

# Conducting Intelligence Ethically

By Clifford C. Kalb

Executive Summary .....	2
Distinctions Between Ethical and Legal Behavior in Intelligence.....	2
Guidelines for Business Conduct.....	2
Guidelines for the Ethical Collection and Dissemination of Intelligence.....	4
Information Gathering Outside the U.S.....	4
Public Information.....	4
Information Gathering Methods.....	5
Reverse Engineering .....	5
Right to Protect Proprietary Information .....	5
Responsibility for Agents' Actions.....	5
Disclosure and Use by the Firm.....	5
Bribery .....	5
Trespass .....	5
Misrepresentation.....	6
Photographs.....	6
Questionable Information.....	6
Guidelines for the Protection of Trade Secrets and Other Intellectual Property .....	6
Intelligence Ethics: Case Histories and Commentary .....	7
Case #1—The Vendor .....	7
Case # 2 – Eavesdropping .....	8
Case #3 – The New Hire.....	9
Case #4 – The Candidate.....	10
SCIP Code of Ethics .....	11
Frequently Asked Questions .....	12
Summary/Recommendations .....	15

## Executive Summary

This article covers the distinctions between ethical and legal behavior in intelligence. It offers guidelines for codes of business conduct, for the ethical collection and dissemination of intelligence and for the protection of trade secrets and other intellectual property. Appropriate ethical behavior is reviewed in several case histories with explanatory commentary. It also provides the SCIP Code of Ethics, Frequently Asked Questions and offers recommendations for intelligence professionals regarding the ethical conduct of their work.

## Distinctions Between Ethical and Legal Behavior in Intelligence

The distinction between law and ethics is not always a clear one for the intelligence practitioner facing daily decisions in an operational context. The difference is not black or white and often falls in the ambiguous world of gray.

For the purpose of our analysis, let us keep the distinction simple:

- ***Illegal behavior*** is conduct that breaks the law. Breaking the law can trigger civil or criminal consequences for an individual or an employer. State or federal law or possibly regional or international law may be broken. Regardless of its definition in jurisdiction, behaving in a legal way, therefore, is conduct that abides by established legal parameters.
- ***Unethical behavior*** is conduct that falls short of standards set by one's profession, peers, employer or other expert sanctioning groups. For example, conduct that is not in compliance with your industry's professional association or your company's code of business conduct may be regarded as unethical. Unethical behavior may also be illegal, such as bribing a government official.

## Guidelines for Business Conduct

Most corporations, especially large multinationals, operate under a general code of business conduct. Companies may refer to these codes of conduct as "standards," "guidelines for conduct," or "business ethics." Generally, a written policy will describe a firm's expectations for its employees' business conduct.

Since each firm establishes its own code, we recommend employees become familiar with their company policy and abide by its provisions. Typically, policy documents will state the company's position on a variety of business issues and will refer the employee to their manager, a corporate

attorney, or an ethics office for clarification. A review of several corporate conduct policies reveals a significant number of common areas where appropriate behavior is outlined.

Acceptable and unacceptable “business behaviors” described in a company’s code of conduct may include relationships with vendors, investors, local community members, government agencies, several categories of clients or customers and other employees. Each of these areas may be broken down in some detail to cover the specific needs of the business and the nature of its employees’ relationships and interactions with both internal and external individuals and groups.

While some small businesses include only a few categories of guidelines for conduct, major multinational corporations have very extensive ones. The guidelines anticipate business situations that individuals working for the firm will encounter in the everyday conduct of their work. Our review of several codes has identified multiple areas where guidelines are commonly provided. These include:

- Abiding by the law
- Penalties
- Antitrust Compliance
- Political Action Committees
- Bribery
- Product Quality
- Concern for the Environment
- Protection of Company Confidential Information
- Conflicts of Interest
- Public Relations
- Fairness in Competition
- Recordkeeping Accuracy
- Gifts
- Safety
- Government Investigations
- Selection and Treatment of Vendors
- Honest Communication
- Sexual Harassment
- Trade Association Policy
- Intellectual Property Protection
- Use of Corporate Property
- Interaction with Local Community

As a firm’s business evolves and the external environment in which it competes changes as well, codes of conduct are routinely update and modified. Many firms have employees sign a document annually indicating their compliance. This practice makes employees aware of the

importance the firm places on its code of conduct. It helps to ensure compliance with modified and new aspects of the code. Within these codes, it is common to illustrate a principle of expected behavior, followed by a case in question and answer format to help the employee clearly understand the application of the principle to a common business situation.

## **Guidelines for the Ethical Collection and Dissemination of Intelligence**

With a code of conduct in place, the systematic collection, analysis and dissemination of intelligence on topics that are of critical interest and importance to a company can be conducted ethically and legally.

Within the context of general codes of business conduct, businesses with intelligence programs may choose to specify guidelines for the conduct of intelligence collection and dissemination. Since situations will emerge that cannot be fully anticipated, guidelines should refer the practitioner to consult with a more senior intelligence professional, and/or an attorney or ethics professional, if available, before undertaking a “gray zone” activity. We define a “gray zone” activity as one where the appropriate ethical behavior is unclear to the practitioner.

We reviewed several examples of multinational corporate guidelines across several industries on obtaining competitive information, and the following principles emerged:

### **Information Gathering Outside the U.S.**

Many firms conduct business on an international basis and competitors are found throughout the world. When gathering information outside the U.S., the firm’s local subsidiary should be consulted for the local rules before any information collection takes place. If the firm has a global code of conduct, it should be observed even when local practices may be different. For instance, business practices in Asia, Latin America, and parts of Europe are distinctly different from accepted U.S. standards. An intelligence professional still represents his firm when practicing in these parts of the world, and the global code should be observed.

### **Public Information**

The use of information that has been openly disclosed to the public cannot be restricted. Information in generally available publications, in public communications, or that is otherwise in public view such as an industry conference or an executive briefing to investors may be freely used and communicated.

## **Information Gathering Methods**

Professionals must not use illegal or unethical means of gathering competitive information. Contacts with competitors involving pricing, marketing strategies, customers, marketing costs or future manufacturing plans can expose a firm to liability for violating antitrust or other laws of business conduct. The gathering of competitive information must comply with such laws.

## **Reverse Engineering**

Information derived by researching back from publicly available or legitimately acquired information can be used. A competitor's product can be purchased in the open market and carefully studied.

## **Right to Protect Proprietary Information**

The professional respects the right of a competitor to have its proprietary information protected from disclosure and will not violate such rights in seeking competitive information.

## **Responsibility for Agents' Actions**

The professional may be held responsible for the behavior of agents or consultants hired by the firm to obtain competitive information, unless the firm did not authorize their actions. An agent or consultant acts as an extension of a firm's professional staff and must comply with its guidelines.

## **Disclosure and Use by the Firm**

All competitive information gathered on behalf of the firm is limited to disclosure and use for the benefit of the firm. It cannot be used for any personal benefit or disclosed to outsiders.

## **Bribery**

Firms do not use or sanction bribes for any purpose. Even some legitimate activities should be avoided because they might be misunderstood—for instance, buying lunch for a government employee after he or she has assisted you with access to public files.

## **Trespass**

It is both illegal and unethical to trespass on a competitor's property. It is permissible, however, to gather information by observation from a public property—for example, a restaurant.

## **Misrepresentation**

Always be open and honest about who you are and what you are doing. Identify yourself as a representative of your firm prior to conducting an interview. An agent of a client must identify themselves as an employee of his agency.

## **Photographs**

In general, any business operation that one can observe from public property can also be photographed from public property. However, the air above a business facility is not public property and aerial photography should generally be avoided.

## **Questionable Information**

If an employee comes into possession of information where any ethical or legal question exists regarding its use, contact an attorney or ethics professional before using or distributing the information.

## **Guidelines for the Protection of Trade Secrets and Other Intellectual Property**

Companies develop and acquire large amounts of information and make that information available to their employees. Information is an important company asset that must be protected. The loss of confidential information can be extremely damaging to a firm's competitive position.

Examples of confidential information include but are not limited to pricing formulas, research results, manufacturing methods, financial data, marketing and sales strategies and plans, engineering drawings and computer programs.

Each employee is responsible for maintaining the confidentiality of company information. This obligation continues even after one's employment with the company ends. It is generally wise to use password protection on computer files, to lock files and cabinets in the workplace, and to avoid discussion of sensitive company business in public.

**Intellectual property** generally refers to ownership rights to intangible products of the mind. Examples of intellectual property important to companies include patents, trade secrets, copyrights, and trademarks. Companies must be especially vigilant to protect their intellectual assets given the intense competition over new technology as a source of competitive advantage. Compliance programs to protect intellectual property have proliferated throughout companies. These programs heighten employee awareness of the proprietary nature of their work, which may be core company assets. The programs not only protect the intellectual property itself, but also serve to constantly educate all employees regarding the importance of protection.

**Trade secrets** are one type of intellectual property that are protected legally. Traditionally, trade secrets have been protected through confidentiality agreements. To realize protections afforded by a trade secret, the owner must demonstrate that measures were taken to protect it, including limiting its distribution, securing it, and appropriately classifying its documentation.

In 1996, The Economic Espionage Act (EEA) was passed in the U.S. It raised concern in the competitive intelligence community that its provisions would severely limit the scope of practitioners' collection activities. It became a matter of significant debate among intelligence professionals and attorneys.

After several programs were held to thoroughly review the impact on practice of intelligence and SCIP, the society of competitive intelligence professionals reached the following conclusions at the time:

- The EEA was not intended to regulate the competitive intelligence community. Rather it was primarily created to give federal authorities a federal law to investigate and prosecute cases of economic espionage conducted by foreign entities in the U.S.
- The focus of the EEA is violation of trade secret law, and the intelligence professional society's ethics code forbids activities that would violate these laws. As such, the professional standards established by the professional society are actually more restrictive than the legal standard in the act.
- The best approach to deal with individual situations involving appropriate intelligence activities is to discuss these situations with legal and ethical advisors in your individual firm and proceed using prudent business judgement and common sense.

## **Intelligence Ethics: Case Histories and Commentary**

Case history analysis serves as a pragmatic means of demonstrating appropriate ethical and legal behavior for intelligence professionals. Several case histories have been selected from a variety of carefully studied situations encountered regularly in the conduct of business intelligence. Following each case, four options for action are described, with expert commentary offered.

### **Case #1—The Vendor**

As an intelligence professional, you've decided to hire a vendor to gather information on a competitor. You're seeking very specific information about a certain product that will be

marketed next year that poses a major threat to your leading brand. Each vendor says they will follow your firm's ethics code in their work. Each proposes a different methodology for the project. Whom would you hire?

*Vendor A* would identify himself and conduct interviews with the competitor's suppliers, ex-employees and customers. He would conduct a thorough review of all secondary public literature to confirm or deny primary research results.

*Vendor B* would identify himself and indicate he was doing a benchmarking study for multiple clients. He would tell the competitor they are viewed as a "model of excellence" in planning for product launches. He would conduct interviews with the competitor's suppliers, ex-employees, customers, and current low-level employees. A minimum of secondary research is proposed.

*Vendor C* would conduct interviews with the competitor's current employees at low, medium and high levels within the firm. He would identify his study client (you) as "one of many" interested in benchmarking their firm as a "model of excellence" even though your firm is the exclusive client. No secondary research is proposed.

*Vendor D* would conduct personal interviews with current employees of the competitor and would offer compensation for providing the information. He would not volunteer the name of his agency or of the study client (you) and would not review the publicly available literature.

*Commentary Case 1, Vendor A: This is appropriate professional conduct. The vendor identifies himself and doesn't intentionally mislead. Public domain research is the cornerstone of his proposal.*

*Commentary Case 1, Vendor B: It is inappropriate to mislead intentionally, for example, by calling it a benchmarking study for multiple clients. This would be considered misrepresentation.*

*Commentary Case 1, Vendor C: As with Vendor B, it is inappropriate to misrepresent intentionally the nature of the exclusivity of the client company. However, internal employees at the competitor at any level can be interviewed if they agree under an honest and ethical introduction of study objectives and parameters.*

*Commentary Case 1, Vendor D: The provision of compensation to employees of a competitor for providing information is unethical, inappropriate, and possibly illegal. Not revealing the vendor firm's identity is misrepresentation and could violate the client's code of ethics.*

## **Case # 2 – Eavesdropping**

You are a competitive intelligence professional seated on a long airplane flight. Your neighbor opens a document entitled "Marketing Plan for Product X" which is directly competitive with one of your firm's major products. After reading a few pages he gets up to go to the restroom on the plane leaving the document on his seat. While he's gone, you should:

- A. Take the marketing plan and hide it in your bag. When he returns and asks if you saw his report, tell him you don't know what he's talking about.
- B. While he's gone, quickly take notes on the key elements of the strategy. Return the document to the exact place he left it, and don't say anything.
- C. While he's gone, ask the flight attendant to change your seat. This will avoid risk of any potential unethical behavior.
- D. Don't look at the document while he's gone. When he returns, advise him you work for a competitor and tell him if he chooses to keep reading, it is at his own risk.

*Commentary Case 2, A: Stealing a competitor's document is outright theft. It is not only unethical, but also illegal and possibly a criminal act.*

*Commentary Case 2, B: This is inappropriate professional conduct. It may be considered trespassing.*

*Commentary Case 2, C: This is the most conservative option and may be overkill. It may not be practical as another seat might not be available. However, it cannot be criticized from an ethical perspective.*

*Commentary Case 2, D: This is appropriate professional conduct. If the competitor continues to read after you've identified yourself and your firm, he has given you implied consent to observe and waived the confidentiality of his document. The competitor is behaving in an irresponsible manner by not protecting his firm's confidential materials and your subsequent behavior is acceptable.*

### **Case #3 – The New Hire**

Your firm just hired the business unit director from your leading competitor. She has worked for the competitor for 20 years and has been responsible for either overseeing or managing products directly competitive with yours. Acting as an ethical intelligence professional, you visit her on her first week on the job as the new business director at your firm. During your interview with her is it both ethical and appropriate to ask about the following?

- A. Items of a general nature regarding her knowledge of the industry and her former firm's business strategies that were a matter of public record.
- B. Specifics of her firm's business and product strategies that were not a matter of public record but had not been identified as confidential while she was employed by the competitor.
- C. Her recollection of her former firm's organizational structure, product specifications, marketing and cost structures and plans. As far as she can remember these had only occasionally been labeled confidential.

- D. Specific details of her former firm's structure, product specifications, cost, forecasts, etc. even though they had been consistently labeled as confidential or proprietary while she was employed there.

*Commentary Case 3, A: This is appropriate professional behavior both on the part of the interviewer and the new employee. All matters that had been released within the public domain can be openly discussed.*

*Commentary Case 3, B: According to the law of trade secrets, this is acceptable legal behavior by both parties, since the competitor made no effort to protect the data as a trade secret by identifying it proactively as confidential, limiting access by physically protecting it or limiting internal distribution.*

*Commentary Case 3, C: It is unethical to ask a question about something you know is protected under the law of trade secrets. It is also unethical to provide an answer to such a question when your prior firm protected the information as such, even if it was only occasionally protected by the competitor.*

*Commentary Case 3, D: Asking for, in a knowing way, or providing an answer about information that was consistently protected as a trade secret is unethical. The behavior should be avoided by both parties, as legal consequences could result.*

#### **Case #4 – The Candidate**

You are an intelligence professional doing a competitor analysis to understand a competitor's marketing and sales costs. Someone in your company sends you the resume and interview write-up of a job candidate who works for the competitor you are studying. It contains salary history, detailed organizational information, and proprietary product data. What would you do?

- A. Read the information and use it.
- B. Return it to the sender in your company with a note explaining why it is being returned.
- C. Send it to your company lawyer
- D. Shred the information

*Commentary Case 4: The scenario presents serious ethical and legal challenges. It is not unheard of for a candidate to bring proprietary materials on an interview to enhance his chances for a job.*

*It is unethical to look at or accept such material. The candidate should be sent packing, and one should consider informing his employer. This type of individual, with a clearly warped sense of morality, is dangerous for any employer. Interviewers have also been known to encourage candidates to divulge proprietary information. This, too, is, unethical. It is inevitable that conduct of this kind will become known in the marketplace and tarnish the company's reputation.*

*Appropriate job interviewing behavior examines the candidate's skills, work habits, ethical standards, and educational background to determine if they meet the needs of the employer's organization. The interviewer should focus on the value that the candidate will add to his organization.*

## **SCIP Code of Ethics**

SCIP members abide by a code of ethics established in the organization's early years. It was extensively reviewed in 1999 as its code of conduct for professional behavior. Since that time, the organization has been renamed SCIP (Strategic and Competitive Intelligence Professionals) and the code has stood the test of time:

1. To continually strive to increase recognition and respect for the profession.
2. To comply with all applicable laws, domestic and international.
3. To accurately disclose all relevant information, including one's identity and organization, prior to all interviews.
4. To fully respect all requests for confidentiality of information.
5. To avoid conflicts of interest in fulfilling one's duties.
6. To provide honest and realistic recommendations and conclusions in the execution of one's duties.
7. To promote this code of ethics within one's company, with third-party contractors and within the entire profession
8. To faithfully adhere to and abide by one's company policies, objectives and guidelines

## Frequently Asked Questions

*SCIP is indebted to the Council of CI Fellows, in particular Cliff Kalb, Dale Fehringer, Joe Goldberg, Tim Kindler, and Craig Fleisher for their creation of these FAQs. The responses were reviewed by Richard Horowitz, an expert attorney in these matters and a CI Fellow as well. Collectively this group has well over 100 years of competitive intelligence experience, and all have served in SCIP senior leadership roles.*

### **Q: What is the SCIP Code of Ethics and what does it mean?**

**A:** The SCIP Code of Ethics is a set of guidelines for ethical behavior for CI companies and practitioners which SCIP expects its members (and third parties hired by its members) to adhere to. SCIP's Code of Ethics is not a corporate policy; rather the code contains guidelines by which companies and practitioners can set their own standards along the ethical spectrum.

### **Q: The news reports discuss a private investigator researching x company. They have investigated through the standard online sources, but they also looked at files that had been discarded by the company. Is this a proper activity?**

**A:** Using confidential information that has been discarded by a competitor, regardless of how it was obtained, may raise ethical questions. Confidential information obtained in an illegal manner is a clear violation of SCIP's code of ethics. In practice, using a competitor's confidential information would violate most organizations codes of conduct. You may want to apply the "red face" test to this and similar situations; i.e., how would the company feel if this behavior was attributed to them in a newspaper?

### **Q: The Wall Street Journal etc. reports that employees frequently call their competitors and pose as a customer or a student to seek information. Is this a valid activity?**

**A:** SCIP's code of ethics expects that its members must accurately disclose all relevant information, including one's identity and organization, prior to all interviews. And, depending on the jurisdiction, misrepresentation may be illegal.

### **Q: Is mystery shopping ethical in the retail space or any space?**

**A:** As long as it complies with all applicable laws, most companies do not consider mystery shopping unethical, provided it does not violate any retailer-specific regulations (such as no photography).

**Q: What about a report of a company buying/obtaining a password to a competitor's site and researching pricing structure and offerings?**

**A:** Obtaining a password to a competitor's site without authorization, for any reason, is illegal and therefore violates SCIP's Code of Ethics. Illegal activity also violates most organizations internal code of conduct.

**Q: Can I hire private investigators for personal investigation of principals of a company?**

**A:** It is permissible and even advisable to create a business profile of the principals of competitor organizations. While this practice itself is ethical and legal, it should begin with the wealth of information that is available in the public domain; e.g., interviews, speeches, articles, etc. Using a private investigator or consultant to help uncover additional information is ethical and legal, providing they follow your firm's corporate code of conduct, the SCIP Code of Ethics, and all applicable local laws.

**Q: Can I hire a firm to tap phone calls of competitors?**

**A:** Tapping phone calls is a serious crime in many countries and is prohibited for any reason.

**Q: Can I receive confidential records at a trade show or by any other means?**

**A:** Receipt of confidential records at a trade show or by other means may raise legal questions. If such information is received, it should be turned over to your management or legal staff with an explanation of the circumstances under which it was obtained.

**Q: How does one research patents filed by competitors across an industry spectrum?**

**A:** There are a variety of patent searching services available that can be used to look for patents. Patents are public records, and as such are expected to be reviewed by competitors. This can be done yourself, or by specialists who are trained to use the services and know what they are looking for.

**Q: How does competitive intelligence differ from corporate spying?**

**A:** Competitive intelligence is the process of legally and ethically gathering and analyzing information about competitors and the industries in which they operate in order to help your organization make better decisions and reach its goals. It should be done within the ethical boundaries established by SCIP, your organization, and your personal standards. Corporate

spying often implies illegal activities, such as bribing or hiring employees to divulge confidential information.

**Q: What does it mean when firms hire former government operatives to direct their intelligence operations?**

**A:** Firms hire a former government operative because they want someone experienced in the intelligence process. Legal and ethical guidelines apply to all employees and contracted personnel, irrespective of their background.

**Q: What is the difference between corporate intelligence and business intelligence?**

**A:** Competitive intelligence is the process of legally and ethically gathering and analyzing information about competitors and the industries in which they operate in order to help your organization make better decisions and reach its goals. Corporate intelligence, business intelligence, market intelligence, and other similar terms are often used interchangeably, and any difference between them is one of semantics more than substance.

**Q: How do corporate attorneys explain competitive intelligence in their codes of conduct?**

**A:** Corporate attorneys, sometimes in combination with ethics and compliance staff, often develop a code of conduct for the overall organization. Corporate attorneys should be familiar with what competitive intelligence staff does and how they do it, and there should be a close working relationship between the competitive intelligence staff and corporate attorneys. The two groups should work together to understand the business value of competitive intelligence, and to assist with developing and updating language that appropriately balances the risks and benefits of competitive intelligence activities for the organization.

**Q: Is it permissible to post a job that you don't have any intention of filling because you know employees from competitor companies will apply, and can you apply for jobs at competitor companies that you have no intention of taking in order to learn about the competitor?**

**A:** These activities would be considered unethical by most CI practitioners and may violate your organization's code of conduct and local laws. They should be avoided.

**Q: What are the limitations regarding information you can get from newly hired employees that used to work at a competitor?**

**A:** Employees who formerly worked for competitors can be valuable sources of competitive intelligence. However, employees owe a duty of confidentiality to their former employers. Therefore, before you interview employee(s) who previously worked for a competitor, you should inform them that you do not want them to tell you confidential information about the prior employer. If an employee reveals information that appears to be confidential, do not use it and report the matter to your management or legal counsel.

## **Summary/Recommendations**

Abiding by the highest ethical standards of professional associations and your firm is your most critical overriding responsibility as an intelligence professional. As the number of practitioners in the field expands and the profession becomes more widely recognized internationally across multiple industries, and in both large and small business in the digital age, the risk of unethical behavior accelerates.

The Council of Competitive Intelligence Fellows and SCIP, experienced intelligence practitioners and academia all strive to embed these ethical principles and guidelines into the professional and educational efforts of all training programs. These groups also urge each firm to develop and periodically update ethical codes to guide behavior covering intelligence gathering and dissemination and the protection of trade secrets.

Finally, it is the responsibility of senior management of all businesses to develop, update and modify general codes of business conduct for all their employees and to educate them on expectations for appropriate business behavior as good corporate citizens.

Kalb, C. 2000. *Millennium Intelligence, Understanding and Conducting Competitive Intelligence in the Digital Age*, edited by Jerry Miller. pp. 189-201. (with adaptations)