Competitive Intelligence White Paper
Presented by 2009 Trade Secrets Committee of the Intellectual Property Owners Association
September 1, 2009

I. Introduction

This paper is presented by Gina Culbert, Carey Jordan and Chris Turoski of the 2009 Trade Secrets Committee of the Intellectual Property Owners Association. It is intended to be an overview of the legal and ethical issues involved in conducting or receiving Competitive Intelligence. The authors were not able to discern a clear and consistent set of ethical norms in connection with all of the types of competitive intelligence activities discussed here. Therefore, the authors wish to emphasize that this paper is not intended to be adopted by the IPO or anyone else as a set of standards. Rather, this paper is intended for informational use of in-house counsel and others involved in the field of competitive intelligence.

A. What is "competitive intelligence?"

1. Definition and description of industry

It does not appear that the term "Competitive Intelligence" ("CI") has a consistent or commonly accepted definition. The Society of Competitive Intelligence Professionals ("SCIP") notes that CI is: "The process of monitoring the competitive environment and analyzing the findings in the context of internal issues, for the purpose of decision support."[1] This definition emphasizes the mechanical aspect of CI. However, SCIP literature also defines CI as: "The legal and ethical collection and analysis of information regarding the capabilities, vulnerabilities and intentions of business competitors."[2] This definition emphasizes that CI should be legal and ethical.

---

[1] This definition is found on the first page of the SCIP web site at http://www.scip.org/content.cfm?itemnumber=2214&navItemNumber=492 (last visited August 27, 2008).
[2] *Id*.

CI has also been described as "a systematic and ethical program for gathering, analyzing and managing information that can affect a company's plans, decisions and operations."[3]

A recent article appearing in the Journal of Competitive Intelligence and Management concludes that the "predominance of definitions or descriptions indicates a process," and that "there is little consensus as to what constitutes this process."[4] The author concludes that CI suggests "a body of varying *practices*, as opposed to a body of practice and process; as a body of *knowing*, *a body of practicing*, or *a body of acting* rather than a body of knowledge.[5] Recently the term "Competitive Technical Intelligence" was used, meaning "CI, especially where technology is a factor."[6]

For purposes of this article, the legal and ethical aspects of CI will be emphasized, in an attempt to highlight awareness of the issues and provide broad guidance to those involved in developing or overseeing CI activities.

2. Types of CI practiced today

Modern CI is a far cry from images of clandestine eavesdropping that the term may have evoked in the past. Today, CI includes war games, data mining, technology scouting via patent tracking, patent search and analysis, SWOT (strengths, weaknesses, opportunities and threats) analysis, psychological profiles of competitor management, trade shows, professional and scientific meetings, employee interviews, Internet research

[3] Stephen H. Miller, *Competitive Intelligence – An Overview*, found at http://www.cic-web.com.br/english/ci%20overview.pdf (last visited September 2, 2008).
[4] Roberta Brody, *Issues in Defining Competitive Intelligence: An Exploration*, Journal of Competitive Intelligence and Management Vol. 4, No. 3 (2008) at 13, *also found at* http://www.scip.org/Publications/CIMArticleDetail.cfm?ItemNumber=2933 (last visited August 27, 2008).
[5] *Id*.
[6] SCIP website, agenda for New York Chapter meeting, June 11, 2007, *located at* http://www.scip.org/Publications/CIMArticleDetail.cfm?ItemNumber=2933 (last visited August 27, 2008).

(including chat rooms, MySpace and the like).[7] Many global companies have established formal CI programs, and others practice CI on an informal basis.

One means to gain competitive intelligence involves analyzing U.S. patents to forecast industry technological trends, analyze competitor technical capabilities, unearth competitor patenting strategies, and discover competitor research interests ("patent analysis"). This activity is discussed in further detail in Section D.

B. Why are competitive intelligence policies important?

Competitive benchmarking is essential to effectively compete in today's marketplace. According to a 1998 survey by The Futures Group, 82% of companies with annual revenues greater than $10 billion had an organized intelligence system, as did 60% of companies with revenues over $1 billion.[8] It is likely that even those without formal groups practice informal competitive intelligence on a daily basis. "Superior positioning requires the delivery of the highest value at the lowest cost. Achieving this position in today's global environment becomes an increasingly difficult task due to the pace and tenor of industry competition. . . . [F]irms that fail to quickly ascertain emerging opportunities and defend against rapidly materializing threats can and will find that their competitive position has quickly eroded." [9]

---

[7] For an overview of CI activities, *see* Stephen H. Miller, *Competitive Intelligence – An Overview*, found at http://www.cic-web.com.br/english/ci%20overview.pdf (last visited September 2, 2008).

[8] Miller, Stephen H. and Samuel Bentley, CI Newswatch: Microsoft, Motorola Declared "CI Eagles," (report on survey by The Futures Group), *Competitive Intelligence Magazine, 1(1), 1998, 506, cited by* Stephen H. Miller, *Competitive Intelligence – An Overview*, found at http://www.cic-web.com.br/english/ci%20overview.pdf (last visited September 2, 2008).

[9] Stephanie Hughes, "Competitive Intelligence as Competitive Advantage," *Journal of Competitive Intelligence and Management*, Vol. 3(3) (Winter 2005), found at http://www.scip.org/files/JCIM/3.3_hughes.pdf (last visited Sept. 3, 2008).

Management of risk and protection of trade secrets are an important aspect of a CI policy. A company may be at a competitive disadvantage if its employees are not aware of the types of CI practiced by its competitors and are not equipped to guard against them. Educating employees about the ways in which CI is collected can serve as an effective guard against accidental disclosure of confidential or trade secret information. Similarly, an understanding of the ethical and legal boundaries may reduce the possibility of ethical or legal line crossing, which can result in liability or costly litigation.

C. Why is ethics in competitive intelligence important?

Competitive intelligence is not industrial espionage. "By definition, industrial espionage refers to illegal activities – which range everywhere from outright theft to bribery and everywhere in between. Conversely, competitive intelligence collection is governed for the most part by adherence to corporate and professional ethics which preclude the use of illegal means to obtain information." [10] Competitive intelligence activity thus implicates both legal and ethical issues. Ethical behavior is not necessarily co-extensive with legal behavior, and in fact may be broader in the sense that strictly legal practices may be viewed in a particular industry or situation as unethical. This can increase the possibility of legal proceedings. Thus it is important for practitioners and in-house lawyers involved in CI oversight to have an understanding of the potential legal liability, and an awareness of the current ethical standards surrounding CI.

In general: "The privilege to compete with others includes a privilege to adopt their business methods, ideas or processes of manufacture. Were it otherwise, the first person in the field with a process or idea would have a monopoly which would tend to

[10] John A. Nolan, III CPP, OCP, What is Competitive Intelligence and What Can It Do To Us? found at http://www.inellpros.com/GOVpages/archives/lib/what.htm, (last visited May 31, 2007.)

prevent competition."[11] However, the privilege to compete does not extend to using improper means to do so: "It is the employment of improper means to procure the trade secret, rather than the mere copying or use, which is the basis of the liability under the rule in [Section 757]."[12]

Stepping over the legal line while engaging in CI activity could implicate the following causes of action:[13]

1. Misrepresentation.

One who fraudulently makes a misrepresentation of fact, opinion, intention or law for the purpose of inducing another to act or to refrain from action in reliance upon it is subject to liability to the other in deceit for pecuniary loss caused to him by his justifiable reliance upon the misrepresentation.[14] This includes representations that are misleading because they are incomplete. "A representation stating the truth so far as it goes but which the maker knows or believes to be materially misleading because of his failure to state additional or qualifying matter is a fraudulent misrepresentation."[15] Misrepresentation is actionable under the common law of most states.

2. Fraud.

Fraud is "a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment."[16] Thus, fraud involves the elements of scienter (knowledge), affirmative misrepresentation or omission of a material fact, and detrimental reliance. Fraud is a common law cause of action.

---

[11] Restatement (Torts) §757 (1939).
[12] Restatement (Torts) §757 (cmt. a).
[13] For an article outlining these legal principles in greater detail, *see* Craig Erlich, The Legal Perils of Misrepresentation, *in* Competitive Intelligence Ethics: Navigating the Gray Zone, (Dale Fehringer and Bonnie Hohhof, ed., Competitive Intelligence Foundation) (2006).
[14] Restatement Second (Torts) §525.
[15] Restatement (Torts) §529.
[16] Black's Law Dictionary (8th ed. 2004).

3. Criminal Fraud (mail and wire fraud).

Mail fraud involves two elements: (1) having devised or intending to devise a scheme to defraud (or to perform specified fraudulent acts), and (2) use of the mail for the purpose of executing, or attempting to execute, the scheme (or specified fraudulent acts).[17] The elements of wire fraud under Section 1343 directly parallel those of the mail fraud statute, but require the use of an interstate telephone call or electronic communication made in furtherance of the scheme.[18]

4. Economic Espionage Act.

The Economic Espionage Act ("EEA") of 1996 makes it a federal crime, subject to a fine of up to $5,000,000.00 or 10 years' imprisonment, to steal trade secrets.[19] Included in the proscribed acts is appropriating or attempting to appropriate trade secrets by artifice or deception.[20] Although the debate among CI professionals surrounding the passage of the EEA centered on the potential for increased liability stemming from CI activities, one CI industry commentator has noted that "accepted industry standards of professional ethics are more stringent than what the law allows." [21]

5. Agents' Torts.

A principal is subject to direct liability to a third party harmed by an agent's tortious conduct when the agent acts with actual authority or the principal ratifies the agent's conduct.[22] The principle can also be directly liable for negligent selection,

---

[17] 18 U.S.C. §1341. *See also* United States Attorneys' Manual, Criminal Resource Manual at 940 (found at http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00940.htm) (last visited September 3, 2008).
[18] 18 U.S.C. §1343. *See also* United States Attorneys' Manual, Criminal Resource Manual, *supra*, at 941.
[19] 18 U.S.C. §1832.
[20] 18 U.S.C. §1832(a)(1).
[21] Richard Horowitz, The Economic Espionage Act: Why the Rules Have Not Changed, *in* Competitive Intelligence Ethics: Navigating the Gray Zone.
[22] Restatement Third (Agency) § 7.03.

supervision or control of the agent.[23] A principle is vicariously liable for the torts of its employees, or an agent acting with apparent authority.[24]

6. Trade secrets misappropriation.

Most states have adopted the Uniform Trade Secrets Act (UTSA). Trade secret misappropriate is also a cause of action under the common law. The Act defines a trade secret as "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, and 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." [25]

The UTSA creates civil liability for misappropriation of trade secrets, enforceable by a private cause of action.[26] The remedies available under the Act include an injunction, damages (including exemplary damages) and in cases of bad faith or willful and malicious misappropriation, reasonable attorneys' fees.[27]

"Confidential information" is information that does not necessarily rise to the level of a trade secret, but is considered by its owner to be confidential and is not readily available in public sources. Misappropriation of confidential information can be a component of various business torts such as tortious interference with business relations, breach of fiduciary duty and unfair competition.

---

[23] *Id*.
[24] Restatement Third (Agency) sec. 7.03.
[25] Uniform Trade Secret Act §1(4).
[26] *Id*. §3.
[27] *Id*. §§2-4.

7. Other liability

In the case of competitors or companies working in a joint venture or contract relationship, CI activities could give rise to various other business torts, such as tortious interference with business relations, breach of fiduciary duty, breach of contract and the like. In addition, many states have unfair competition laws prohibiting unfair competition, and providing civil remedies such as damages and attorney fees for violation of the same.

8. Rules of Professional Conduct

In the case of in-house counsel responsible for conducting or overseeing CI activities, the Rules of Professional Conduct also may apply. Model Rule 4.1 provides: "In the course of representing a client a lawyer shall not knowingly: (a) make a false statement of material fact or law to a third person; or (b) fail to disclose a material fact to a third person when disclosure is necessary to avoid assisting a criminal or fraudulent act by a client, unless disclosure is prohibited by Rule 1.6 [relating to confidentiality of information]." Model Rule 5.3 provides:

With respect to a non-lawyer employed or retained by or associated with a lawyer:

(a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;

(b) a lawyer having direct supervisory authority over the non-lawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

D. Special considerations for patent analysis activities

Competitive patent intelligence is potentially valuable, in that it may allow a corporation to plan research efforts strategically, evaluate the strength of its patent portfolio relative to its competitors, and identify potential licensing opportunities. Moreover, through patent analysis, corporations can plan their IP strategy vis-a-vis their competitors to gain the most value from the money spent on prosecution and enforcement activity. Patent analysis can indicate how competitors' patent portfolios have evolved, demonstrate the geographical distribution of a competitor's patents, and key technological areas of pursuit. Patent analysis reports also can indicate trends or anomalies, key dynamics, such as market leaders and domestic versus international activity. Merger and acquisition, and licensing targets also may be identified.

While patent analysis is considered by some to be valuable, it can be a risky proposition because knowledge of any patents identified in the analysis may create legal duties that, if not satisfied, carry great consequences. In a patent infringement litigation, failing to satisfy these legal duties can result in a finding of willful infringement, which can result in treble damages. These findings also can support an award to an opposing party of its attorneys' fees, which can be significant in a patent case. Given these potential consequences, corporations conducting such patent analysis must be mindful of how these legal duties arise and are satisfied.

Prior caselaw imposed an affirmative duty to exercise due care to determine whether or not there was infringement. This included a duty to seek and obtain competent legal advice from counsel before the initiation of possible infringing activity.[28] An accused infringer asserting the defense of advice of counsel waived the attorney-client privilege as to the subject matter of the attorney's advice.[29] On the other hand, if the accused infringer chose not to rely on an advice of counsel defense, the jury was instructed that it could infer that the accused either did not obtain advice of counsel, or that it did so and that it was advised that its activities would infringe.[30] The determination of whether an infringer had satisfied its duty of care depended upon the "totality of the circumstances" which did not provide clear guidance as to what was acceptable conduct.[31]

Recent case law has arguably set a higher bar for the patentee seeking to prove willful infringement. In 2004, the Federal Circuit ruled that the failure to obtain an

[28] *Underwater Devices, Inc. v. Morrison-Knudsen Co.*, 717 F.2d 1380, 1389-90 (Fed. Cir. 1983).
[29] *Quantum Corp. v. Tandon Corp.*, 940 F.2d 642, 643-44 (Fed. Cir. 1991).
[30] *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565, 1580 (Fed. Cir. 1986).
[31] *Knorr-Bremse*, 383 F.3d 1337, 1342-43 (Fed. Cir. 2004)(citing *Rolls-Royce Ltd. v. GTE Valeron Corp.*, 800 F.2d 1101, 1110 (Fed. Cir. 1986)).

exculpatory opinion of counsel no longer would result in an adverse inference or evidentiary presumption that the opinion would have been unfavorable.[32] Three years later, in *In re Seagate*, the Federal Circuit tightened the burden on the patentee, holding that willfulness requires a showing of "objective recklessness." This requires a showing by the patentee, by "clear and convincing evidence, that the infringer acted despite an objectively high likelihood that its actions constituted infringement of a valid patent."[33] Under *Seagate*, once this objective threshold is met, the patentee must demonstrate that the objectively-defined risk was either known or so obvious that it should have been known by the accused infringer.[34]

The court in *Seagate* emphasized that there is "no affirmative obligation to obtain opinion of counsel."[35] While the willfulness standard was changed in that opinion, it appears that the totality of the circumstances analysis remains intact.[36] Although the *Seagate* court left application of the standard open for further development, the court mentioned in a footnote that it expected standards of commerce would be considered by the courts.[37] In a later case, the Federal Circuit observed (in *dicta*) that "legitimate defenses to infringement claims and credible invalidity arguments demonstrate the lack of an objectively high likelihood that a party took actions constituting infringement of a valid patent."[38]

These cases form the backbone of the risk analysis involved where a company investigates that patents of its competitors. There do not appear to be reported cases

[32] 383 F.3d at 1344.
[33] *In re Seagate Tech., LLC*, 497 F.3d 1360, 1371 (Fed. Cir. 2007) (en banc).
[34] *Id*. at 1371.
[35] *Id.*
[36] *See Honeywell Int'l Inc. v. Universal Avionics Sys. Corp*., 585 F. Supp. 2d 636, 641-42 (noting that a footnote in the Seagate opinion suggests that the previous factors still apply to the willfulness analysis).
[37] 497 F.3d at 1371 n.5.
[38] *Black & Decker, Inc. v. Robert Bosch Tool Corp*., 260 F. App'x 284, 291 (Fed. Cir. 2008).

involving discovery of prior art during competitive intelligence activities. In one reported decision involving an extensive pre-litigation patent analysis by the defendant, the district court noted that the evidence is more relevant to the subjective knowledge prong of the *Seagate* standard, but that such evidence also tends to show that the corporation's conduct was not objectively reckless.[39]

In sum, while competitive patent analysis may allow a corporation to monitor technological advances, developing trends, and critique competitors, serious legal risks may be created that must be managed. The Federal Circuit's stricter willful infringement standard should significantly reduce a corporation's risk in implementing a competitive patent analysis strategy, but corporations should still proceed cautiously, being careful to institute procedures and policies aimed at managing the potential risks arising from unsatisfied duties.

II. Components of an effective CI program.

Note: This information has been gathered from an examination of published and unpublished CI policies available from the Internet, publicly available sources and from non-public sources available to the committee members. It is intended only to suggest the elements of a CI program. It is not intended to state "best practices."

A. Statement of Guiding Policy

A statement of guiding policy is important to set the tone of and expectation for behavior of the company's employees or agents conducting CI. An example statement of guiding policy is as follows:

In all parts of the world, Company A is governed by Company A's Guiding Principles. The Guiding Principles serve as the foundation of Company A's shared values and

[39] *Honeywell*, 585 F. Supp. 2d at 643-44.

expected behavior of all employees. These principles are the framework for examining any problem arising in any country. Some of these Guiding Principles include:

* Company A will comply with the laws of all countries to which it is subject.

* Company A will not knowingly assist any third party to violate any law of any country, by creating false documents or any other means.

* Company A will not pay or receive bribes or participate in any other unethical, fraudulent or corrupt practice.

* Company A will always honor all business obligations that it undertakes with absolute integrity.

* Company A will keep its business records in a manner that accurately reflects the true nature of its business transactions.

* Company A managers and supervisors will be responsible that employees, consultants, and contract workers under their supervision are familiar with applicable laws and company policies and comply with them. Further, they will be responsible for preventing, detecting, and reporting any violations of law or Company A policies.

* Company A employees will not become involved in situations that create a conflict of interest between the company and the employee.

B. Guidelines for conducting CI – limits of acceptable and unacceptable activity.

The following guidelines are suggestions gleaned from examination of the code of ethics and competitive intelligence guidelines of various organizations, including those reported in the SCIP publication *Competitive Intelligence Ethics: Navigating the Gray Zone*.[40] They are not intended to be cited as "best practices," nor are they intended to be statements of legal or illegal activity or of the law. They are offered as suggested guidelines only.

[40] Dale Fehringer and Bonnie Hohhof, ed., Competitive Intelligence Foundation (2006).

1. Notify employees that they are expected to exercise good judgment consistent with the Guiding Principles. No employees will be asked or expected to compromise these standards, and doing so could be grounds for disciplinary action including termination.

2. Notify employees that they must consult with management or the legal department if they are in doubt about any action.

3. When gathering competitive information all laws, domestic and international, governing business conduct, including antitrust and trade secret laws, should be followed.

4. Competitive information may be gathered from public sources, lawful disclosures by third parties and legitimate reverse engineering. Some examples of acceptable sources are: published material and documents, court records, disclosures made by competitors obtained without subterfuge, market surveys, consultants' reports, public financial reports, broker's research brochures, trade fairs, exhibits, competitor's brochures, FOIA requests, news reports, Internet sources (except chat rooms) and the like. Obtaining samples from a competitor is acceptable unless the competitor attaches confidentiality conditions to the sample.

5. Employees may not directly or through third parties, engage in fraud, misrepresentation, bribery, theft, subterfuge, trespass, hacking or other illegal means to obtain competitive information; and may not make use of information acquired in this matter. If the legality of the method of gathering any information is in question, employees must not disseminate it and must bring it immediately to the attention of the legal department.

6. Employees may not directly or through third parties engage in the following activities: Pretexting, which involves creating false documentation (such as trade show badges), misrepresentation of who you are, or your reasons for wanting information, any other misrepresentation or omission of facts if the omission is misleading, dumpster diving, collecting competitors' materials by trickery, misprepresentation or other improper means, inducing a vendor, competitor or anyone else to give you confidential information, eavesdropping where there is an expectation of confidentiality, All of this behavior is a violation of the company's Guiding Principles.

7. Never ask a prospective hire to disclose confidential or trade secret information about their previous employer. Never ask an employee to disclose this information.

8. Do not solicit confidential information from vendors or other third parties. It is acceptable to obtain general industry information, but not specific information regarding pricing, marketing, distribution, general business strategy, sales tactics or strategy, that is not available from public sources or that the vendor is required to keep confidential.

C. Methods of educating and training employees about CI policy

The following may assist in ensuring that employees are aware of CI issues and are properly trained:

- New hire training
- Periodic employee training
- Case study and example scenarios

Example: In order to assist employees at Company A, the BCC issues periodic case studies which raise Guiding Principles issues and challenges so that employees can benefit from the experience of others dealing with such issues in their locations.

One example case study is attached as EXHIBIT A. The case study illustrates the necessity of conducting competitive intelligence through methods that are legal and ethical. The case study coaches employees that they must gather data and competitive information in a manner consistent with Company A's compliance policies which prohibit employees from engaging in illegal means to obtain competitive information.

The case study highlights that Company A is committed to being a good corporate citizen and conducting its activities in a manner that enhances its reputation. Company A's compliance policies related to gathering competitive information recognize the importance of gathering such information for the success of our business, but it is critical that gathering such information is done consistent with all laws governing business conduct, whether done by Company A or by a Company A-retained consultant. This case study illustrates the problems that will be encountered when Company A gathers competitive intelligence in a manner that is unlawful or unethical. Company A employees will not, directly or through third parties, engage in fraud, misrepresentation, bribery, subterfuge or other illegal means to obtain competitive information.

- Requiring managers to report results from CI training
- Designating legal or other department with oversight task

D. Strategies for protecting trade secrets from competitors' CI activity

- (All of the above strategies, listed in section C.)

Example: Company A also uses case studies (published by the BCC) to protect trade secrets from competitor's CI activity. One such example case study is attached as EXHIBIT B. The case study illustrates the growing trend by outsiders trying to compromise proprietary computer networks by engaging in a process called "social engineering" or "pretexting". Social Engineering is a term describing a non-technical

type of intrusion into a computer or network that relies heavily on human interaction and often involves misleading company employees to bypass the company's established security procedures.

E. Information management policies

Inside the workplace:

• Clean Desk Policy – After normal business hours and on weekends.
• Lock confidential documents in desks or cabinets.
• Turn off PC's/laptops when leaving office for extended periods of time.
• Do not share passwords – do not tape underneath keyboard/desk, or anywhere in office, or on carrying case.
• Use shredders to destroy confidential documents.
• "Dumpster Diving" – Widely used activity by business intelligence professionals.
• Be careful of giving out information over the telephone – verify/know who you are speaking with.
• Be aware of cold calls from outside "consultants" seeking information – could be business intelligence professional.
• Be suspicious of unsolicited "Market Surveys" and "Benchmarking Questionnaires".
• Be suspicious of pretext calls from "Head Hunters" seeking information on your area of expertise.
• Be suspicious of invitations to submit professional papers at upcoming conferences – many of these invitations are orchestrated by business intelligence professionals.
• Adhere to escort policy for visitors, etc.
• Challenge unescorted strangers in office.
• Do not discuss your confidential work with friends (a secret shared is no longer a secret).

Outside the workplace:

• Do not engage in conversation with strangers about your job (on airplane, in bars/waiting lounges, etc.).
• Do not lose sight of your briefcase/laptop case in airports, taxis, hotel lobbies etc.
• No I.D. (Re: Company A or your Position) on luggage, briefcase, laptop case, etc.
• Be careful/cautious at trade shows and conferences – fertile ground for business intelligence professionals.
• Be suspicious of invitations to private (restricted attendance) parties at trade shows and conferences – again, many of these functions are orchestrated by business intelligence professionals.
• Keep confidential documents in hotel safety deposit box versus leaving unattended in room (take as little as possible with you on trips).
• Be aware that faxes can be read and copied by hotel staff (always wait until fax is sent and then retrieve original).
• Be circumspect on telephone conversations from your hotel room.
• Remain alert and trust your instincts.