The Economic Espionage Act: Turning Fear into Compliance

by Naomi R. Fine, Esq., President, Pro-Tec Data

FEAR

We are all guilty of being curious about our competitors. We are interested to know what they do and how they do it. What are their costs? Who are their customers? Throughout your company, interest and curiosity about the competition may manifest itself in a variety of ways. Prime examples, which will be used throughout this guide, are:

- your sales people 'discover' information about competitors from customers;
- vendors share insights they've gleaned from your competitors;
- consultants use models they developed while working for your competitors;
- your market analysts target competitors to study their strategies and tactics;
- employees bring valuable information from former employers.

All of these business practices have been cause for concern in the past. Under the Economic Espionage Act of 1996, that concern may become well-founded fear.

The Economic Espionage Act of 1996 (the "EEA") makes it a federal crime to take, download, receive or possess trade secret information obtained without the owner's authorization. Trade secrets are defined to include all forms and types of financial, business, scientific, technical, economic or engineering information. If the information has been reasonably protected by the owner and has economic value from not being generally known, it meets the criteria of a trade secret under the EEA.

If an employee or contractor working for your company is suspected of having trade secret information without authorization, you could find yourself responding to an FBI raid and investigation and a federal prosecution. Anyone found to have conspired to commit the crime could face up to 15 years in prison. Your company could be fined up to $10 million. In addition, you may have to forfeit to the US government any property, such as computer equipment, used to commit or facilitate the commission of the EEA violation.

COMPLIANCE

How should we change business practice to avoid liability as federal criminals? The Federal Sentencing Guidelines provide a roadmap. The Guidelines instruct organizations to design, implement, and enforce an effective program to prevent and detect violations of law. According to the commentary to §8A1.2 of these Guidelines, "The hallmark of an effective program...is that the organization exercised due diligence in seeking to prevent and detect criminal conduct by its employees and other agents."

The official commentary to the Federal Sentencing Guidelines describe the seven minimum requirements of meeting the due diligence standard. Each of the sections below begins with the description of these requirements provided by the Federal Sentencing Guidelines. Each section then discusses the application of these requirements to the EEA.

1. Policy and Procedures

"The organization must have established compliance standards and procedures to be followed by its employees and other agents that are reasonably capable of reducing the prospect of criminal conduct."

The EEA sets out quite clearly the activities which constitute a federal offense. The statute's language can be used as a template to draft a policy and procedures tailored to your company. A general policy statement prohibiting the possession or use of trade secrets without authorization is a good start.

A company's confidential information protection or ethics policies and procedures may include this type of policy statement. However, it is a good idea to review these policies and procedures to make sure they are specific enough to be effective in preventing employees and contractors from violating the letter and spirit of the EEA. Many companies will find it in their best interest to develop a new policy and procedures devoted exclusively to avoiding liability under the EEA.

The devil is in the details. Standards or procedures that "are reasonably capable of reducing the prospect of criminal conduct" under the EEA should also provide guidelines with respect to sticky issues such as:

- the information a sales representative can 'discover' about competitors from customers;
- the insights an employee can glean from vendors who work with your competitors;
- the models your consultant developed while working for your competitors;

- the methods your market analyst uses to study your competitors' strategies and tactics;
- the information your employees' learned while working for former employers.

These guidelines will be difficult to develop because companies often do not want to deter behavior that runs the risk of violating the EEA. Gathering information from other companies is increasingly important in our hyper-competitive business environment. Companies will face conflict as they attempt to draft standards which help them both comply with the EEA and meet their business needs for competitive intelligence. (1)

The conflict is created by the gray area between legal and illegal activity. As with any law, the EEA is subject to interpretation. For example, your marketing manager might 'find' a competitor's product roll-out strategy report at a hotel conference center. If your marketing manager brings the report to your company offices, she and your company might be federal criminals. On the other hand, the same activity might be perfectly legal. The verdict will depend in part on whether the owner of the information took reasonable steps to protect the roll-out strategy report. Some would argue that if the report was marked "CONFIDENTIAL", the owner took reasonable steps to protect it. Others would argue that if the report was easily available in a public hotel conference center, the owner failed to take reasonable steps to protect it. Many would prefer to ignore the issue altogether, assuming the risks of discovery and legal repercussions are slim.

Developing standards and procedures which draw the line between what is illegal and what is desired business practice will not be easy.

2. Management Leadership

"Specific individual(s) within high-level personnel of the organization must have been assigned overall responsibility to oversee compliance with such standards and procedures."

The success of any corporate initiative depends on the support of executive staff and the leadership of management. Companies that have a confidential information protection program typically have an executive level 'champion' or sponsor of the program. Companies that have an ethics program generally have a corporate officer charged with the responsibility for overseeing the ethics and legal compliance program. These senior executives are good candidates for spearheading your company's EEA compliance program.

Compliance with the EEA may require changing both individual behavior and corporate culture. The "high-level personnel" assigned the responsibility for leading your EEA compliance program will be most effective if he or she can

influence all levels of the organization to participate actively in the program. Leadership by example is key.

3. Limit Discretion

"The organization must have used due care not to delegate substantial discretionary authority to individuals whom the organization knew, or should have known through the exercise of due diligence, had a propensity to engage in illegal activities."

Policies, standards and procedures cannot provide guidance for every situation where an employee or contractor may be at risk of violating the EEA. It would take volumes to address every potential situation in which trade secret information might be available without authorization. Therefore, at some point, a company must rely on the good judgment of its employees and agents. However, the Federal Sentencing Guidelines warn that it may not be appropriate to rely on the good judgment of our sales reps, our purchasing agents, our market analysts, and others who may have "had a propensity to engage in illegal activities" under the terms of the EEA.

To limit the discretion of those who may not know how to exercise it, your company should:

- provide clear, detailed guidelines for compliance as described above;
- designate an internal expert who can respond to questions about compliance with the EEA which may be left unanswered by the policies and procedures; and
- Require authorization for certain activities, such as receiving information about a competitor from a customer, prospect, vendor or contractor.

The additional requirements of a compliance program, described in the sections that follow, will also help to reduce the number of individuals who might otherwise have "a propensity to engage in illegal activities" under the terms of the EEA.

4. Communication and Training

"The organization must have taken steps to communicate effectively its standards and procedures to all employees and other agents, e.g., by requiring participation in training programs or by disseminating publications that explain in a practical manner what is required."

Communication is essential to changing individual behavior and corporate culture to comply with the EEA. Most companies which have an information protection or ethics program have the infrastructure in place for effective communication related to the EEA. Typically, communication includes:

- An orientation for new employees, describing the company's policy against misappropriation of trade secrets;
- Written notification to all employees of their specific responsibilities under the EEA compliance policy and procedures;
- Education and training, particularly for managers and for those employees and contractors who are most inclined to benefit from using another companies' information; and
- An ongoing reminder campaign to maintain a high level of awareness of the risks of violating the EEA.

Some companies may find it appropriate to integrate the EEA compliance program communications into their existing information protection or ethics program communications. However, for many companies, addressing the issues raised by the EEA will require separate guidelines, training programs and reminder campaigns.

5. Auditing and Reporting

"The organization must have taken reasonable steps to achieve compliance with its standards, e.g., by utilizing monitoring and auditing systems reasonably designed to detect criminal conduct by its employees and other agents and by having in place and publicizing a reporting system whereby employees and other agents could report criminal conduct by others within the organization without fear or retribution."

Your company is responsible for ensuring compliance with the policies and procedures you establish. The Federal Sentencing Guidelines suggest that your company monitor and audit operations to detect violations. Further, each employee and agent must have an easy way to report suspected violations of the EEA.

Most companies with an information protection or ethics program in place will have an audit process and an electronic or telephonic confidential hot line for reporting concerns. In most cases, the existing audit process can be expanded to audit compliance with the EEA. Similarly, the hot line can be expanded to accommodate reports and questions related to EEA compliance.

6. Enforcement and Discipline

"The standards must have been consistently enforced, through appropriate disciplinary mechanisms, including, as appropriate, discipline of individuals responsible for the failure to detect an offense. Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific."

Corporate legal departments have often expressed concern about the competitive intelligence gathering activities which may take place in various ways throughout their organizations. However, in many cases, the corporate response has been to look the other way. The risks of trade secret misappropriation claims have been outweighed by the benefit of obtaining competitive intelligence.

The EEA has tipped the scales. The risks of claims of trade secret theft are much higher than ever before and the consequences of a violation are much more severe. Your company can no longer afford to look the other way. The Federal Sentencing Guidelines dictate that individuals are responsible for both complying with the EEA and detecting offenses. Those who fail to do either must be disciplined.

7. Continuous Improvement

"After an offense has been detected, the organization must have taken all reasonable steps to respond appropriately to the offense and to prevent further similar offenses -- including any necessary modifications to its program to prevent and detect violations of law."

Your company must be prepared to take "all reasonable steps" to respond appropriately to a situation where an employee or contractor has obtained another company's information in violation of the EEA. Establishing an EEA compliance program means anticipating your company's response to any of these likely scenarios:

- a sales representative 'discovers' the contents of a proposal from your competitor to your customer;
- a vendor shares insights they've gleaned from your competitors;
- a consultant uses a model she developed while working for your competitor;
- your market analyst hires a competitive intelligence professional to interview your competitors so that your organization can study your competitors' strategies and tactics;
- your employees bring reference materials from their former employers.

Like an information protection program or ethics program, an EEA compliance program is an ongoing process. The Federal Sentencing Guidelines make clear that when violations are detected, the program must be updated to "prevent further similar offenses."

Summary

Our natural curiosity about our competitors is escalated in today's hyper-competitive business environment. Most companies have competitive intelligence activities occurring in a variety of ways throughout the organization. Under the newly enacted EEA, concern that such activity will result in criminal liability may become well-founded fear. The risks of a federal offense are high and the consequences are costly and severe.

Implementing an effective program to comply with the EEA is guaranteed to be a challenge. If your company has an information protection or ethics program, it should be reviewed and brought up to date to comply with the EEA. Many companies will choose to establish a new program focused solely on achieving the goals of an EEA compliance program.

The EEA tests the very fabric of business conduct. The EEA may require changing both individual behavior and corporate culture. The Federal Sentencing Guidelines provide a roadmap. This guide should help you navigate.

Footnote:
(1) Competitive intelligence involves gathering and analyzing information that helps companies understand their competition. Information about a competitor's capabilities and intentions provide a solid basis for improving market position and crafting strategic plans. Competitive intelligence can be obtained legally and ethically.

This article was originally published in the Society for Competitive Intelligence Professional's Competitive Intelligence Review, Vol. 8 (3), Fall1997. © John Wiley & Sons, Inc.

About the Author

Naomi Fine is an attorney and the President of Pro-Tec Data, a consulting firm dedicated to helping companies identify and protect confidential information. Pro-Tec Data develops and implements information protection programs that incorporate legal, computer security, human resources, and audit protections for information. These programs help companies avoid claims of misappropriation and liability under the Economic Espionage Act. Pro-Tec Data's clients include many of the Fortune 500. Ms. Fine has helped thousands of executives and managers incorporate information protection into their corporate vision and business objectives. She is the author of hundreds of information protection policies, procedures and standards, employee handbooks, training programs and employee communication materials. She has served as both faculty and chairperson for nationwide conferences on information protection and Economic Espionage Act compliance. Ms. Fine is a member of the American Corporate Counsel Association, the American Society for Industrial Security, the Information Systems Security Association, and the Society of Competitive Intelligence Professionals.