DO YOU WANT TO KNOW A SECRET? 
WHEN THE EMPLOYEE KNOWS TOO MUCH.

Jim Hunter Birch
K&L Gates LLP
1717 Main Street, Suite 2800
Dallas, Texas 75201
214-939-5988
klgates.com
jim.birch@klgates.com

INTRODUCTION.

In the past, many employers believed that their most valuable assets--their employees and the knowledge they possessed--walked out the door at the end of each day. Given the explosion of information technology and communications advances over the past twenty years, that is more true than ever. Indeed, in light of the ubiquity of telecommuting and remote access, many workers rarely, if ever, come to the employer’s office, and key information of the employer may be stored at or accessed from the workers’ home.

The wide scale use of electronic communications and storage of information have led employers to rethink their practices of protecting confidential information through confidentiality policies and agreements, privacy policies; electronic communications policies, covenants not to compete and the pursuit of common law and statutory protections such as claims for breach of the duty of loyalty or trade secret misappropriation. However, employers and their counselors must also be careful to avoid pitfalls that can trap unwary or overzealous employers who seek to investigate and remedy perceived breaches of confidentiality and loyalty by employees. These
pitfalls can include claims from employees relating to privacy or other protected rights, claims of unfair competition, claims of interference with contract or business expectations and other common law claims under tort or contract theories. In evaluating the merits of investments in the protection of confidential, proprietary information and trade secrets, an employer should assess the information it intends to protect, identify the categories of employees to be provided with access to data and structure its policies, agreements and practices to reasonably protect the employer’s interests without unduly infringing on legitimate interests of employees and the public.

This paper is not intended to provide a survey of the law of the fifty states regarding restrictive covenants or the fiduciary duties of employees.¹ (There simply is not enough room in this paper or hours in the Saturday on which this is presented.) Rather, we hope to provide some practical pointers for employers and their counselors to consider in developing programs and policies to protect competitive, proprietary information, while pointing out some recent developments that raise concerns in the implementation and enforcement of those programs and policies.

DISCUSSION

1. Identify And Assess The Information Which Needs Protection.

Employers frequently make the mistake of trying to protect too much information under the rubric of trade secret or proprietary information. The first step in developing a program to protect trade secrets, proprietary information and competitive

¹ That job is better left to the ABA Section on Labor & Employment Law’s excellent treatises, Employee Duty of Loyalty, a State-by-State Survey (Third Ed.), Brian M. Malsberger, Editor, and Covenants Not to Compete, A State-by-State Survey (Fifth Ed.), Brian M. Malsberger, Editor.
information is a realistic assessment of which information adds value to the company by virtue of the information’s confidentiality. In the areas of trade secret protection and employee non-competition law, the concepts of value and confidentiality are crucial to determining whether information is entitled to protection. Under the Uniform Trade Secrets Act (“UTSA”) drafted by the National Conference of Commissioners on Uniform State Laws, a “trade secret” means “information, including a formula, pattern, compilation, program, device, method technique or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, an not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”

Similarly, the common law on trade secrets requires that information be both “secret” and valuable because of its secrecy in order to qualify for protection. Under both the UTSA and common law of trade secrets, the information in question must be subject to reasonable measures to preserve its secrecy. Courts refuse to extend protection to information where the owner has failed to take reasonable measures to preserve secrecy for at least three reasons: (i) the lack of effort is persuasive evidence that the alleged trade secret has no value, (ii) courts should not expend their limited resources to assist a trade secret owner which did not act reasonably to protect itself; and (iii) if the acquiring company uncovers information that the owner did not think

2 UTSA at §1(4). The UTSA, which was first promulgated in 1972 by the National Conference has been adopted in some form by at least 46 states. Milgrim, Trade Secrets at 1-57-1-60 (Matthew Bender, 2007)

was special enough to warrant protection, the trade secret law would act as a trap but for the “reasonable efforts” requirement.⁴

Likewise in the context of a confidentiality agreement or a non-competition covenant, the courts almost uniformly require that the agreement be reasonably designed to protect a “legitimate business interest” of the employer, such as trade secrets, specialize training, goodwill (either of the business or customer relationships), customer contacts, but such an agreement cannot be supported for the sole purpose of limiting competition.

While many courts have held that customer lists can be proprietary information or trade secrets, as with all information, it depends upon the nature of the list. For example, an employer who publishes a list of customers on its web site with testimonials from key contacts can hardly say that it has taken reasonable measures to protect that list. If the customer list can be readily ascertained from directories or public filings, it might not be protectable. However, in such a case, contact information relating to such customers, a compilation of particularized needs and pricing for customers, and terms of contracts with the customers may be trade secrets if they are subject to reasonable measures to preserve their confidentiality.

Many employers rely on broad definitions of “confidential information” in their policies which include almost all information that the employee could be conceivably

---

⁴ Bondpro Corp. v. Siemens Power Generation, Inc., 463 F.3d 702, 708 (7th Cir. 2006) (applying Wisconsin UTSA). See also, e.g. Delcath Systems, Inc., v. Foltz, 2007 Conn. Super. LEXIS 101, **4,16 (Conn. Super.Ct. Jan. 12, 2007) (Where employer had no policy or procedures concerning trade secrets or confidential information, and, prior to the litigation, had never asked the employee to return company information known to be on his home computer, and had disclosed information in a letter to a stockholder, the employee could not be said to have “misappropriated” a trade secret under the Connecticut UTSA.
exposed to in the course of employment. Such a broad definition might however undermine the credibility of the claimed necessity of the policy or agreement, because of its inclusion of non-confidential information with confidential information.

2. Limiting Access to Persons on a Need to Know Basis.

One technique to preserve the confidentiality of information is to limit access to it. Thus, an employer should share confidential information with or provide specialized training to only those employees who have a need to know it in order to perform their jobs. Those employees should be provided with training to help them recognize confidential information and take reasonable measures to preserve it, such as restrictions on distribution and use, passwords for electronic files, proper storage, and simply marking “Confidential” on paper copies. If identifiable confidential information is to be shared with an employee, the employer should require the employee to at least sign a non-disclosure and non-use agreement. Likewise, if confidential information is to be shared with current or prospective service providers, vendors, contractor and even customers, the employer should take steps to insure that the disclosure is limited to the information that is actually required and subject to appropriate non-disclosure or confidentiality agreements.

The decision regarding which employees have a need to know should be made based on the nature of the information and the particular employee’s duties. It would be rare for a cost accountant to need to know the secret formula for Coke®, but there may be those occasions where such a disclosure would be appropriate. The goal is to have the appropriate level of management make the decision as to what information
should be shared, with whom, and under what conditions. The absence of procedures to limit access to the information might prove fatal to a later claim that it is confidential or a trade secret. That absence, in turn, may limit the employer’s ability to restrict the use of the information by former employees in competition (either through a covenant not to compete or through an unfair competition, duty or loyalty or trade secret theory).


   a. Vetting New Employees.

       As a matter of self protection, a prudent employer should take steps to ensure that its proprietary information does not become commingled or contaminated by another employer’s information. Often, a newly hired applicant will bring forms and contact information from a prior employer. If that information is claimed as proprietary by the applicant’s former employer, the company could face the prospect of a claim for misappropriation of trade secrets, unfair competition, tortuous interference with the former employer’s contracts with the employee or worse. In addition, the former employer might claim that information developed by the employee was derived from the former employee’s information and therefore, any such information belongs to the former employer.

       In order to avoid this dilemma, the prudent employer will enact policies to ensure that employees do not bring information from a prior employer into the work environment. Those policies might include: (i) references to the policy in the pre-employment application and/or interviews; (ii) orientation on the policy upon initial employment; (iii) a statement of the employer’s expectation in any offer letter; and (iv)
if the employee is expected to sign an agreement governing confidential information (which may or may not include a covenant not to compete), a representation from the employee that he or she will not introduce a prior employer’s information into the employer’s workplace or use it in the course of employment with the company. An example of such a contractual provision might appear as follows:

(x) You represent and warrant that:

(i) You are not subject to any legal or contractual duty or agreement that would prevent or prohibit You from performing Your duties for the Company or complying with this Agreement;
(ii) You are not in breach of any legal or contractual duty or agreement, including any agreement concerning trade secrets or confidential information owned by any other party, and
(iii) You will not during Your employment with the Company, use, disclose, or reverse engineer (a) any confidential information or trade secrets of any former employer or third party, or (b) any works of authorship developed in whole or in part by You during any former employment or for any other party, unless authorized in writing by the former employer or third party.

b. Training and Communication of Policy

Employee handbooks and company policy manuals should contain policies on maintenance of confidential information. The policy should identify the types of information covered by the policy; the procedure for designating information as confidential; the company’s expectation that confidential information be used only as necessary for the company’s business and that it not be disclosed or used for other purposes; the procedures for storage, retention and destruction of confidential information; and the identity of person(s) to whom questions or issues may be referred. As mentioned above, the policy and the employer’s expectations of confidentiality and
loyalty from its employees should be communicated to employees during the orientation program and continually throughout employment. Many employers now include compliance with confidentiality policies as a performance evaluation item.

An additional way to enforce confidentiality is for the company to have a sound and enforceable conflict of interest policy and code of conduct. The risk of a disclosure of confidential information is reduced if employees are aware of potential conflicts of interest that might tempt the inadvertent or intentional disclosure of information to a competitor or other person who might derive a benefit from confidential information.

c. E-mail and Information Technology Policies.

Any program to protect a company’s information and proprietary interests must necessarily include a policy regulating its employee’s use of information technology, including e-mail, Internet access, telephone use, and now, text and instant messaging. Technology gives employees new ways to get themselves and their employers into trouble. While e-mail and Internet access present many opportunities to make companies more efficient, they also open new avenues of liability. Business problems once created in person or on paper now may happen electronically. Additionally, given the informality of e-mails, many employees are now committing errors by making e-mail statements they would never have placed upon company letter-head or put in the regular “snail-mail.” In addition, new technology permits employers to monitor employee activity in novel ways. Programs can now monitor work output, global positioning, and even keystrokes on the employee’s computer. But this increased
monitoring capability is accompanied by claims for the expansion of employee privacy rights and statutory rights to e-mail and Internet usage.

**Confidentiality—“Gone in 60 Seconds”**

In past years, employees would have to photocopy or otherwise duplicate materials in order to acquire copies of confidential information. Now, however, an employee only has to copy a file into an e-mail in order to distribute it to an almost unlimited number of recipients. An unscrupulous employee might also use remote devices such as pen drives, thumb drives or remote hard drives to save copious amounts of information and simply walk out the door with the company’s future in a backpack. Therefore, any information technology policy must take this into account and prohibit the use of such devices without the permission of an appropriate supervisor or IT Manager.

**Contract Liability**

Employees can enter into contracts with e-mail or over the Internet that may be binding on the company. This can occur on both sides of the transaction: an employee’s statements equaling a contract “acceptance” or an employee’s statements becoming a contract offer. In either event, the employee’s actions can produce a contract binding the company.

Any employee with actual or apparent authority who makes a contract offer, which is accepted, or who accepts the offer of another, has created a contract on behalf of the company. Remember that “apparent authority” does not mean that the employee is
actually authorized to enter into the contract; the test is whether the person on the other
side of the agreement was reasonable in believing that the employee was authorized.
While apparent authority is a good defense to prevent a contract involving many types
of company purchases, when a company has an official website, statements made on
the website generally have the indicia of apparent authority to bind the company
(unless the statement is clearly disclaimed as not being a “contract offer” but being a
mere request for an offer).

While statutes may limit the validity of certain non-written contracts; many cases
hold that an e-mail or Internet exchange provides sufficient “written” record to make
contracts enforceable, even in some situations that would otherwise require a writing.
Congress and some states have enacted Electronic Signature Acts to provide legal
methods of affixing a distinctive “signature” to certain e-mail transactions in order to
make them binding. These signatures, however, only serve to verify the authenticity of
the communication. Even without an electronic signature, an e-mail communication, if
proved genuine, can create a binding contract in certain instances.

Many states have adopted the Uniform Electronic Transactions Act (“UETA”),
and Congress has enacted the Electronic Signatures in Global and National Commerce
Act (the “E-Signatures Act” or “ESA”), which incorporates many of the substantive
provisions of the UETA and makes them applicable to certain transactions affecting
provide that a “Signature, contract or other record may not be denied legal effect,
validity or enforcement solely because it is in electronic form.” 15 U.S.C.A. §7001(a)(1). The ESA allows state law to supersede it if the state adopts the UETA in the form recommended by the Commissioners on Uniform State Laws. Id.

The ESA and UETA do not mandate use of electronic records by any private party, and they preserve the right of a party to insist on paper documentation. 15 U.S.C.A. §7001(b)(2). However, the ESA does not require affirmative consent, and the mere use or acceptance of electronic records and signatures should be sufficient to make them valid in most contexts. Robert A. Wittie and Jane K. Winn, Electronic Record and Signatures Under the Federal E-Sign Legislation and the UETA, 56. Bus. Law. 293, 297 (2000). Government agencies are required to accept electronic documentation submitted by parties. 15 U.S.C.A. §7001(b)(2) and Wittie, 56 Bus. Law at 300. The qualifying form of an electronic record or signature is very broad. A signature is defined as “an electronic sound, symbol or process, attached or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.” 15 U.S.C.A. §7006(5).

Courts have found that an electronic record can be as simple as an email message, and that a name attached to the bottom of an email qualifies as an electronic signature. In dicta, Judge Posner addressed the effect of the Electronic Signatures Act on the UCC’s statute of frauds in Cloud Corp. v. Hasbro, 314 F.3d 289, 295 (7th Cir. 2002). The parties had exchanged emails regarding a deal, which were then asserted as a binding contract. The contract was challenged on the grounds that it failed to meet the UCC’s requirement that contracts to be in writing and signed. In dealing with the issue
of whether the name at the bottom of an email could qualify as a signature under the UCC, Posner stated that “The Electronic Signatures in Global and National Commerce Act . . . would be conclusive in this case.” Id. The Act was not conclusive because the agreement was reached before its adoption, and as the Act is not procedural it does not apply retroactively. However, the implication of Posner’s statement is that a signed email message is an electronic record covered by the Act. Id.

A similar result as the one presumed by Judge Posner was reached In Re Cafeteria Operators, 299 B.R. 411, 418 (N.D. Tex. 2003). An alleged contract stemming from a series of emails was challenged on the basis that it failed to meet the writing requirement of the Perishable Agricultural Commodities Act. The Bankruptcy Court dismissed this challenge, holding that the issue was resolved by the passage of the Electronic Signatures Act. Despite this holding, the court found that the emails did not constitute a contract because they failed to indicate a “meeting of the minds” regarding the conclusion of negotiations. Still, the email format was not an impediment to the formation of a valid contract and the alleged agreement was addressed in the same manner as if it was written. Id.

The ESA contains several provisions limiting its application in consumer finance and consumer transactions. These provisions require the consumer’s consent to the use of electronic records for mandated consumer disclosures. 15 U.S.C.A. §7001(c)(1). The ESA also contains several exceptions to its general rule. Section 7003 of the ESA identifies several areas of contracts and records in which its general rule does not apply, including laws governing the creation and execution of wills and trust; matters relating
to family law; court documents; notices of cancellation of utility services; foreclosure and eviction notices; termination of health benefits and product recalls.

As the above discussion demonstrates, an employer should include a provision on the avoidance of e-mail contractual liability and should carefully train employees to avoid the potential of creating contractual commitments for the company through electronic communications.

**Copyright Infringement.**

Employee access to the Internet greatly increases the likelihood of copyright infringement. As in the case of personal injury, any business may be liable for copyright infringement by its employees if the infringement occurred in the course of their employment. Several organizations (e.g., the Copyright Clearance Center; the Software Publisher’s Association; and the Business Software Alliance) are very active in locating and prosecuting infringement of commercial software. These (and other) organizations have begun to turn their attentions to copyright infringement of Internet materials.

An employer should assume that virtually everything on the Internet is protected by copyright. Contrary to popular belief, it is not essential that notice of copyright is given—any original expression is entitled to protection. Furthermore, almost any use of the Internet will result in copies of materials being made. Even the downloading of images or text to the RAM of a computer is the creation of a “copy” within the meaning of the Copyright Act. Fortunately, not all copying of copyrighted material results in liability for copyright infringement. The doctrine of “fair use”
protects certain types of copying. The copyright statute describes factors to be taken into account in determining whether a particular use is a “fair use.” They include:

- The purpose and character of the use;
- The nature of the copyrighted work;
- The amount and substantiability of the portion used; and
- The effect on the potential market or value of the work.

In light of the risk of copyright infringement, not to mention the risk of downloading viruses or Trojans, an employer’s information technology policy should limit the downloading of files and programs from the Internet in the absence of approval from the head of the employer’s IT department.

**Inappropriate E-mail**

E-mail, and now text messaging, has a chatty, informal quality that creates the illusion of privacy. Messages are quickly written and deleted, seeming as fleeting as conversation. The e-mail lesson is simple, but must be repeatedly emphasized to all employees: e-mail is not confidential and does not disappear when it is deleted. Nothing should be communicated by E-mail that an employee would be embarrassed to see distributed publicly. Indeed, cases in which e-mails or text messages are cited as evidence of harassment of bias are now commonplace. Indeed, the case that is considered the groundbreaking decision in the area of e-mail and e-discovery was an employment case in which thousands of e-mails were scoured for evidence of sex discrimination. *See Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003.).
In one early case, *Daniels v. WorldComm Corp.*, Civ. 3:97-CV-0721 1998 WL 91261 (N.D. Tex. Feb 23, 1998), the court was faced with evidence of offensive e-mail that was alleged to constitute racial discrimination. In this case, the Court held that the company’s prompt remedial action to the allegations, including reprimanding the authors of the offensive e-mails and holding a training meeting regarding the company’s e-mail policy, was sufficient to prevent vicarious liability for the improper e-mails. In contrast, racist e-mails sent by employees have been held sufficient to prevent dismissal of a lawsuit. *See Owens v. Morgan Stanley & Co.*, 74 F.E.P. Cases (BNA) (S.D. N.Y. 1999). In this case prankster employees used the “old send an e-mail in someone else’s name” trick. The e-mails in question were sent in the name of an African-American employee and contained racist jokes. The hapless victim of this prank asserted that the prank and the resulting turmoil were sufficient to create a hostile work environment. The Court agreed that a possible violation existed and allowed the case to continue.

**Privacy Issues.**

Many employers have not considered the implications of monitoring employees e-mails or Internet usage. Under the theory “It’s my computer I can do anything I want to with it,” these employers have entered into a practice inspecting e-mails and making employment decisions based on the results. *See Smyth v. the Pillsbury Co.*, 914 F.Supp. 97 (E.D. Pa. 1996)(Termination of at-will employee upheld – Company can review e-mails sent on its own computer). Indeed, although there have been a few very publicized cases in this area, as of yet, these cases have not resulted in big awards for employees
whose e-mails or Internet usage has resulted in termination. Even so, based on the increasing numbers of Internet related claims, the cost of litigation alone is a sufficient basis for companies to review prophylactic measures. Government employers have an additional privacy concern under various freedom of information or Open Records Acts. E-mails may be public records of a governmental employees conduct and thus open to disclosure under those statutes. However, at least one court has held that its state’s open records law prevented the disclosure of private e-mail messages sent by a secretary to a prosecutor’s office. *Tiberino v. Spokane County*, Wash. Ct. App., No. 18830-2-III, (12/14/00).

An employer’s policy on e-mail and information technology usage should make clear that the employee should not have an expectation of privacy on information sent or stored on the employers servers or equipment, including e-mails and text messages. Indeed, there has been much commentary on a recent case from the Ninth Circuit in which the court held that an employee had an expectation of privacy with regard to text messages sent over a device paid for by his employer. *Quon v. Arch Wireless Operating Co.*, No 07-55282, 2008 WL __________ (9th Cir. 6/18/08). The *Quon* case should not be as chilling on employer monitoring of employee e-mail and messaging on company servers as some commentators have suggested. The employer in *Quon* was a city police department; therefore, its inspection of the police sergeant’s messages raised 4th Amendment and state constitutional concerns that a private employer would not face. Also, the employer in *Quon* had previously led Quon to believe that he had an
expectation of privacy by telling him that it would **not** inspect his messages if he paid the cost of the service for use over a certain level. Quon honored that commitment.

Another key aspect of the Quon case was the fact that the communications in question (text messages) were not stored on the employer’s server, but were stored on the server of the wireless communications provider, Arch Wireless. The Ninth Circuit held that Arch as a “electronic communications services” (ECS) provider, could only turn over the contents of stored communications with the consent of the sender or intended recipient under the Stored Communications Act (part of the Electronic Communications Privacy Act 18 U.S.C. Sec. 2701-2711).

However, it does appear clear that the ECPA does **not** prevent the employer from reviewing e-mails on its own e-mail system. *See Andersen Consulting L.L.P. v. Bickel & Brewer*, 991 F.Supp. 1041 (D. Ill. 1998). *See also McLaren v, Microsoft Corp.,* 1999 WL 339015 (Tex. App. – Dallas, May 28, 1999). Also, a federal court found that an employer did not violate state or federal wiretapping acts or the ECPA when it retrieved stored e-mail communications from a computer used by one of its agents, because the company did not “intercept” or access the messages sent by the agent “during transmission”. *Fraser v. Nationwide Mutual Insurance Co.,* No. 98 CV 6726 ( E.D. Pa. 3/27/01) affirmed 352 F.3d 107, 113-114 (3rd Cir 2003). The Fifth Circuit has held stored e-mail communications are exempt from the ECPA. *Steve Jackson Games v. U.S. Secret Service* 36 F.3d 457 (5th Cir. 1994). But the Ninth Circuit has found a potential violation of the Stored Communications Act portion of the ECPA where an employer accesses
communications stored on a secured and password-protected website established by one of its pilots. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879-9-880 (9th Cir., 2002).

**Employee Use of E-mail for Protected Activity.**

An employer must exercise care to ensure that its e-mail and Internet monitoring policies do not violate other employees’ rights, although current court and administrative interpretations appear to give employers reasonable latitude. For example, in *Niswander v. The Cincinnati Insurance Company*, the employer terminated Niswander after she forwarded e-mails and other files containing customer and business information to her counsel in an employment discrimination case involving an equal pay claim. The Sixth Circuit upheld the employer’s decision based upon the employee’s breach of the employer’s confidentiality policy and disclosure of customer information. Since the information was not directly related to her claims, and were provided to her counsel more as background or to refresh her memory for future deposition testimony, the Court concluded that it was not “participation” in a proceeding; rather, it was “opposition” to an employment practice which was entitled to less protection. Applying the “opposition standard the Court applied a six point balancing test to determine whether the employee was engaged in protected activity: (1) how the documents were obtained; (2) to whom the documents were produced; (3) the content of the documents, both in terms of the need to keep the information confidential and its relevance to the employee’s claim of unlawful conduct; (4) why the documents were produced, including whether the production was in direct response to a discovery request; (5) the scope of the employer’s privacy policy; and (6) the ability of the
employee to preserve the evidence in a manner that does not violate the employer privacy policy. After considering these factors, the Court concluded that the employer’s interest in the privacy of its personnel and customer records outweighed Niswander’s interests in using the records to pursue her claims. *Niswander*, No. 07-3738, 2008 WL ____ (6th Cir. 6/24/08).

An employer’s right to control access to its electronic communications systems has also been implicated in recent decisions under the National Labor Relations Act. 29 U. S. C. Sec. 150 et. seq. In *Guard Publ’g d/b/a Register-Guard*, 351 N.L.R.B. No. 70, 12/16/07 [released 12/21/07], a newspaper publisher did not violate federal labor law by maintaining a policy prohibiting employee use of the employer's e-mail system for "non-job-related solicitations" and legally enforced the policy against an employee/union president who sent two e-mails to employees urging them to support the union. Employees of *The Register-Guard*, a daily newspaper in Eugene, Ore., have no statutory right to use the publisher's e-mail system for activity protected under Section 7 of the National Labor Relations Act, a board majority consisting of Chairman Robert J. Battista and Members Peter C. Schaumber and Peter N. Kirsanow wrote. They found that an employer has a basic property right to regulate and restrict employee use of its e-mail system. The decision is dated Dec. 16, the last day of the chairman's term. Modifying the Board's previous standard for determining whether an employer discriminatorily enforced a policy against union activity, the Board majority found that that "unlawful discrimination consists of disparate treatment of activities or communications of a similar character because of their union or other Section 7-
protected status." The board adopted the analysis used by the U.S. Court of Appeals for the Seventh Circuit. "[A]n employer may draw a line between charitable solicitations and noncharitable solicitations, between solicitations of a personal nature (e.g., a car for sale) and solicitations for the commercial sale of a product (e.g., Avon products), between invitations for an organization and invitations of a personal nature, between solicitations and mere talk, and between business-related use and no-business-related use," the board said.

Finally, the Board held that the publisher did not insist on an illegal bargaining proposal explicitly banning use of the publisher's e-mail system for union business and therefore did not violate NLRA Section 8(a)(5).

In contrast to the Board’s affirmation of an employer’s right to control its e-mail systems in Register Guardian, the Board has held recently that an employer may be required to post a remedial notice under the NLRA by issuing it in an e-mail to employees, since many of the employer’s employees worked remotely. Windstream Corp. 6-CA-35483, 352 NLRB No. 68 (May 23, 2008).

d. Confidentiality and Covenant Not to Compete Agreements

Any program to protect an employer’s trade secrets or other protectable information must necessarily include consideration of the use of confidentiality agreements or non-competition agreements for appropriate employees. Again, the purpose of the paper is not to provide a state by state survey of the laws governing such agreements, but some general practice tips can be supplied.
First, analyze the legal requirements for the state in which the employee will be employed to determine the requirements for an enforceable covenant not to compete. Many states will not recognize a choice of law provision in a covenant not to compete based on public policy grounds. Where possible, the employer should explore choice of law and consent to jurisdiction provisions to help select the law and forum most favorable to the employer.

Second, in those states where a covenant must be ancillary to another enforceable agreement, define the agreement which will give rise to and support the covenant. In all other states, make sure the agreement defines the interest of the employer that gives rise to the need for the covenant.

Third, determine the type of restriction that is appropriate for the interest to be protected and the circumstance. For some types of employees and information, a simple non-disclosure agreement might suffice. Other situations may require a non-solicitation provision applicable only to certain employees or identified customers. Yet another may require an absolute prohibition against engaging in competitive activity. Finally, many employers utilize a “golden handcuff” or “claw back” approach under which an employee’s entitlement to exercise or retain options or grants of stock are tied to his or her refraining from competition.

Fourth, identify the consideration required to support the promise not to compete in the relevant jurisdiction. Is continued employment sufficient? In many states, the consideration must support the need for the covenant, such as a promise to provide confidential information or specialized training.
Fifth, reasonably identify the scope and nature of the restriction. Determine what activities need to be restrained to protect the employer’s interests without unduly affecting the public’s interest in competition. Determine the temporal and geographic limits of the covenant consistent with the needs of the business and the law of the jurisdiction. Keep in mind that many jurisdictions do not permit a court to “blue-pencil” an agreement to reform it to make it enforceable. The limitations on conduct, geography and time should not be any broader than is reasonably necessary.

Sixth, if the employee is also executing an agreement to arbitrate claims, include an exception in the arbitration clause for claims arising under the non-competition agreement. At the very least, include a proviso to permit the employer to obtain interim injunctive relief pending final resolution of any arbitration proceeding.

Finally, determine whether to include a provision identifying any stipulated or agreed relief in the agreement. Many employers find that a liquidated damage provision is as effective in deterring the employee from unfair competition as an injunction. Other potential remedies might include an accounting, stipulated injunction and/or notification of subsequent employers and customers.

CONCLUSION

As can be seen from the discussion above, employers face great challenges in protecting their confidential information and goodwill in light of technological developments. However, through perseverance and creativity, an employer can craft policies and programs to protect its reasonable interests consistent with law.