n58] Under circumstances where trade secret information is in a relatively vulnerable position, additional precautions may be required. Such circumstances might include those where there is evidence of espionage in the industry or where improper access to information is a common occurrence. [n59]

*312 Technical commentators have indicated that LANs create a relatively vulnerable environment, [n60] especially when compared to other types of computer systems such as mainframes. [n61] Much of this vulnerability is due to the general dissemination abilities of LANs and to the relatively young and undeveloped state of the LAN industry as compared with other computer environments. [n62] In addition, persons accustomed to using detached stand-alone microcomputers are often unaware of LAN security issues [n63] and/or they resist controls over their computers that LANs impose. [n64] Also, allowing remote access to a LAN adds additional levels of vulnerability. [n65]

*313 As indicated above, the amount of reasonable precautions needed to protect trade secret information depends upon the surrounding circumstances. By using trade secret information on a LAN, this information is arguably placed in a vulnerable environment in which a higher level of precautions would likely by required. Since technical commentators have indicated reasons why information used on a LAN may be unsecure, it is also arguable that unauthorized access to this information would not be considered "unanticipated, undetectable, or unpreventable," as per the situation in DuPont. This then raises the question of what specific precautions might be considered "reasonable" to protect trade secret information on a LAN?

At present, there is no case law where the issue of reasonable precautions and information used on LANs is discussed. Therefore, any prediction regarding the amount and type of specific precautions that would be required has to be accomplished by interpolation. This is done in the following section by examining existing court decisions addressing issues pertaining to reasonable precautions generally. Analogies are then made between the factors the courts use to determine whether reasonable precautions were taken and conditions which may exist on a LAN.

The analogies made between existing case law and conditions on a LAN are supported by statements from technical commentators. These statements are indicative of what the LAN community believes is necessary (from a technical perspective) to protect information used on LANs. Since courts would be likely to take recommendations from technical commentators into account, the following analogies, which consider the statements of these commentators, may provide insight into what courts would consider reasonable precautions.

The issues (denoted as "themes" below) that courts discuss regarding reasonable precautions vary somewhat from case to case and from jurisdiction to jurisdiction. However, there appear to be several (somewhat overlapping) themes which are frequently mentioned. These themes can be broken down into two general groups: physical protection [n66] and notice. [n67] Themes which relate to physical protection include whether the location (or at least the immediate area) where the trade secret is kept is secure, whether the trade secret is locked up and *314 to what extent the trade secret is permitted to disseminate among employees and outside persons.

Themes relating to notice include whether confidentiality agreements were signed or policy statements were distributed and whether markings were placed on the trade secret itself indicative of the secret status of the information. [n68] While courts have indicated that factors concerning any one of the above-noted themes may not affect a finding of reasonable precautions, factors relating to a combination of these themes can be decisive. [n69]

These themes as they specifically relate to trade secret information used on a LAN are discussed below.

IV. Physical Protection of the Trade Secret

A. General Security Of The Area Of The Trade Secret

The first theme concerning physical protection as a means for taking reasonable precautions addresses whether the area in which a trade secret is used is sufficiently secure. The case of Electro-Craft Corp. v. Controlled Motion, Inc. [n70] is illustrative of this theme. In this case, plaintiff Electro-Craft Corporation (ECC) accused defendant Controlled Motion Inc. (CMI) of misappropriating ECC's trade secrets concerning the manufacture of servo motors for computer disk drives. The evidence indicated that a servo motor manufactured by CMI had nearly identical dimensions and tolerances to that of an ECC motor. In discussing the security of the area surrounding the trade secret, the court indicated that ECC did not take appropriate measures to secure the area in which the trade secret was used. [n71] In one example, the court noted that "many informal tours were given to vendors and customers without warnings *315 as to confidential information." [n72] Although the court appeared to indicate that ECC's placement of "authorized personnel" signs in various locations was a step toward taking reasonable precautions, [n73] it was nonetheless insufficient by itself to convince the court that reasonable precautions had been taken.

Another court decision illustrating this theme is Wilson Certified Foods, Inc. v. Fairbury Food Products, Inc. [n74] In this decision, the defendant was accused of misappropriation of the plaintiff's process of manufacturing cooked bacon particles (known as Bits-O-Bacon). The plaintiff had asserted that this process was a trade secret. According to the plaintiff, the president of the defendant corporation (a former employee of the plaintiff) applied his knowledge of the plaintiff's process in his work at the defendant corporation and thereby unlawfully appropriated the plaintiff's trade secrets. [n75] In finding that the plaintiff did not take reasonable precautions to protect its alleged trade secret, the court determined that the general area surrounding the trade secret was not protected by adequate security measures. [n76] For example, the court noted that the " s igns on the floor where Bits-O-Bacon was produced restricting access to the Bits-O-Bacon production area were maintained with great irregularity." [n77] While the court did take notice that plaintiff's manufacturing plant had a general security system where non-employees were questioned as to their motives for visiting and were subsequently issued passes, the court nonetheless found that "these measures constitute nothing more than general plant security of a type which is often present in manufacturing operations." [n78]

*316 The cases discussed above illustrate that the degree of security surrounding the area in which a trade secret is used is a factor considered by courts in determining whether reasonable precautions were taken. Although these cases do not relate to LANs directly, analogies can be made between the area security as discussed by the courts and the conditions which may exist on a LAN. In addition, comments from technical commentators regarding the conditions necessary to maintain LAN security can be used to support these analogies. Analysis of these comments is valuable, since such comments are likely to be considered by courts when determining whether reasonable precautions were taken to protect trade secret information used on a LAN.

In general, commentators indicate that the area surrounding a trade secret should be more heavily protected than those areas where there are no trade secrets. [n79] The "surrounding area" of a LAN can be defined as the area around its various components. These components include printers, workstations and the devices that are used to connect these components to each other. Permanent storage facilities for the information (e.g., file servers) are also components of the LAN [n80] which define its "surrounding area."

Technical commentators have indicated that attention to physical protection surrounding the various components of a LAN is important and that security around these components is needed. [n81] Consequently, the *317 area around these components should (where possible) be considered "restricted." Security measures such as guards and/or personnel badges are one means for enforcing these restrictions.

Card-key mechanisms are another means for maintaining security around a given area. These mechanisms can be used to indicate who has entered the area and when. [n82] Additionally, audit trails on the LAN itself can be maintained and used in the same manner. These issues will be discussed further with regard to licensing considerations below.

Workstations are the portals through which access to information on the LAN can be gained and their distribution is instrumental in defining the "area" in which the LAN exists. Since they can be placed in any number of locations, an attempt should be made to ensure security in those locations. [n83] Methods for doing this might include limiting access to trade secret information only to certain workstations [n84] within a restricted area. Visitors to this restricted area should be kept to a minimum [n85] and those that are allowed to enter should be kept under close employee supervision. [n86]

*318 One method to help ensure that security procedures are followed generally and to show that reasonable precautions were taken to protect the trade secret information is to assign one or more persons the duty of implementing and maintaining security procedures throughout the LAN environment. In many companies, one or more "LAN managers" are hired in part to enforce LAN security. Some commentators have indicated that the role of such LAN managers in maintaining security should not be underestimated. [n87]

Protecting the area around file servers is crucial [n88] and is less complicated where the configuration of the LAN is server-based. However, if peer-based LANs are used or where workstations are widely disseminated, it may be very difficult to protect the area around the LAN with locks and badges. [n89] In situations which may make it difficult to implement meaningful security procedures around the "area" of the LAN, other types of physical protection should be emphasized. These other types of physical protection are discussed below.

B. Locking Of The Trade Secret

Another theme concerning physical protection is whether the trade secret itself was kept "locked up." Many cases indicate that this theme is taken into account by courts in determining if reasonable precautions have been taken.

One court decision illustrating this theme is Defiance Button Machine Company v. C&C Metal Products Corp.[n90] In this decision, the plaintiff had sold the defendant several of its assets. These assets as "listed" on the sale sheet included a computer, but did not include any computer programs or data. During the defendant's removal of the "listed" assets from the plaintiff's computer room, a representative of the defendant asked a computer operator formerly employed by the plaintiff to *319 demonstrate the operation of the computer. While demonstrating the computer, the computer operator discovered that a copy of the plaintiff's customer list had been left in the computer's memory. In addition, the code word enabling the computer to print the customer list was found in source books located in the plaintiff's computer room.

From this evidence, the court stated:

[plaintiff] did not take adequate measures to ensure the secrecy of the lists. Hence, even though [defendant] may have obtained the lists by improper means -- paying [the former computer operator] to extract the information from the computer -- any such impropriety does not create liability for use of a trade secret, since by failing to protect the lists from ready access by [defendant] independent of [the computer operator's] assistance, [plaintiff] has forfeited the protections of trade secret law. [n91]

Thus, by not keeping the trade secret information adequately "locked" and inaccessible to unauthorized persons, the court held that the plaintiff's information could not properly be deemed a trade secret. This was so held even though the trade secret had been obtained by "improper means."

Other cases also emphasize the importance of keeping trade secrets locked up. In Electro-Craft, the court noted that the plaintiff's "documents such as motor drawings were not kept in a central or locked location, . . ." [n92] Similarly, in Wilson, the court found that "a copy of the plant operating instructions for the Bits-O-Bacon operation was kept unlocked in a former employee's desk, and access to his office was not restricted." [n93]

The above cases demonstrate that keeping trade secret information locked up is a factor considered by courts in determining whether reasonable precautions have been taken. Neglecting this factor consequently can contribute to the demise of a trade secret. This appears true even where the trade secret was acquired by improper means, as the Defiance case demonstrates.

A difficulty in applying this theme to LANs is that trade secret information used on a LAN inherently does not lend itself to being put into a safe and locked up. This is because information used on a LAN is electronically accessible to the various devices comprising the LAN. However, technical commentators have indicated that there are ways of keeping this information "locked" that are somewhat analogous to the idea of "locking" information in a more traditional sense.

*320 One way of locking trade secret information used on a LAN is to lock that information at the source. For example, rooms containing the permanent storage devices (usually file servers) upon which the trade secret information resides, as well as printer rooms [n94] where trade secret information is printed, should be kept locked. [n95] Where peer-based LANs are used rather than more centralized server-based configurations, security becomes more difficult, since all of the workstations containing trade secret information need to be locked. [n96]

Of course, when trade secret information is used on a LAN, the cables connecting servers (and other devices) to workstations in effect act as "holes" through which the information leaks. To effectively "lock up" the trade secret information, unauthorized access to these "holes" needs to be prevented. "The most popular technique to prevent unauthorized access to information is password security, which forces users to enter unique identification codes before they can access shared data." [n97]

Password protection usually consists of two components: a personal identification token (to identify the user) and a personal authentication token (to validate the identity of the user). [n98] Password protection can be used to protect varying amounts of information, from specific pieces *321 of information to access to the LAN generally. [n99] Some courts have specifically acknowledged that the use of passwords (in conjunction with other precautionary measures) is a means for taking reasonable precautions. [n100] However, technical commentators warn us not to place too much faith in password protection alone. [n101]

Although present password schemes generally require a user to enter an alpha-numeric code from a keyboard, other types of identification means are gaining acceptance. They include the use of "hand geometry, fingerprint and eye retina pattern readers, signature verification and voiceprint recognition." [n102]

Other steps toward locking trade secret information which may be seen as taking reasonable precautions include the utilization of automatic log-off facilities when workstations have been left unattended. [n103] Also, a user should not be permitted to enter too many invalid passwords. [n104] *322 In addition, the keyboards to the workstations themselves should be locked when not in use. [n105] Implementation of these precautions would serve to inhibit an unauthorized intruder from gaining access to trade secret information and also may serve as evidence that reasonable precautions were taken.

C. Dissemination of the trade secret

In addition to 1) securing the area of the trade secret information and 2) keeping the trade secret "locked up," a third theme courts often consider concerning physical protection relates to dissemination of the trade secret. Courts have indicated that a lackadaisical approach to distribution and dissemination of a trade secret is an indication that reasonable precautions have not been taken to protect the trade secret.

For example, in Wilson, the court found that " . . . a general description of the manufacturing process was distributed to Wilson's sales brokers." [n106] In Electro-Craft, the court noted that "discarded drawings and plans for motors were simply thrown away, not destroyed." [n107] These findings contributed to the courts' decisions that reasonable precautions had not been taken.

In Surgidev Corporation v. Eye Technology Inc., [n108] the court discussed steps it believed the trade secret owner (plaintiff) had taken toward inhibiting dissemination of the trade secret. In holding that reasonable precautions had been taken by the plaintiff, the court stated that the plaintiff had made efforts to promote "distribution of allegedly secret materials on strictly a 'need-to-know' basis," [n109] and "to separate sensitive departments or processes from the central facility" [n110] This case, as well as Electro-Craft and Wilson, indicate that the control of dissemination of a trade secret is a factor courts may use to determine if reasonable precautions were taken.

The issue of dissemination of trade secrets is particularly pertinent to LANs, since the very purpose of a LAN is to disseminate information. The potential dissemination of information used on a LAN can be very widespread, depending upon its configuration. Moreover, dissemination can increase greatly when access to information on a LAN is *323 permitted via remote devices. If trade secret information is allowed to disseminate too freely, a court may find that reasonable precautions were not properly taken.

The holding in Surgidev indicates that trade secrets should be limited, where possible, to distribution on a need-to-know basis. From a technical perspective, one commentator has stated that, with regard to LANs, "users should receive access only to files and services they need for their work." [n111] Since a court is likely to take such comments into account, these comments can only serve to increase the weight that a court will give to factors relating to dissemination of information.

In addition to advising that trade secret information should be used on a need-to-know basis, technical commentators have also indicated that allowing "dial-in" devices, such as modems, to be attached to a LAN can make information on the LAN more vulnerable. [n112] While methods exist which can make modem access to a LAN more secure, [n113] attachment of modems can still decrease the overall security of information used on a LAN. [n114] Thus, where possible, a LAN should remain truly "local" by having no modems attached. Technical commentators have also suggested that, for similar reasons, the attachment of bridges and gateways to the LAN should also be avoided. [n115]

*324 Although it may be optimal from a security perspective not to attach the above-mentioned devices to a LAN, business considerations may nonetheless require their attachment. In these situations, monitoring the information passing through these devices may provide some protection. However, it is often difficult to identify who is accessing the information. [n116]

One solution to this problem may be to install some mechanism which will prohibit trade secret information from passing through a remote device. In this way, a user who normally can access trade secret information via a workstation directly attached to the LAN would not be able to access that same information through a remote device. A possible method for implementing this is to encode all trade secret information with some identifying mark which indicates that the information is a trade secret. The remote device could then be set up to prohibit the passage of any information containing the identifying mark.

The use of remote devices is not the only way in which information can be disseminated to the detriment of a trade secret. Printers, for example, can disseminate information in ways which may not be consistent with taking reasonable precautions. This is because printers make it easy to produce multiple copies of trade secret information, all of which may not be properly accounted for or destroyed when the user is finished with them. If printed copies of trade secret information are carelessly thrown away, a situation similar to that discussed above in Electro-craft could occur. As a result, in the realm of computerized information (such as that used on a LAN), printers may replace the photocopy machine as the traditional "enemy" of trade secrets. [n117]

In view of the potential effect of printers on the dissemination of sensitive information, technical commentators advise taking special precautions when printing sensitive information. These precautions include allowing sensitive information to be printed only on designated printers [n118] and monitoring those printers. [n119] In addition, a password can *325 be required to print trade secret information. Also, a document destruction policy should be implemented. [n120] These precautions would inhibit dissemination and theft of the trade secret information, as well as potentially show that reasonable precautions were taken.

Another problem regarding the dissemination of trade secret information used on a LAN concerns the fact that workstations are typically self-contained computers having removable storage devices. This makes it possible for a user at a LAN workstation to access trade secret information from a server, copy that information to a removable storage device (such as a floppy disk) on the workstation and then walk away with the storage device and the trade secret information. [n121] Thus, the fact that workstations have their own storage devices makes them a potential information dissemination problem.

To alleviate possible dissemination problems facilitated by removable storage devices, "diskless" workstations can be used. [n122] Diskless workstations are usually self-contained computers, but without any type of permanent storage facilities. [n123] In this way, users can take advantage of *326 the facilities of a LAN without having the ability to copy and remove valuable trade secret information.

In many situations, it may be desirable for the workstations to contain local storage facilities, yet equally desirable to maintain the kind of security that diskless workstations can afford. One possible solution is to provide a mechanism which automatically encrypts any information which is written to the local storage facility. When the information is read back from the local storage facility, it is automatically decrypted. In that way, information can be saved locally, but can only be used by systems that can decrypt the information.

With the advent of wireless LANs (which use some form of radio frequency or infra-red technology to send information to and from various devices on the LAN), some concern has been raised regarding the degree of security that they provide. [n124] Where spread-spectrum technology [n125] is used, however, many consider wireless LANs to be more secure than LANs using conventional wire cables. [n126] Thus, using wireless LANs may actually be a means to show that reasonable precautions were taken to protect the trade secret information.

The cables that are used to connect the devices comprising a LAN may themselves be a source of dissemination which can detrimentally expose trade secret information. [n127] This is partly because conventional copper cables emit radio waves. Information passing through the cables can be re- created by capturing these radio waves. Also, these cables can be tapped into directly. Solutions to this problem include the use of *327 "shielded" cable, [n128] or the use of fiber optic cable (which emits no interceptible radio waves [n129] and is difficult to tap into [n130]

Compounding the problem of unauthorized access via cables is the fact that many LANs use information access methods which effectively broadcast information to some or all workstations on the LAN. This occurs even though the information may be sent from one workstation for receipt by only one other workstation. [n131] Security protocols are currently being developed to alleviate this problem. [n132] Use of these protocols would help prevent an intruder from accessing the information via cables or another workstation.

In addition to the cables, the workstations themselves can generate radio waves which can be interpreted from a distance. [n133] If the workstations are spread out in many locations (and near the outside of a building), the chances of capturing the radio waves is greater. However, radiation shields can be placed around workstations so that these radio waves will not be emitted. [n134] Such precautions may be warranted, depending upon the "surrounding circumstances."

Encryption has become an important method for protecting sensitive information from falling into the hands of unauthorized persons. [n135] In addition to its value for local storage, as discussed, the use of encryption *328 can encompass anything from encrypting passwords [n136] or select transmissions to encrypting all transmissions within a LAN. [n137] Encryption of trade secret information is particularly important when the trade secret information is transmitted over telecommunications lines. [n138] In any event, the use of encryption could be used as evidence that reasonable precautions were taken to protect the trade secret information used on a LAN.

V. Notice Requirement

In addition to themes concerning physical protection, courts consider whether reasonable precautions were taken to put persons "on notice" of the existence of trade secret information. This is particularly pertinent to trade secret information used on LANs due to the relative vulnerability of LANs and the information dissemination capabilities that they possess. As a result, special efforts should be made to put persons on notice of the existence of trade secret information used on a LAN.

Two themes addressing this issue are discussed below. The first theme is whether those who have access to the trade secret are aware of its secret status in view of signed confidentially agreements [n139] and/or corporate policy statements. The second theme is whether the trade secret itself was marked as a trade secret in some way.

Courts typically examine factors relating to these themes when considering the question of whether persons had adequate notice that the information was considered a secret. The answer to this question can then be used to help answer the broader question of whether reasonable *329 precautions were taken to protect the secrecy of the information. Again, while there are no cases on point concerning LANs, an idea of what a court may find as constituting adequate notice can be interpolated from existing case law, as was done above for issues concerning physical protection.

A. Signed agreements and notification of trade secrets

Courts have held that the use of signed agreements and other forms of notification of a trade secret's existence (aside from actually marking the information as a trade secret) can be evidence that reasonable precautions were taken to protect a trade secret. However, any such form of notification must identify with some specificity that which is considered secret. Some of these court decisions concerning this issue are examined below.

In Electro-Craft, the fact that the plaintiff neglected to notify persons of the specific subject matter considered to be secret contributed to the court's determination that reasonable precautions were not taken. Specifically, the court stated that "ECC's efforts were especially inadequate because of the nonintuitive nature of ECC's claimed secrets here. The dimensions, etc. of ECC's motors are not trade secrets in as obvious a way as a 'secret formula' might be . . . . ECC never issued a policy statement outlining what it considered to be secret." [n140] Thus, the precise nature of what ECC considered to be its trade secrets was never disclosed to its employees.

Similarly, the Wilson court found that two relevant agreements signed by the defendant did not specifically mention what information was considered a trade secret. In addition, the court decided that the two agreements were of a type signed by employees generally and not just by those privy to the trade secret information. Specifically, the court stated that "neither agreement mentions the Bits-o-Bacon process in any respect, and it is undisputed that forms of this type were signed by untold numbers of Wilson employees over the years, most of whom were never involved in the Bits-o-Bacon operation." [n141]

The Electro-Craft and Wilson cases indicate that persons having access to trade secret information should be notified as to precisely what information is considered a trade secret. Generic forms which broadly indicate that confidential information may not be disclosed appear insufficient to show that reasonable precautions were taken. In addition, *330 generic forms which indicate that virtually everything in the corporation is to be considered "confidential" may be considered overreaching and may be deemed null and void by a court as an unreasonable restraint on the mobility of an employee. [n142]

Some cases where courts have upheld the existence of trade secrets indicate that the trade secret itself was clearly identified to those who had access to it. For example, in Cybertek Computer Products, Inc. v. Whitfield, [n143] the plaintiff asserted that its "auto/issue" computer system was a trade secret. In upholding the computer system as a trade secret, the court noted that the nondisclosure agreement signed by the defendant "specifically made reference to the auto/issue system" [n144] as a trade secret.

In J&K Computer Systems, Inc. v. Parrish, [n145] the court adopted a somewhat broader view than that of the Cybertek court, finding that reasonable precautions were taken partly because of the plaintiff's use of an employee contract. Specifically, the contract stated that "the methods and programs used in conducting the employer's business are valuable, special and unique assets of the employer's business." [n146] Although the agreement only mentioned "programs" generally, this was specific enough for at least this court. The broad scope of this employee contract should be viewed as a minimum standard of specificity, however. It would be prudent, in view of other court decisions, to provide greater specificity in identifying the subject matter which is considered secret.

From the above-noted cases, it can be appreciated that those persons that are using trade secret information on a LAN (be they employee *331 or contractor [n147]) should sign some type of confidentiality agreement or contract indicating the existence of the trade secret information. [n148] These confidentiality agreements should identify the specific information considered a secret and should vary depending upon the type of information used by a particular employee. [n149] In addition to confidentiality agreements, general policy statements should also be issued to each employee to identify the subject matter considered to be a trade secret. [n150]

In a LAN environment, users of trade secret information could potentially be spread out over a department, a building or even the world, if modems or the like are attached to the LAN. Thus, it is difficult, yet important, to make these users aware of company policy concerning the scope, as well as the treatment, of trade secret information. [n151] This can be done by electronically posting company policies via the LANs, particularly to those persons using the trade secret information. In addition, when access to trade secret information is first given to users, it is important to make sure that all of these users (wherever they are) *332 are identified and sign a confidentiality agreement indicating their awareness of the trade secret status of the specific information. [n152]

One way to ensure that persons using trade secret information on a LAN sign the proper confidentiality agreements is to require that they sign interactively. This can be done by providing workstations with light pens or digitizing pads to allow the user to interact directly with the computer screen or pad. [n153] When users (using their specific personal identification token) access trade secret information for the first time, a computer program can request that they sign their name on the screen or pad before being allowed access the trade secret information. This digitized signature can be recorded and used to show that the signer was on notice of the trade secret status of the information. [n154]

Another problem with putting persons on "notice" concerns keeping track of all trade secret information accessible on the LAN. Since LANs allow users to place information on the LAN for access by other users, [n155] a user can potentially place trade secret information on the LAN so that it is easily accessible by unauthorized sources. Where the LAN is interconnected to other devices via modems, gateways, etc, an even greater potential for dissemination of the information can occur.

In addition to the dissemination problems caused by allowing users to place information on a LAN, the specific information available to users via the LAN is often unknown to the trade secret owner. This, in turn, makes it difficult for a trade secret owner to determine the scope of the confidentiality agreements that employees should sign. Thus, mechanisms for monitoring information made accessible to other users should be implemented and policy statements prohibiting free access to certain types of information should be distributed.

*333 B. Marking trade secret information

Marking a trade secret to show that it is considered a secret is another theme discussed by courts in determining whether reasonable precautions were taken. In Cybertek, the court noted that the plaintiff had taken steps such as "the marking of documentation relating to its products as confidential, [and] the use of registration numbers in connection with copies of its documentation . . ." [n156] In J&K Computer Systems, the court noted that "the program was marked with the following legend: 'program products proprietary to J&K Computer Systems, Inc. authorized use by license agreement only." [n157]

Conversely, there are cases where reasonable precautions were not found to have been taken, in part because the trade secret was not properly marked. For example, in Electro-Craft the court noted that "None of [ECC's] technical documents were marked 'confidential,' and drawings, dimensions and parts were sent to customers and vendors without special marking." [n158] These decisions thus indicate that marking information as a trade secret is a factor which courts look to in deciding whether reasonable precautions have been taken.

To begin with, documentation and portable physical storage media, such as diskettes, containing trade secret information to be used on a LAN should be marked as "confidential," "proprietary," etc. [n159] In addition, the trade secret information should contain an explicit statement on how the information should be treated. [n160] Regarding trade secret information in the form of computer programs and data, notice of the trade secret should be embedded within the information or actually made to *334 appear when the information is used. [n161] In this way, a user anywhere on the LAN (or connected remotely) will be notified of the trade secret status of the information when it is used.

In addition, printers attached to the LAN which print trade secret information could be made to automatically stamp "confidential" on any printouts of such information. This would not only put persons printing the information on notice, but would also put any third party to which the information was shown on notice as well. Also, the trade secret information could be printed with markings that identify the specific printer used, so that the source of the information can more easily be traced. [n162]

Ensuring that the notice accompanies the trade secret information itself is particularly important in a LAN environment, since access to the information potentially can come from many different sources. If the notice is brought to the user's attention during the use of the information, then the trade secret owner can be assured that all users will be apprised of the trade secret status of the information. Of course, additional reasonable precautions should still be taken as per the other themes discussed above.

VI. Reasonable Precautions And Licensing Of Trade Secrets

In addition to using trade secret information on its own LANs, a trade secret owner may also want to license its trade secret information to others. [n163] General business considerations would typically dictate this decision. In addition to these business considerations, an issue that needs *335 to be addressed is whether licensing this information may adversely affect the trade secret status of the information. More specifically, the trade secret owner should consider whether circumstances surrounding a particular licensing situation might prompt a court to determine that reasonable precautions were not taken. [n164]

In evaluating a particular licensing situation, the owner/licensor should identify specific precautions which the license would need to take to properly protect the trade secret information. The type of precautions needed would depend upon the "surrounding circumstances," as addressed earlier in this discussion. In essence, greater precautions should be required of a licensee where the facilities of the licensee and/or the competitive nature of the industry would render use of the trade secret information by the licensee more vulnerable.

Specific stipulations imposed on a licensee to ensure that reasonable precautions are taken should at least include those which the licensor imposes upon itself. [n165] These might include the preparation of confidentiality agreements for employees of the licensee, [n166] in which the exact nature of the trade secret subject matter is defined. [n167] Such stipulations are particularly important where the employees of the licensee are widely disbursed and where the precise amount and type of trade secret information accessible to the employees may otherwise be difficult to determine. In any event, imposing such stipulations on a licensee not only serves to maintain the secrecy of the information, but also may *336 serve as evidence that the licensor took reasonable precautions to protect its trade secrets. [n168]

In addition to those precautions which the licensor has implemented at its own facilities, a licensee may need to take additional precautions to properly protect the trade secret information due to the licensor's lack of direct control and supervision over the licensee. Because the licensor typically does not oversee the day-to-day operations of the licensee, it would be prudent to impose stipulations which compensate for this fact. For example, a licensor might consider requiring a licensee to use diskless workstations. Since the licensor cannot easily monitor the activities of the licensee's employees, use of diskless workstations would inherently inhibit attempts of theft of trade secret information.

Other precautionary measures which compensate for a licensor's lack of direct control include the use of mechanisms which generate audit trails. These mechanisms can generate a log of who accessed the LAN, when, from where, and what specific information was accessed. [n169] In addition, they can be used in conjunction with card-key mechanisms, [n170] so that a log of who entered the area where workstations and/or servers reside can also be maintained. By compelling the licensee to use mechanisms which generate these logs, a licensor can maintain some supervision over its trade secret information and ensure that the licensee (and, in effect, the licensor) is taking reasonable precautions to protect the information.

Site inspection of a licensee's premises can be used to ensure that a licensee is complying with the stipulations in the license agreement. A site inspection could include inspection of the areas where trade secret information is being used, as well as inspection of components of the LAN itself. This would help ensure that the licensee is conforming to all stipulations of the license agreement. Both site inspections and the use of audit trails should be carefully documented for use as evidence that reasonable precautions were taken.

*337 Reasonable precautions regarding trade secrets should also be taken into account when determining what type of license agreement to enter into. In general, licensing relating to LANs falls into three major categories: 1) Site licensing: a network version of single -- user agreements allowing unlimited copies of information at a specific location, 2) Server -- based licensing: users on a single network server all have access to the information, 3) Per-user agreements: a limited number of users access the information at a given time. [n171]

A site license typically allows the licensee to use the licensed information anywhere within some defined site. Depending upon the definition of "site" and the security taken around the site, this type of license agreement could potentially allow the trade secret information to disseminate into unprotected areas. Thus, where this type of license is used, the licensor should be sure that the entire site in which the trade secret information may be used is secure.

Server-based licensing typically provides for a more limited dissemination-potential for trade secret information. However, the ultimate determination of reasonable precautions will depend in part on what is attached to the server. For example, where modems, bridges and/or gateways are attached to the LAN, then a single server can still be accessed by a multitude of workstations. Thus, a licensor may want to include a provision in the license agreement in which the licensee is prohibited from attaching modems, bridges or gateways to the LAN on which the licensed trade secret information is being used. As a less stringent alternative, the licensor may insist that mechanisms be installed so that the licensor's information is made inaccessible via these devices.

A per-user agreement would tend to be safest with regard to maintaining reasonable precautions, since only a limited number of users could access the information at any time. In any event, the effect that any of the above- mentioned license agreement schemes would have with regard to reasonable precautions would depend on the degree to which the licensor enforces the agreement.

In general, the issues discussed in this and the previous sections need to be addressed when considering the terms of a license agreement involving the use of trade secret information on a LAN. As a general proposition, the license agreement should be drafted so that the agreement itself could be used to show that reasonable precautions were *338 taken. In addition, inspections of the licensee's operations (using site inspections and/or audit trails) should continue throughout the duration of the license agreement.

CONCLUSION

Using trade secret information on a local area network may conflict with the legal requirement that reasonable precautions be taken to preserve the secrecy of that information. Since there is presently no case law addressing reasonable precautions with respect to LANs, other means were used to predict specific factors a court might consider in determining whether sufficient reasonable precautions were taken. First, existing case law addressing reasonable precautions in general was examined. Then, analogies were drawn between the factors the courts used in their discussions and conditions which may be present on a LAN. Opinions from technical commentators were also examined with respect to how these conditions affect security of information used on a LAN.

In performing the above analysis, it appeared that the courts would most likely take a variety of factors into account. In view of these factors, the owner of trade secret information used on a LAN should try to implement the following:

1. Where possible, keep all the various components of the LAN (and those that can access the LAN) within a secure, restricted area. If this is impractical, then at least

keep the file servers and printers within a restricted area and put extra emphasis on other types of precautionary measures.

2. Keep the trade secret information locked. For example, lock the room containing file servers (and the file servers themselves) and maintain password protection for access to the information.

3. Where possible, LANs should be truly local (that is, no modems, gateways, bridges, etc., should be attached). If this is not practical, access to sensitive information via such remote means should be restricted.

4. Communication links should be protected. Measures such as encryption of information (especially when using devices such as modems, gateways or bridges) and shielding of cables should be taken.

5. Designated printers for printing sensitive information should be chosen and monitored. A destruction policy of redundant or unneeded sensitive documents from these printers should be maintained.

6. Where possible, diskless workstations should be used.

7. All persons using the trade secret information should be put on notice as to what specific information is considered a trade secret. This *339 should be accomplished via signed agreements and/or company policy statements, both of which can be distributed via the LAN itself. Also, the trade secret information should be marked as confidential so that all users of this information on the LAN will observe this notice.

8. If the trade secret information is licensed, the licensor should impose all precautionary measures that it uses itself on the licensee. In addition, site inspections of the licensee's premises should be made and auditing mechanisms should be implemented.

The factors mentioned in this discussion should be considered by trade secret owners before using sensitive information on its own LANs or the LANs of a licensee. Of course, the owner of trade secret information needs to evaluate the amount of precautions desirable from a legal perspective in light of the actual value of the trade secret information. Where this information is highly valuable, it would be unwise to compromise precautionary measures necessary to maintain the trade secret.

[na] B.S. 1985, Emory University; J.D., 1988, The George Washington University. The author is an associate at the law firm of Sterne, Kessler, Goldstein & Fox of Washington, D.C. Copyright (c) 1991 Scott Alter. All rights reserved.

[n1]. Healthy Growth Forecast For Network Industry, PC Week, September 10, 1990, at S51.

[n2]. See, e.g., Smith, F., All in the Family, Business Atlanta, August, 1989, at Section 1, page 76, ("[T]he use of a LAN is increasing in popularity.") See also Stephens, M., It Took Longer Than Anyone Though, But 1990 May Be The Year Of The LAN, Infoworld, January 15, 1990, at 49, 50, stating that the 1990's will be "the decade of the LAN.".

[n3]. See, e.g., Madron, T., Local Area Networks, The Second Generation, 190 (1988), first discussing networks generally, ("Since the inception of computer networks, security has been an often discussed topic . . . . Since one of the primary objectives of a Local Area Network is connectivity, successful implementation of a highly connective system tends to thwart some methods of security and control."

[n4]. See, e.g., King, S., Network Complexity, PC Tech Journal, June 1988, at 44, 52, ("Although all LANs have some security features, many are deficient in this area . . .")

[n5]. See, e.g., Derfler, F., The LAN survival guide, PC Magazine, May 29, 1990, at 97, 99, ("Security is an important consideration for most organizations . . .")

[n6]. Menkus, B., Evaluating the Local Area Network, Modern Office Technology, August, 1989, at 84; See also, Buerger, D., As Networks Pick Up More Novices, Security Suffers, Infoworld, June 13, 1988, at 13 ("LAN security is a growing concern, especially as businesses become more dependent upon networked computer systems.")

[n7]. Krumrey, A., LAN Security, PC Tech Journal, January, 1988, at 96; See also, Korzeniowski, As LANs Multiply, Security Is Debated, Software Magazine, November, 1989, at 85, quoting another commentator discussing security problems concerning dissemination of information on LANs, ("Large corporations are storing confidential memos and creating corporate budgets on microcomputers, then passing them around on a local area network.")

[n8]. See, e.g., Nolle, T., The Wake-Up Call Comes, Computerworld, October 2, 1989, at 47, ("Studies show that most businesses have no real awareness of the state of their local area network security, and those who do invariably think it is better than it really is."); See also, Korzeniowski, supra note 7, at 91, ("Many companies refuse to acknowledge security violations. Instead, they cover up breaches. Consequently, few statistics outline just how many systems have been compromised.")

[n9]. See Crain's New York Business, June 11, 1990, at 22, ("Avoid using . . . local area networks for sensitive information")

[n10]. See Milgrim, R, Milgrim On Trade Secrets, (Release 35, October 1990), § 2.04, at 2-55, ("Essentially, the courts require that the possessor of a trade secret take reasonable measures to protect its secrecy.")

[n11]. See generally, Id. at § § 2.03 - 2.05

[n12]. "Wireless" LANs also exist. For a general discussion of wireless LANs, see, Derfler, F., LANs Without Wires, PC Magazine, May 29, 1990, at 295

[n13]. See, e.g., Menkus, supra note 6, at 84, defining a LAN as "some number of microcomputers, terminals, printers, facsimile units, and other devices with an assortment of application programs (including electronic mail and keyboard-to-keyboard conferencing) and databases--and facilitates the sharing of these resources."

[n14]. An example of such a computer program is Lotus 123 by Lotus Corporation.

[n15]. Data is often that which is read or otherwise manipulated by a computer program. It can be representative of virtually anything, including customer lists or source code.

[n16]. Madron, supra note 3, at 3; See also Martin, T, Local Area Networks; Architectures and Implementations, 4 (1989), quoting the Institute of Electrical and Electronics Engineers (IEEE) definition for a LAN: ("A datacomm system allowing a number of independent devices to communicate directly with each other, within a moderately sized geographic area over a physical communications channel of moderate data rates.")

[n17]. See generally, Madron, supra note 3, at 2.

[n18]. "Servers" as used in this discussion refer to file servers as opposed to, for example, a print server, which allows workstations to share a single printer.

[n19]. See, e.g., Schweitzer, J., Protecting Information On Local Area Networks, 10 (1988), ("There are many types of workstations, but the most common is the personal computer (for example, the Xerox 6065 personal computer or the IBM PC-AT.)")

[n20]. See, e.g., Madron, supra note 3, at 14, ("There are on the market today LANs that [can support] a wide variety of computer devices from micros to mainframes, . . . [but that] it is also true that the massive current expansion of the use of [microcomputers] has probably done more to spur the interest in and acquisition of LANs than any other single development."); See also, Martin, supra note 16, at 8, ("A local area network interconnects computing devices, such as personal computers, which may be of the same or different types.")

[n21]. See, e.g., James, G., Checking Out Connections, Network World, February 1, 1988, at 37, ("Processing work load is distributed among the network workstations."); See also, Madron, supra note 3, at 9, ("[V]irtually all processing is distributed out to microbased workstations, . . .")

[n22]. See, e.g., Liebing, E., What About Distributed Processing, LAN Times, July, 1990, at 4, ("The LAN concept offers many enhancements to network computing, two of which are connectivity and distributed processing.")

[n23]. See, e.g., Goos, G., Lecture Notes in Computer Science, at 3 (1989), containing the article Why is a LAN a LAN by Kirkpatrick, stating that a characteristic not present in WANs is that "all [workstations] on a LAN are able to listen to most information on the LAN. For example, in a [LAN using a carrier sense multiple access with collision detection (CSMA/CD) access method] all stations may listen to the information. In a [LAN using a token ring access method], only those stations which are between the sending and receiving stations on the ring are able to listen to information."

[n24]. See e.g., Martin, supra note 16, at 168, ("A bridge is able to interconnect physically distinct networks, . . ."), and at 175, ("A gateway is used to interconnect networks that may have entirely different architectures.")

[n25]. See, e.g., Madron, supra note 3, at 11, ("Connectivity is a central concept in local area networks, meaning that any device on the LAN may be addressed as an individual connection. For a large computer with many ports, each port is a connection, whereas a single-user terminal or microcomputer is also a connection.")

[n26]. See Thomas, R., How Can We Help Stop The OSI Merry-Go-Round?, Network World, July 4, 1988 at 17, ("Linking disparate computers via common applications and multiple medias in a plug-compatible manner is the promise of the ISO model for the OSI.")

[n27]. See, e.g., Tangney, J., Local Area Networks And Their Applications, 215 (1988) ("The MAP standards [developed by General Motors] are essentially an application-specific subset of the ISO protocols designed to meet the needs of factory automation.") See also, Madron, supra note 3, at 25, ("OSI is a key factor in the development of the Manufacturing Automation Protocol (MAP), developed by General Motors.")

[n28]. See, e.g., Madron, supra note 3, at 25 ("the U.S. Department of Defense . . . supports its own Transport Control Protocol (TCP).")

[n29]. See, e.g., Madron, supra note 3, at 190, ("Since one of the primary objectives of a Local Area Network is connectivity, successful implementation of a highly connective system tends to thwart some methods of security and control.")

[n30]. See, e.g., Bender, The Future Of Software Protection: Protection of Computer Programs: The Copyright/Trade Secret Interface, 47 U.Pitt L. Rev. 907, (Summer 1986) ("Those seeking to protect [computer programs] have traditionally relied on trade secret law."); See Also, Rodau, Computer Software: Does Article 2 of the Uniform Commercial Code Apply?, 35 Emory L.J. 853, 854 n6 (Fall 1986) ("Early attempts to protect software successfully relied on Trade Secret Law.")

[n31]. Regarding patent protection see, e.g., Fraser, J., Keeper of the Faith, EDN, October 1, 1990, at 174, 178 ("The U.S. Patent Office began granting patents on software in 1981. Thousands of them have issued so far, and they cover many common and widely used functions."); Regarding copyright protection see, e.g., Hammond, H., Software Purchases Gives Buyer Limited License, The National Law Journal, August 20, 1990, at 19, ("Federal copyright laws protect computer software"), citing case law; See also, 17 U.S.C. Sections 101, 102 and 117 indicating that computer programs are protected by copyright law as literary works.

[n32]. For example, patents and copyrights are usually meant for public distribution. Consequently, dissemination of the subject matter will not affect the validity of a copyright or patent. However, when the subject matter of a trade secret becomes

publicly known, it is lost forever as a trade secret regardless of the wrongfulness of the public dissemination.

[n33]. See, e.g., Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974), stating that [n]ovelty in the patent law sense, is not required for a trade secret." See also, Milgrim, supra note 10, § 208[2] at 2-192 - 2-194, ("[A] trade secret need not be patentable"); Sadler, C., Federal Copyright Protection And State Trade Secret Protection, 33 Am. U. L. Rev 667, 669 n10, ("The Copyright Act of 1976 explicitly denies protection to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is expressed . . . . All of these, however, may properly be protected by trade secret.")

[n34]. The duration of copyright protection is the life of the author plus 50 years (see 17 U.S.C. Section 302. For works created before January 1, 1978, see 17 U.S.C. Sections 303 and 304); Regarding the duration of trade secrets, see, e.g., Readio, M., Minnesota Development: Balancing Employers' Trade Secret Interests in High-Technology Products Against Employees' Rights and Public Interests in Minnesota, 69 Minn. L. Rev. 984, 987 note 17, ("Unlike patent and copyright protection, trade secret protection is potentially unlimited in duration, . . ."); see also Moore v. University of California, 793 P.2d 479, 15 U.S.P.Q.2d 1753, 1782 (Cal.Sup.Ct. 1990) stating that trade secret protection "is both quickly acquired and unlimited in duration."

[n35]. An unpublished work can be subject to copyright protection. (See 17 U.S.C. Sections 104(a) and 102). However, an action for infringement may not be instituted until registration of the work at the U.S. Copyright Office. (See 17 U.S.C. Section 411(b)). Although this registration requires a deposit of the work, it is possible to deposit only portions of the computer program listing. This permits trade secret and copyright protection to be maintained simultaneously. (See 37 C.F.R. Section 202.20(c)(2)(vii)).

[n36]. When a patent issues, it is published and becomes part of the public record, and is readily accessible. Thus, it cannot be maintained as a secret. See, for example, 35 U.S.C. Section 13, stating that patents may be sent to public libraries "which shall maintain such copies for the use of the public, . . ." See also, Milgrim, supra note 10, § 8.02[2], at 8-10 - 8-11, ("[F]or all practical purposes it may be stated that a claim of trade secret and patent protection for the same matter is inherently inconsistent if the matter is published.")

[n37]. The conditions of patentability are set forth generally in Title 35 of the U.S. Code.

[n38]. An advantage of patent law is derived from 35 U.S.C. Section 271(a). This section provides that "whoever without authority makes, uses or sells any patented invention, within the United States during the term of the patent therefore, infringes the patent." Under this section, one could create a previously patented invention independently of any information derived from the patent owner and still infringe the patent. This differs from trade secret protection, which gives the trade secret owner a cause of action only against one who has unlawfully used or disclosed the owner's information in violation of some contract or duty owed to the owner. See Milgrim, supra note 10, at § 8.02[8] for a comparison of patent and trade secret protection regarding this and other issues. See 35 U.S.C. Sections 281-295 for available remedies for infringement of patents. But see also, supra note 51 for remedies for misappropriation of a trade secret.

[n39]. Patent law is derived from Title 35 of the U.S. Code, and Copyright law is derived from Title 17 of the U.S. Code.

[n40]. Restatement of Torts (First), Section 757

[n41]. 14 UTA 329 (Supp. 1988)

[n42]. It is noted that the UTSA was formed from the perceived need to develop a statutory scheme for protecting trade secrets. The Commissioners Prefatory note to the UTSA states that "notwithstanding the commercial importance of state trade secret law to interstate business, this law has not developed satisfactorily . . . ." One commentator observed ". . . clear uniform trade secret protection is urgently needed . . ." (See 14 Uniform Laws Annotated 434).

[n43]. See, e.g., Miller, S., Florida's Uniform Trade Secrets Act, 16 Fla.St.L.Rev 863, 868 (Fall 1988) ("[T]he UTSA and the common law [which is summarized by the Restatement] 'are in harmony, and both can be cited to support the same result."); However, some differences do exist. See, for example, UTSA Section 1 (commentary), ("The [UTSA] definition of 'trade secret' contains a reasonable departure from the Restatement of Torts (First) definition which required that a trade secret be 'continuously used in one's business.")

[n44]. Alabama, Alaska, Arizona, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Hawaii, Idaho, Illinois, Indiana, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Montana, Nevada, New Hampshire, New

Mexico, North Dakota, Oklahoma, Oregon, Rhode Island, South Dakota, Utah, Virginia, Washington, West Virginia and Wisconsin.

[n45]. Comment b of the Restatement states that "[a] trade secret may consist of any formula, pattern, device or combination of information . . ." Section I (4) of the UTSA states that "[t]rade secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process, . . ." For cases specifically holding that computer programs are protectable subject matter, see Integrated Cash Management v. Digital Transactions 732 F.Supp 370, 13 U.S.P.Q. 2d 1397 (S.D.N.Y. 1989); Cybertek Computer Products, Inc. v. Whitfield, 203 U.S.P.Q. 1020 (Cal. Super. Ct. 1977).

[n46]. Comment b of the Restatement states that a "trade secret" gives a person "an opportunity to obtain an advantage over competitors who do not know or use it." UTSA Section 1(4)(i) states that a trade secret "derives independent economic value [from not being known to or ascertainable by] other persons who can obtain economic value from its disclosure or use, . . ."

[n47]. Comment b of the Restatement states that "[m]atters of public knowledge or of general knowledge in an industry cannot be appropriated by one as his secret." Comment b also states that relevant factors are "(1) the extent to which information is known, outside of [the owner of the information's] business; . . . (6) the ease or difficulty with which the information could be properly acquired or duplicated by others." Section 1(4) (i) of the UTSA states that a trade secret is subject matter "not being readily ascertainable by proper means . . ." See also Milgrim, supra note 10, at 2-175 - 2-176, ("[A] matter cannot be considered a trade secret if it is well known or readily ascertainable.")

[n48]. See, e.g., Comment b of the Restatement, stating that "[a]n exact definition of a trade secret is not possible." See also, Klitzke, The Uniform Trade Secrets Act, 64 Marq. L. Rev. 277, 284 n37 (1980)), ("While different sets of criteria have been set forth by various authorities enumerating what defines a trade secret, one commentator has stated that "the parameters of trade secret protection generally defy precise identification.")

[n49]. Comment b of the Restatement states that a factor in determining whether given information is a trade secret is "(3) the extent of measures taken by [the trade secret owner] to guard the secrecy of the information; . . ."; Section 1(4)(ii) of the UTSA states that for subject matter to be a trade secret, it must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

[n50]. See, e.g., Milgrim, supra note 10, § 2.04 at 2-55, stating "the courts require that the possessor of a trade secret take reasonable measures to protect its secrecy", and citing a plethora of case law supporting this statement

[n51]. Comment e of the Restatement suggests that the person harmed "may recover damages for past harm, or be granted an injunction against future harm by disclosure or adverse use, or be granted an accounting of the wrongdoer's profits, or have the physical things embodying the secret . . . surrendered by the wrongdoer for destruction." According to the UTSA, the owner of the trade secret can get an injunction and/or damages where another party has "misappropriated" the owner's trade secret (see UTSA, supra note 41, Sections 2 and 3). In addition, where there has been "willful and malicious misappropriation . . . the court may award reasonable attorney's fees . . ." (Id. at Section 4), as well as "damages in an amount not exceeding twice any award made under subsection [3(a) of this Act]" (Id. at Section 3(b)). Further, It should be noted that a breach of duty arising from a finding of a misappropriation of a trade secret may also be a breach of contract (See the Restatement at Comment j).

[n52]. Comment f of the Restatement states that "[e]xamples of such means are fraudulent misrepresentations to induce disclosure, tapping of telephone wires, eaves dropping or other espionage." Section 1(1) of the UTSA states "Improper means' includes theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means; . . ." Rather than mentioning "improper" means and "breach of duty" separately as does the Restatement, the UTSA specifically mentions "breach of a duty" as constituting "improper" means. The UTSA does, however, loosely break down misappropriation by "acquisition" (Section 1(1)(2)(i)) and "disclosure or use" (Section 1(1)(2)(ii)). For a general discussion of what constitutes improper means, see Hilton, What Sort Of Improper Conduct Constitutes Misappropriation Of A Trade Secret, 30 IDEA 287 (1990).

[n53]. Section 757(b) of the Restatement indicates that one will be liable for misappropriation where a disclosure of a trade secret "constitutes a breach of confidence . . ." The UTSA mentions breach of duty in Section 1(1). A typical relationship where such a duty arises is an employer-employee relationship, where the employee has learned valuable trade secrets from his employment (see Milgrim, supra note 10, at § 5.02 for a general discussion of this topic).

[n54]. The definitions relating to misappropriation in both the Restatement and the UTSA speak in terms of a "trade secret," whose definition has been established as discussed above. For example, Comment c of the Restatement states that "[o]ne who has a trade secret may be harmed merely by the disclosure of his secret to others . . ." [emphasis added]. Sections 1(2)(i) and (ii) of the UTSA speak of "acquisition of a trade

secret of another . . ." [emphasis added] and "disclosure or use of a trade secret of another . . ." [emphasis added], respectively.

[n55]. See, e.g., Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 897, 220 U.S.P.Q. 811, 816 (Minn. Sup. Ct. 1983), ("Without a proven trade secret there can be no action for misappropriation . . .")

[n56]. 431 F.2d. 1012, 166 U.S.P.Q.2d 421 (5th Cir. 1970)

[n57]. Id. at 1016, U.S.P.Q. at 424. The defendants were found guilty of misappropriation by virtue of acquiring the trade secret by improper means.

[n58]. See, e.g., Surgidev Corporation v. Eye Technology Inc., 828 F.2d 452, 455, 4 U.S.P.Q.2d 1090, 1092 (8th Cir. 1987), citing the UTSA, and stating that "Surgidev was required to take efforts 'reasonable under the circumstances' to maintain the secrecy of its customer information." See also UTSA at Section 1 (commentary), ("The efforts required to maintain secrecy are those 'reasonable under the circumstances." [emphasis added]); See also, Milgrim, supra note 10, § 2.04 at 2-60, ("[T]o determine if secrecy has been maintained, the trier of fact must consider the entirety of circumstances surrounding use.")

[n59]. See, e.g., Samuelson, P., CONTU revisited, 1984 Duke L.J. 663, 761, ("The law will usually protect those who make reasonable efforts to keep their secrets secure. But what a reasonable effort to maintain secrecy is depends on the circumstances. Given that "hacking" to gain improper access to computer systems is a common sport among young computer enthusiasts, the standards for maintaining trade secrecy as to computer programs may be higher than for other types of work."); See also, Unkovic, D. The Trade Secret Handbook, 192 (1985), indicating that espionage in high-tech industries is a relatively common occurrence, and that in such situations "[e]spionage should not be a surprise; it should be anticipated and not allowed to happen."

[n60]. See, e.g., Buerger, D., Computer Security Issues Now Front Page News, Infoworld, January 9, 1989, at S1, ("In the strictest sense, popular LANs provide little, if any, network security."); See also, Nolle, supra note 8, at 47, ("LAN security is, frankly, a joke in most companies.");

[n61]. See Korzeniowski, supra note 7, at 86, quoting another commentator, ("LAN security does not measure up to mainframe security. LAN security is usually limited to password schemes, which can be broken."); See also, Shields, J., Security:

From Passwords To Protocols, Its A Risky Business, Government Computer News, July 24, 1989, at 67, ("Local area networks based on PC's not only run many of the same security risks as large computer systems, they add vulnerabilities all their own."); Tangney, supra note 27, at 116, ("Centralized systems have their own security problems, but using a LAN introduces additional ones."); But note that this opinion is not universally held. See, for example, Korzeniowski, supra note 7, at 86, quoting another commentator, ("LAN security is good, especially when compared to security on some IBM mainframes, . . .").

[n62]. See, e.g., Booty, Local Area Networks, Computer Fraud and Security Bulletin, June 1989, at 11, ("[W]hile security in large computer systems is well developed and mature, [LAN] security is still in its infancy.") See also, Ambrosio, Prevailing View Of LAN Security: Lots Of Talk, Software Magazine, October 1988, at 99, quoting another commentator, ("PC LANs aren't as mature as other technologies like mainframes . . . [s]o the level of security built in isn't as sophisticated."); Lenko, LAN-WAN Issues, Telecommunication, November, 1989, at 75, 76, ("WAN environments have historically been more security conscious than LAN environments.")

[n63]. See, e.g., Harris, M., Off-line data storage calls for security measures, Government Computer News, February 19, 1988 at 36, ("Network users who have migrated to LANs from single-user, stand-alone PCs may be unaware of data security issues.")

[n64]. See, e.g., Korzeniowski, supra note 7, at 91, indicating that when microcomputers are suddenly attached to a LAN, that "[m]any users who have had free access to data may resist added security measures."

[n65]. See Krumrey, supra note 7, at 96, ("Gateways and bridges do wonders in providing wider access to resources, but also multiply the risks and increase the need for vigilance . . . . Outside competitors, market analysts, and hackers also can gain access to the network by using . . . a modem, in the event that the LAN has dial-in connections.")

[n66]. In the context of this discussion, "physical protection" includes physical barriers, as well as logical barriers (such as password protection) which are implemented, for example, by the LAN operating system.

[n67]. That is, whether adequate "notice" was given to potential users of the trade secret indicating that the subject matter was considered secret.

[n68]. It should be noted that the implementation of physical protection can also serve as a way of indicating to persons that the information is considered a secret (that is, as a form of notice). See, for example, Miller, supra note 43, at 889, ("A defendant is on notice if, while viewing the trade secret, he is exposed to 'obvious security measures designed to keep the trade secret from general view . . .")

[n69]. See, e.g., Wilson Certified Foods, Inc. v. Fairbury Food Products, Inc., 370 F.Supp. 1081, 1086 (D.Neb 1974), indicating that a combination of factors (relating to various themes) led the court to find that the plaintiff had not taken significant efforts to protect its alleged trade secret.

[n70]. 332 N.W.2d 890, 220 U.S.P.Q. 811 (Minn. Sup. Ct. 1983)

[n71]. See Id. at 902, 220 U.S.P.Q. at 820, ("ECC's physical security measures did not demonstrate an effort to maintain secrecy. By 'security' we mean the protection of information from discovery by outsiders. For example, the main plant had a few guarded entrances, but seven unlocked entrances existed without signs of limited access.")

[n72]. Id. at 903, 220 U.S.P.Q. at 821

[n73]. See Id. at 902, 220 U.S.P.Q. at 820, ("One sign was posted at each plant, however, marking the research and development lab . . . and the machine shop . . . as restricted to 'authorized personnel.")

[n74]. 370 F.Supp. 1081 (D.Neb 1974)

[n75]. See Id. at 1082

[n76]. See ID. at 1085, where the court noted that "[a]pproximately ten to twelve tours of college students were conducted through the Bits-O-Bacon production area each year and viewed the entire procedure."

[n77]. Id. at 1085

[n78]. Id. at 1085; See Also, Wheelabrator Corporation v. Fogle, 317 F.Supp 633, 638, 167 U.S.P.Q. 72, 76, where the plaintiff/trade secret owner "introduced evidence

relating to the fencing of the manufacturing facilities." In finding that the plaintiff had not taken reasonable precautions, the court indicated that the plaintiff made no distinction "between the [sensitive area] and other manufacturing facilities within the fenced area. The [sensitive area] was afforded no greater security than the admittedly non-secret facilities."

[n79]. See, e.g., Protect Your Trade Secrets -- Now, Inside R&D, January 11, 1989, at 3, giving advice on how to protect trade secrets, ("Here are some ways to protect trade secrets: . . . Designate key areas, make them more secure, and monitor visitors' access.")

[n80]. Servers are also discussed regarding the issue of "locking" trade secret information in the following section.

[n81]. See, e.g., Schweitzer, supra note 19, at 60-61, stating that one must "be concerned about physical access to the network infrastructure. This includes the switching centers, data centers, network servers, and communication junction boxes. All LAN resources should be considered privileged; . . . Effective office physical access controls are a minimum requirement . . . [O]n-line printers also must be secured." See also, Id. at 102, stating that where PCs are used as workstations, "[a]reas where PCs are usedshould be secured according to the company classification of the information processed, [and that] high-value information . . . may require special efforts . . ."; Id. at 84, discussing LAN security, ("Electronic security elements: . . . Physical elements: door locks, guards, closed circuit television monitors, trespass alarms, entry control systems, . . ."); See also, Shields, supra note 61, at 67 ("LANs store common data on file servers, in addition to which the networked [workstations] themselves can store data. All the networked hardware--individual LAN workstations as well as file servers--needs physical protection."); Durr, Michael et al., Networking Personal Computers, 352 (1989), ("Data security can take many forms. The simplest is physical security, which may be . . . a guard at the door . . . Locks can set up barriers anywhere from the back door to the office . . .")

[n82]. See, e.g., Computer Site Protection Provides Cheap Insurance, Digital Review, April 16, 1990 at 37, 41, ("A smart card can also keep an audit trail similar to a software audit trail, by which every transaction is recorded on the chip.") See also, infra note 169; See also, Wellborn, S. Microchip Brings Plastic Junkies To Their Knees, U.S. News And World Report, February 2, 1987 at 50, 51 ("By incorporating some form of foolproof identification, smart cards could serve as keys to restricted areas.")

[n83]. See, e.g., Buerger, Computer Security Issues Now Front Page News, supra note 60, at S2, ("Workstations present a risk because network users are often sloppy

about workstation security procedures, and workstations are everywhere." [emphasis added]); See also, Booty, supra note 62, at 12, ("Workstations constitute the highest security risk in a LAN."); With regard to workstations generally (i.e. computer terminals), see Banks, Security Policy, Computers and Security, November, 1990, at 605, 608, discussing a general computer security policy, ("Access to computer systems via terminals will be permitted only to staff so authorized by the data owner.")

[n84]. See, e.g., Krumrey, supra note 7, at 99, ("A complete security scheme should allow powerful IDs to be restricted to actual workstations that belong to the ID's owner.")

[n85]. See, e.g., Seidel, A, What The General Practitioner Should Know About Trade Secrets and Employment Agreements, 90 (1984), ("Sensitive areas ordinarily should be closed to visitors. However, if simple observation would not jeopardize trade secret security, this precaution may be modified.")

[n86]. See, e.g., Saunders, Protecting Your Business Secrets, 78 (1985), ("All visitors should be channelled securely to a reception point . . . . The visitor should then be escorted to the member of staff or collected by him to ensure that no visitor can get 'lost'. All visitors should, of course, be escorted off the premises on conclusion of their business.")

[n87]. See, e.g., Booty, supra note 62, at 11, ("The most important, yet often neglected, aspect of LAN security is the role of LAN managers."); See also Shields, supra note 61, at 70, ("Someone has to be in charge of seeing that the LAN operates safely and reasonably. If everyone is responsible, then no one is.")

[n88]. supra note 81. See also, Schweitzer, supra note 19, at 115, discussing a LAN security policy checklist, ("Are network servers installed in secure areas to prevent unauthorized physical access?")

[n89]. See, e.g., Durr, supra note 81, at 353, ("A local area network presents some additional security problems because of its dispersed nature and because many people have access to the network . . . . Badges and personal recognition, therefore, may not be successful in large companies where everyone is not personally known.")

[n90]. 759 F.2d 1053, 225 U.S.P.Q. 797 (2nd Cir. 1985)

[n91]. Id. at 1064, U.S.P.Q. at 804

[n92]. 332 N.W.2d at 902, 220 U.S.P.Q. at 820

[n93]. 370 F.Supp at 1085

[n94]. Security issues regarding printers as they relate to the dissemination of information are discussed in the section below.

[n95]. See, e.g., Gerber, Safeguarding servers calls for a fortress mentality, PC Week, April 24, 1989 at 48, ("[W]e've got to give our servers physical protection from intruders. In essence, we have to build fortress servers."); See also Shields, supra note 61, at 70 ("Depending on the site's overall security, it may be a good idea to locate file servers and printers in rooms that are locked or have controlled access, particularly after working hours."); See also, Booty, supra note 62, at 11, ("LAN configurations often require that the file servers and printers be installed in secure environments.")

[n96]. See, e.g., Booty, supra note 62, at 12, ("Security problems are high [in peer based LANs] because of the lack of centralized data storage across the network.")

[n97]. Korzeniowski, supra note 7, at 85; See also, Krumrey, supra note 7, at 99, ("The user ID literally is the key to network access. Every password should have a minimum of six or seven characters.")

[n98]. See Schweitzer, supra note 19, at 85, indicating that "Computers and devices connected to networks (directly or via dial-up) or processing company classified information require the following controls:

1. A unique, personal identification token (for instance, an employee ID or account code) must be assigned to each user.
2. A unique, personal authentication token (such as a password, fingerprint code generator, or combination thereof) must be used to validate the identity claimed."

[n99]. See, e.g., McGiffert, Buckling Down On LAN Security Issues, Computerworld, October 16, 1989, at 80, describing passwords and privileges, ("Initial access is gained through a user/password system, an operating system function. Upon log-on, users require differing access privileges. Different operating systems distribute these in different ways. In some, each user is assigned access privileges directly; the user's access is activated after log- on. In others, users are assigned 'sharenames' and

passwords. Users gain access by typing the appropriate names and passwords after logging on to the network.")

[n100]. See, e.g., Schalk v. State, 767 S.W. 2d 441, 444, (Tex. App. Dallas 1988), where the court found that the trade secret owner had taken reasonable precautions in part because the trade secret information, consisting of several computer programs, "were stored in a memory bank of a computer system in the speech laboratory. [Defendant] was allowed access to these programs through a code or password specifically assigned to him. The password or code assigned to an employee in the laboratory was personal to that employee andwas assigned only if their job duties required access to the information and any of those confidential programs stored in the memory bank."

[n101]. See Morissey, J., Managers Tackle LAN Security Gaps, PC Week, January 23, 1989, at 33, quoting another commentator, ("Any business whose entire existence depends on knowledge remaining secure and depends on passwords to protect it [is] foolish.")

[n102]. Wilson, D., Trends in Information Security, Computer Security Journal, Vol. 4, No. 2, 1987 at 29; See also, Johnson, R., The Ins and Outs of security, Financial Times, May 23, 1989 at 40, ("Biometric systems can recognize almost any characteristic of the human body to identify the individual. They can recognize voices, fingerprints, footprints, and the pattern of blood vessels and the back of the retina.")

[n103]. See, e.g., Shields, supra note 61, at 70 ("Workstations, just like many computer or mainframe terminals, ought to be logged off the network when they remain unattended for a time.")

[n104]. See, e.g., Durr, supra note 81, at 354, ("The system should enable a user to attempt a log-in no more than three times.") See also Korzeniowski, supra note 7, at 85, ("Most network operating systems cut off a user who unsuccessfully tries three times to enter his password.")

[n105]. See, e.g., Booty, supra note 62, at 12, ("Unauthorized use may be prevented by keyboard lock devices.")

[n106]. 370 F.Supp. at 1085

[n107]. 332 N.W.2d at 902, 220 U.S.P.Q. at 820

[n108]. 648 F. Supp. 661 (D. Minn. 1986), aff'd, 828 F.2d 452 (8th Cir. 1987)

[n109]. Id. at 694

[n110]. Id. at 693

[n111]. Shields, supra note 61, at 70; See also, Schweitzer, supra note 19, at 61, ("When high-value files are in file servers, only specifically authorized persons should be given privileged access to those files; . . .") With regard to trade secrets generally, see Unkovic, supra note 59, at 36, advising corporations to "[r]estrict disclosure of trade secrets to selected employees who have a genuine reason to know what they contain."

[n112]. See, e.g., Schweitzer, supra note 19, at 14, ("[A] dangerous situation exists with regard to dial-up services to a LAN. A dial-up connection requires only that the person attempting such a connection has a suitable terminal device, a modem . . ., and a telephone."); See also Shields, supra note 61, at 70, ("When off-site parties, known or unknown, dial in by modem, they can bypass many of the LAN's physical security components.")

[n113]. See, e.g., Korzeniowski, supra note 7, at 86, discussing, "a modem call-back system, which prevents hackers from using a corporation's dial-up lines."

[n114]. See Ambrosio, supra note 62, at 104, quoting and paraphrasing another commentator, ("What is considered adequate security depends on . . . whether the LAN is really local or whether it allows dial-in.' . . . as LANs become more interconnected, security needs to be beefed up.")

[n115]. See Buerger, As Networks Pick Up More Novices, Security Suffers, supra note 6, at 13, ("Dial-up links aren't the only weak spots to network security. Bridges and gateways that connect multiple sites increase exposure."); See also, Nance, Everybody In The Pool, Byte Magazine, November 14, 1989 at 126, ("Unless it's only for occasional dial-out use, a gateway should receive some of the same security precautions you give file servers."); Enyart, OS/2 LAN manager security still a problem, PC Week, October 16, 1989, at 52 ("[S]ecurity is a bigger concern when people bridge multiple LANs, because people outside your local work group may be getting at this information.")

[n116]. See, e.g., Schweitzer, supra note 19, at 14, ("Once connected on any network (wide or local), the caller has the potential to access files on many other networks. Further, the original network accessed has very little reliable means to ascertain the identity, and hence the rights, of the caller once an entry is achieved.")

[n117]. See, e.g., Weckstein, Trade Secrets, 19 (1988), ("Where trade secrets constitute an appreciable portion of the employer's work, the greatest enemy to security is the common copying machine.")

[n118]. See, e.g., Buerger, Computer Security Issues Now Front Page News, supra note 60, at S3 ("If people print confidential information on network printers, reserve a high-security printer for this purpose.")

[n119]. See, e.g., Krumrey, supra note 7, at 98, ("Printers connected to the LAN also can be a security threat. Sensitive information should not be printed on unattended printers where it might be seen (or even taken for copying) by any unauthorized personnel." [emphasis added])

[n120]. See, e.g., Urbonya, T., Getting A Grip On Sensitive Documents, Minneapolis - St. Paul City Business, May 14, 1990, Vol. 7, No. 48, Sec. 1, at 15, ("Record managers said it is important that documents be destroyed properly to avoid their falling into the hands of competition."); See also, Weckstein, supra note 117, at 23, ("[T]he employer should destroy any copies of trade secret documents that are not absolutely necessary for the conduct of business.")

[n121]. See, e.g., Durr, supra note 81, at 358, ("[A] local disk drive permits data theft. A person with access to the network and with a local disk drive can copy large amounts of data onto floppy disks in just minutes. The data then can be easily hidden and removed from even reasonably secure buildings.")

[n122]. See, e.g., Ferris, D., Most LANs Benefit From Diskless Workstations, Infoworld, March 27, 1989, at 42, ("Diskless workstations are excellent when you're dealing with confidential information, where you don't want users able to remove sensitive data."); see also, Glass, A Fairwell To Floppies: Diskless Bootstrapping, InfoWorld, August 13, 1990, at S9 ("Diskless workstations can provide LAN managers and users with increased security."); Durr, supra note 81, at 116, ("A diskless workstation . . . enhances security. The lack of any simple means of unloading files from the network or, for that matter, loading files onto the network (such as security-breaking programs) adds an additional level of protection.")

[n123]. See, e.g., Sobol, M., Security Concerns In A Local Area Network Environment, Telecommunications, March 1988, at 96, indicating that with regard to microcomputers, a diskless workstation "has all the microcomputer-processing capabilities with one major exception -- it has no disk-storage capacity."

[n124]. See, e.g., Smith, T., Analysts See Limited Use Of Wireless LANs, Network World, November 5, 1990, at 23, ("[A] cause for user skepticism about wireless LANs is security, . . .")

[n125]. This technology involves the sending of information over multiple frequencies which are spread out over a large bandwidth.

[n126]. See, e.g., Derfler, F., LANs Without Wires, supra note 12, at 295, stating that in certain UHF-type wireless LANs which qualify as spread-spectrum systems, "[s]pread-spectrum technology improves security - even beyond that of a conventional wired LANs - since no single frequency can be tapped to siphon off data."; See also, Nash, K., New Breed Of Wireless LANS Overcome Speed, Interference Problems While Keeping Costs Low, Computerworld, October 2, 1989 at 8, ("Spread spectrum is one radio system . . . that 'just isn't detectible . . .")

[n127]. See, e.g., Booty, supra note 62, at 12, ("Cabling becomes a security risk if people are allowed to attach a network monitor or protocol analyzer to the network. User passwords and sensitive information are just some of the items that can be captured."); See also, Durr, supra note 81, at 359, ("Whenever information is transmitted, even through cable, unauthorized persons can potentially intercept that information . . . . More sophisticated devices can intercept the signals a considerable distance from the cable.")

[n128]. See, e.g., Durr, supra note 81, at 359, ("You can eliminate the likelihood of a signal interception by using a shielded cable, a cylinder of braided copper wire that encases the intelligence-carrying wires.")

[n129]. See, e.g., Terlaga, R., Is Your LAN Safe?, United States Banker, July, 1989, at 50, ("[Fiber optic cable] does not send any radio frequency emissions, which could conceivably be intercepted.")

[n130]. See, e.g., Id. at 50, ("[I]t is much more difficult to physically tap into a fiber optic LAN to intercept the data on it.").

[n131]. supra note 23.

[n132]. See, e.g., Goos, supra note 23, at first page of the article Architectural Considerations for LAN Security Protocols, by Lambert, ("Within the Institute of Electrical and Electronics Engineers (IEEE) standard activities, [persons are] developing a security protocol and key management for LANs. This standard is still in the preliminary phases of definition.")

[n133]. See, e.g., Krumrey, supra note 7, at 99, ("[A]ll electronic devices emit electromagnetic signals produced by electricity. Sensitive snooping devices can pick up these signals from a workstation, whether or not it is on a LAN, and intercept the data flow.")

[n134]. See, e.g., Krumrey, supra note 7, at 99, ("If the workstation is shielded, usually with lead, electrical emissions can be reduced to an undetectable level.")

[n135]. See McGiffert, supra note 99, at 80, ("Data encryption is a highly effective barrier to network data theft."); See also, Sobol, supra note 123, at 96, ("[E]ncryption represents one of the most effective methods of controlling sensitive data on portable media.")

[n136]. See Durr, supra note 81, at 355, indicating that a sophisticated thief "can collect log-in routines and passwords as they are entered, often simply by tapping into the network . . . . Passwords can be encrypted at the workstation and decrypted at the central processor so that the data on the cable is unusable through a tap."; See also, Highland, J., How Secure Is Your Network?, Computers and Security, October, 1990, at 470, 471, discussing a LAN security checklist, ("Do you . . . keep the password list encrypted on the system?")

[n137]. See, e.g., Buerger, Computer Security Issues Now Front Page News supra note 60, at S3, discussing encryption of all data in a LAN versus encryption of only passwords, ("Password encryption only ensures that plain- text passwords never transmit over the network. Data or session encryption is more secure because everything is coded.")

[n138]. See Schweitzer, supra note 19, at 86, stating that where "high value" information is concerned, "[e]ncryption of such information is required when transmitted over telecommunications circuits." See also, Highland, supra note 136, at 472, discussing

a LAN security checklist ("Do you . . . require critical data to be encrypted during transmission to external nodes?")

[n139]. For the purposes of this discussion, signed agreements are discussed as a factor in determining whether reasonable precautions were taken. As indicated above, however, they could also be used as evidence of a breach of contract.

[n140]. 332 N.W.2d at 902, 903, 220 U.S.P.Q. at 820, 821.

[n141]. 370 F.Supp. at 1085.

[n142]. See, e.g., Seidel, supra note 85, at 23, ("It is unwise for an employer to attempt to restrain an employee from using anything other than that which is truly a trade secret. Otherwise, the entire agreement may be declared 'null and void' for 'overreaching' by unduly and unfairly restricting the freedom of movement of an employee."); See also, Milgrim, supra note 10, § 3.02[2][a] at 3-112, ("The cases are numerous in which courts have declined to enforce restrictive covenants because they were too broad and therefore constituted unreasonable restraints on trade."), citing numerous cases.

[n143]. 203 U.S.P.Q. 1020 (Ca. Super. Ct., Los Angeles County, 1977).

[n144]. Id. at 1021.

[n145]. 642 P.2d 732 (Utah 1982).

[n146]. Id. at 734.

[n147]. See, e.g., Unkovic, supra note 59, at 37, 38, ("Commercial reality often dictates that trade secrets are needed by parties who are not your employees. As a general rule, the law says a trade secret holder must prove disclosures of its trade secrets were necessary and done in an appropriate fashion [i.e. there was a "need-to-know"] . . . . There is no magic formula, but what is absolutely necessary is a conscious corporate effort to maintain the secrecy at the time of disclosure and while it is used by a third party."); See also, Milgrim, supra note 10, § 3.02[1][c] at 3-15, ("A written agreement clearly and unequivocally puts an employee or an independent contractor on notice of the trade secret owner's claims.")

[n148]. See, e.g., regarding trade secrets generally, Seidel, supra note 85, at 23, ("The proprietor of a trade secret should require all employees who may have access to the trade secret to sign an agreement not to divulge the secret.")

[n149]. See, e.g., Id., ("Agreements should be varied to cover particular situations, and no agreement should be used for all employees. Employees in research and development, who most likely will learn and develop trade secrets, should have an agreement especially tailored for them.")

[n150]. See, e.g., Electro-Craft, supra at note 70, at 332 N.W.2d at 902, 903, 220 U.S.P.Q. at 820, 821; See also Weckstein, supra note 117, at 20, ("The employer should make certain that each employee is alerted to the employer's trade secret policies.")

[n151]. See, e.g., Schweitzer, supra note 19, at 116, outlining procedures for LAN security, ("Do employees have a clear understanding of their responsibilities for protection of company information? With hundreds or thousands of terminal users, the company simply cannot supervise activities; individual employee understanding and motivation are critical.")

[n152]. See, e.g., Seidel, supra note 85, at 22, ("Generally, the proprietor of a trade secret should require all employees who may have access to the trade secret to sign individualized agreements not to divulge it." [emphasis added])

[n153]. For an example of a product which electronically verifies signatures, see Toigo, Biometrics Creep Into Businesses, Computerworld, June 11, 1990, at 75, discussing a signature verification system, ("As the user signs his name with a special pen on a digitizing tablet, Sign-On -- currently the top seller of signature verification devices -- measures various elements of the signature, such as stroke length and how fast each stroke is completed.")

[n154]. Where strict security measures are appropriate, users can be required to sign their name each time they access the information as well.

[n155]. See, e.g., Durr, supra note 81, at 45, ("LANs permit users to share information and communicate.")

[n156]. 203 U.S.P.Q. at 1021.

[n157]. 642 P.2d 732 at 735.

[n158]. 332 N.W.2d at 903, 220 U.S.P.Q. at 821.

[n159]. See Seidel, supra note 85, at 90, ("All intracompany documents that reflect on the trade secret should be marked "Confidential.")

[n160]. See, e.g., Brown, Protecting Trade Secrets, Electronics, March 10, 1983, at 24, ("All documentation disclosing the trade secret . . . should carry clear instructions limiting its dissemination, duplication, and use."); See also, Seidel, supra note 85, at 20, stating that with regard to trade secrets generally, "[t]rade secrets that are embodied in drawings or other written material should have the term 'Confidential,' 'Secret,' or the like, stamped on them. Preferably a longer legend should indicate that no use is to be made of the drawings or written material without the express written permission of the named employer.")

[n161]. See, e.g., Kutten, Software Developers Must Take Steps To Protect Own Secrets, Computerworld, August 25, 1986, at 86, ("Typical protective steps include the following: . . . Placing proprietary notices on the software media and on the opening screen of the software."); See also Schweitzer, supra note 19, at 87, ("[C]lassified information in visual display or document forms must be clearly marked with the appropriate symbol or computer-generated equivalent, of sufficient size to be obvious.")

[n162]. See, e.g., Saunders, supra note 86, at 84, discussing security techniques for photocopiers, but which can be applied to printers as well, ([P]hotocopiers located on different floors of a building can each be fitted with a device that clearly marks the floor number on every sheet of copying paper in such a way that it cannot be erased but not so noticeably that it obscures any of the text copied . . . Coloured toners can also be employed in the different machines and a code devised, . . .")

[n163]. In the context of this discussion, the license agreements contemplated are the type signed by the licensor and licensee, and not the shrink-wrap licenses used in mass-marketed software. For a discussion of shrink-wrap licenses, see Gemignani, Computer law, 199 (1985). For an example of a court case addressing the issue of shrink-wrap licenses, see Vault Corporation v. Quaid Software Ltd., 847 F.2d 255 (5th Cir. 1988).

[n164]. Of course, the owner of the trade secret should clearly set forth in the license agreement that the trade secret information being licensed is to be kept confidential. See generally, Milgrim, supra note 10, § 12.

[n165]. See, e.g., Milgrim, supra note 10, § 12.16[2][b], at 12-587, giving an example of possible contractual language, ("To protect the Confidential Information disclosed by the Licensor to the Licensee under this License Agreement against unauthorized use or disclosure the Licensee shall use protective measures no less stringent than those used by the Licensee within the Licensee's own business to protect its comparable confidential information.")

[n166]. See, e.g., Milgrim, supra note 10, § 12.16[1][b], at 12-582, ("[I]t is often prudent and desirable for the disclosing party to require the disclosee to impress upon those of its individual employees to whom access is to be granted the fact that the matter involved belongs to the disclosing party, is confidential, is being disclosed to only a limited number of employees of the disclosee (on a strict need-to-know basis) and is subject to restrictions on use and disclosure.")

[n167]. See, e.g., Milgrim, supra note 10, § 12.16[2][b][i], at 12-588, ("Since the disclosee takes on the duty not to use or disclose the confidential information . . ., a first principle is to define the subject matter of the restriction on use and disclosure." [emphasis in original])

[n168]. See, e.g., Milgrim, supra note 10, § 12.16[2][b] at 12-588, commenting on the effect of imposing security procedures on a licensee, ("the existence of these procedures may have evidentiary value to prove that the licensor has taken reasonable measures to protect its trade secrets in lawsuits by the licensor against third parties.")

[n169]. See, e.g., Durr, supra note 81, at 335, ("An audit trail is a record of who used the network, how long the network was used, and what file was accessed. This information can be used to provide . . . network security."); See also Shields, supra note 61, at 70, ("a record of network log- ons, file accesses and disk usage proves invaluable for . . . detecting attempted unauthorized access . . ."); Booty, supra note 62, at 13 ("Access accounting generates a report which details each user's access statistics.")

[n170]. See supra note 82.

[n171]. See generally, Kramer, Strength in numbers, PC week, July 22, 1986, at 57