002 - Use of Private Investigators - Ethical & Practical Considerations

Theodore Banks
Chief Counsel & Senior Director - Global Compliance
Kraft Foods Global, Inc.

John Stephen Dzienkowski
Professor of Law
University of Texas School of Law

Dennis P. Haist
General Counsel & Secretary
The Steele Foundation

Elizabeth Wilson
SVP & Deputy General Counsel
CNA Insurance

Faculty Biographies

Theodore Banks

Theodore L. Banks is chief counsel and senior director of global compliance policy at Kraft Foods in Northfield, Illinois. His responsibilities include, among other things, risk assessment, policy development, training, and communications for Kraft's compliance program.

Throughout his legal career, Mr. Banks has been responsible for antitrust, environmental, and corporate legal matters, in addition to his current compliance responsibilities. He coordinated numerous major transactions, including the IPO of Kraft Foods.

He is the author of several legal treatises, including Distribution Law: Antitrust Principles and Practice, published by Aspen, now in its second edition, and was one of the pioneers in developing ways that in-house attorneys can use computers in their practices. Mr. Banks has written numerous articles on compliance, antitrust, and legal management topics, and co-edited the Corporate Legal Compliance Handbook, also published by Aspen. He is a frequent speaker at continuing legal education programs, where he strives not to bore the attendees too much. He currently serves as a board member of Keep Chicago Beautiful, and is president of the Chicago region of the Jewish National Fund.

Mr. Banks received a B.A. from Beloit College and is a graduate of the University of Denver College of Law.

John Stephen Dzienkowski

John S. Dzienkowski is the John S. Redditt professor of state and local government at the University of Texas School of Law in Austin. Mr. Dzienkowski teaches and writes in the areas of professional responsibility of lawyers, property, international energy transactions, and oil and gas taxation. He has delivered almost one hundred ethics presentations to law faculties, continuing legal education programs, in-house corporate departments, and large and small law firms.

Mr. Dzienkowski received the Texas Exes Faculty Teaching Award for excellence in teaching. He is a two-term member of the drafting committee for the national Multistate Professional Responsibility Examination. In the area of professional responsibility, Mr. Dzienkowski has authored or co-authored leading articles on topics related to conflicts of interest in lawyering: "Positional Conflicts of Interests," "Lawyers as Intermediaries," "Equity Investments in Clients," "Regulating Referral Fees Paid by Nonlawyers to Lawyers," and "Regulating MDPs." He is a co-author (with Ronald Rotunda) of a leading ABA sponsored treatise, *Legal Ethics: The Lawyer's Deskbook on Professional Responsibility* (updated annually).

Dennis P. Haist

Dennis P. Haist is the general counsel and secretary of The Steele Foundation, an enterprise risk management company headquartered in San Francisco, with offices across the United States, Europe, Latin America, and Asia. His responsibilities include management of the company's legal and human resources departments, worldwide legal compliance, and complex intellectual property investigations.

Prior to joining The Steele Foundation, Mr. Haist served as vice president, general counsel and secretary of Dillingham Construction Holdings, an engineering and construction company that originated in Honolulu. Earlier in his career, Mr. Haist additionally worked in the field of engineering both with Bechtel Corp. and with the U.S. Nuclear Regulatory Commission, where he gained valuable investigative and regulatory experience in connection with high-profile investigations of nuclear plant quality assurance issues.

Mr. Haist received his B.S. from the University of Michigan and is a graduate of the Golden Gate University School of Law. He also holds a Master of Laws from Santa Clara University.

Elizabeth Wilson

Elizabeth Wilson is the senior vice president and deputy general counsel of property casualty insurance operations at CAN in Chicago. In this capacity, she is responsible for overseeing and managing the property casualty legal division, which services all aspects of the North American and international operations. The support provided by her division extends from home office strategic planning to field operation's implementation covering all aspects of regulatory, compliance, contractual, and general legal advice and counsel.

Prior to joining CNA she served as in-house counsel in the food and drug industry providing legal support to parent company as well as their operating subsidiaries with over 2000 locations throughout the United States. The representation consisted of all aspects of corporate law, regulatory compliance, employment law, commercial litigation, and transactional matters. Ms. Wilson has also been in the private practice where she provided legal representation to municipal and private corporate entities in federal, state, and administrative litigation with a concentration in the areas of employment law, commercial litigation, tort defense, and real estate.

She serves on several local boards: Robert Morris College paralegal advisory board, Chicago Metro History Education Center, Chicago Mass Choir and several insurance industry guaranty fund and associations. She is a chair-qualified arbitrator with the Cook County mandatory arbitration program and a former adjunct professor at Robert Morris College.

Ms. Wilson received her B.A. from Dillard University in New Orleans and her J.D. from The Ohio State University College of Law.

SESSION 002-USE OF PRIVATE INVESTIGATORS
ETHICAL AND PRACTICAL CONSIDERATIONS

PRESENTED AT THE ACC ANNUAL MEETING
OCTOBER 29, 2007
CHICAGO, IL

Contents

1.0 INTRODUCTION

The use of private investigators was the focus of intense scrutiny by the media, state attorneys general and the Congress in 2006, resulting in new and proposed legislation to restrict investigative activity. Simultaneously, companies have been conducting internal and external investigations with growing frequency to address suspected fraud and other misconduct such as intellectual property theft, counterfeiting and piracy. The trend toward increased internal investigations is predicted to continue[1].

This paper supplements the guidance contained in the ACC's Leading Practice paper on the use of internal investigators[2] and explores the legal and ethical issues presented by the use of private investigation firms in major corporate investigations, both internal and extending outside the company. It should serve as legal counsel's basic guide to the applicable regulatory framework governing investigators and their activities including the major privacy-related laws and the ethics rules that apply to the lawyers and investigators retained by them. It also provides a comprehensive listing of practical considerations to guide counsel and others in their efforts to comply with legal and ethical obligations, proceed in a controlled and efficient manner and avoid missteps that could result in embarrassment to the Corporation.

There are often legal and ethical gray areas to be considered when planning and conducting an investigation as well as lines which should not be crossed. The complexity of applicable federal and state law mandates that a knowledgeable member of the legal team should be involved in any investigation conducted by outside investigators, whether the investigation originated within the Human Resources, Corporate Security, Internal Audit or other departments. In the case of an investigation initiated by the Audit Committee or other special committee of the Board, in-house or outside counsel should be involved.

This paper does not contain an exhaustive listing of all statutes and regulations affecting the activities of private investigators, particularly in the expanding body of privacy law at both the federal and state level. Counsel are advised to keep abreast of changes in privacy legislation and to question prospective private investigators about recent changes in the laws affecting their practice. Reputable private investigation firms will likely be members of professional associations which are involved in lawmaking and communicate regularly to their members on new developments in the law. It should be noted that private investigators are generally not as well versed in the ethical obligations of lawyers as they are in the statutes and regulations that apply to their practice.

2.0 WHAT PRIVATE INVESTIGATORS DO

There were 43,000 private investigators in the United States in 2004 with approximately 26% being self-employed.[3] Private investigation firms are called upon by a variety of corporate clients, including in-house and outside legal counsel, directors of internal audit, audit committee members, directors of corporate security, IT directors and operating managers. They are engaged for special expertise in investigations and surveillance and their abilities to access and obtain information from databases and networks of contacts, place undercover operatives and conduct transactions not traceable back to their clients.

Examples of typical investigative assignments are set forth below:

Internal

- Investigation and surveillance of employees suspected of financial fraud, theft, release of confidential information, or other misconduct in the workplace.
- Investigation of lifestyles, assets and property of employees suspected of fraud or theft.
- Placement of undercover operatives in the workplace to confirm suspicions of theft, drug use and dealing, trade secret misappropriation and other misconduct.
- Forensic examination of books, records, accounts and computers.
- Background investigations of prospective directors, officers, managers and other key employees.
- Sweeps of critical office spaces to detect the presence of "bugs."
- Surveillance and behavioral analysis of employees threatening workplace violence.

External

- Surveillance of insurance claimants' physical activities where fraud is suspected.
- Surveillance of outside individual(s) after receiving threatening communications.
- Due diligence investigations of potential joint venturers, distributors, resellers, suppliers and other strategic business partners and their principals, particularly those located overseas.
- Competitive intelligence gathering.
- Controlled purchases of counterfeit or gray-market goods or pirated intellectual property.
- Location of debtors or assets.
- Determination as to whether facilities are under surveillance by third parties (surveillance detection) and, where indicated, counter-surveillance on such parties.
- Social compliance audits of foreign manufacturers.
- Investigation of allegations of bribery, kickbacks or FCPA violations.

3.0 HOW THEY DO IT

Examples of general investigative techniques include the following:

- Use of pretext
- Open- and closed-source database mining
- Site visits
- Physical surveillance
- Technical surveillance
- Eavesdropping
- Use of "front" companies
- Use of undercover agents
- Use of contacts in law enforcement, immigration, customs, airlines, hotels, etc.
- "Dumpster diving"

4.0 REGULATION OF PRIVATE INVESTIGATORS IN THE U.S.

4.1 General. State law regulates the investigative activities that require licensing and the qualifications necessary to obtain a license. The regulatory framework governing private investigators ranges from no state licensing requirements (Alabama, Alaska, Colorado, Idaho, Mississippi, Missouri, and South Dakota) to minimal requirements to the majority of states, which have stringent regulations. Private investigators are regulated by various departments such as the Department of Consumer Affairs, Bureau of Security and Investigative Services in California, the Division of Licensing Services, Department of State in New York and the Division of Licensing, Department of Agriculture and Consumer Services in Florida. Licenses are generally valid for two years. There are websites that have collected links to state agencies and regulations, but they are not always updated on a regular basis.

4.2 Definition of a Private Investigator. The California Private Investigator Act[4] is typical of many state statutes and regulations in setting forth the definition of a Private Investigator and his or her activities as:

> …a person…who, for any consideration whatsoever engages in business or accepts employment to furnish…or agrees to make or makes, any investigation for the purpose of obtaining, information with reference to:
>
> (a) Crime or wrongs done or threatened against the United States of America or any state or territory of the United States of America.
>
> (b) The identity, habits, conduct, business, occupation, honesty, integrity, credibility, knowledge, trustworthiness, efficiency, loyalty, activity, movement, whereabouts, affiliations, associations, transactions, acts, reputation, or character of any person.
>
> (c) The location, disposition, or recovery of lost or stolen property.
>
> (d) The cause or responsibility for fires, libels, losses, accidents, or damage or injury to persons or to property.

> (e) Securing evidence to be used before any court, board, officer, or investigating committee.
>
> For the purposes of this section, a private investigator is any person, firm, company, association, partnership, or corporation acting for the purpose of investigating, obtaining, and reporting to any employer, its agent, supervisor, or manager, information concerning the employer's employees involving questions of integrity, honesty, breach of rules, or other standards of performance of job duties.[5]

4.3 Typical Qualifications and Experience. The number of years of experience, level of education and qualification process varies by state with typical requirements being:

- Applicant must be at least 18 years old (25 in New York).
- Applicant must be able to prove three years (6,000 hours) of experience in investigative work for qualified employers (5 years in Nevada).
- Applicant must pass a criminal history background check by the California Department of Justice and the FBI (in most states, convicted felons cannot be issued a license); and receive a qualifying score on a two-hour written examination covering laws and regulations. There are additional requirements for a firearms permit.
- A college degree in criminal law, criminal justice or police science can usually be applied toward part of the experience requirements.

4.4 Other Requirements. Many states require the private investigation firm to provide a bond and a certificate of general liability insurance. The surety bond penal sums vary from $2,500 to $10,000 and the general liability insurance limit is typically $100,000 each occurrence, $300,000 aggregate. Evidence of workers' compensation insurance can also be required.

4.5 Exemptions. Many states exempt attorneys from the licensing requirements for private investigators. In California, the requirements for licensing as a private investigator do not apply to an attorney when performing his or her duties as an attorney-at-law. Also exempted are employees employed exclusively and regularly by an employer, insurance carriers, agents, brokers and adjusters, and peace officers who are "off duty" and privately employed.[6]

4.6 Unlicensed Investigators. In California, any person who violates any provision of the licensing statute is guilty of a misdemeanor punishable by a fine of $5,000 and/or imprisonment for up to one year. The same punishments apply to anyone who conspires with another person to violate any provision of the licensing statute or anyone who knowingly engages a nonexempt unlicensed investigator.[7] Any person who acts as or represents himself or herself to be a private investigator when that person is not licensed is guilty of a misdemeanor punishable by a fine of $10,000 and/or imprisonment for up to one year.[8]

5.0 PROHIBITED PRACTICES

5.1 State Prohibited Practices

5.1.1 Private Investigator Statutes and Regulations. Once again, prohibited practices under state law vary, but there are some typical practices such as:

- Divulging any information acquired to anyone other than the investigator's client (and law enforcement if the information relates to a criminal offense).
- Making false reports to his or her client.
- Using a badge, uniform, identification card or making a statement with the intent of giving the impression that one is connected with the federal or state government.
- Entering a private building without permission.
- Using a fictitious business name without the agency's approval.

California's Private Investigator Statute also contains a prohibition on "any act constituting dishonesty or fraud."[9] This prohibition has been broadly interpreted by the Bureau of Security and Investigative Services and affirmed by a California Court of Appeal in the case of *Wayne v. Bureau of Private Investigators and Adjusters*.[10]

In *Wayne*, a private investigator visited several witnesses and obtained statements about auto accidents after representing himself as an investigator assigned to check out the accident and with knowledge that his client was adverse to the witnesses being contracted. The trial court found that the essence of the fraud and dishonesty was that the investigator did not disclose that he was acting on behalf of an adverse party. The trial court also noted that the investigator did not actively misrepresent that he was from an interviewee's insurer. In considering whether there was "dishonesty", the trial court commented that the term "seems to be incapable of exact definition or precise limitation because among other things of the infinite variety of circumstances which affect the relations and affairs of mankind in our society". The court stated that the investigator "did not act entirely in good faith with the persons he interviewed", "knew that the interviewees wanted in fact to know whom he represented", "knew that he did not tell the interviewees the whole truth about whom in fact he represented" and "knew from what he told the interviewees that they were mistakenly of the belief that in some capacity or way he was connected or associated with those whose interests were with the interviewees". The trial court characterized the investigator's activity as "not a simple or casual omission to tell the exact and whole truth on a single occasion, but …a studied course deliberately to mislead the unwary …." In considering the fraud question, the trial court stated that "Fraud embraces multifarious means whereby one person gains an advantage over another and means in effect bad faith, dishonesty or overreaching". The court focused on the admission by the investigator that he refused to give any answers to the questions put to him by the interviewees with reference to whom he represented (he merely answered their questions by stating that he was an independent investigator assigned to check out the accident).

The holding in *Wayne* has not only been cited in other cases, but the liability of the investigator has been extended to damages to the person whose privacy has been invaded[11] and those retaining the investigator may also be vicariously liable for the intentional torts of the investigator.[12] Corporations and their attorneys may also have liability based upon negligent supervision or negligent entrustment theories.[13] This case and those which extend the interpretation of acts constituting "dishonesty and fraud" should raise concerns about the legality in California of many investigative techniques commonly used by investigators, such as using pretext to obtain information not specifically prohibited, the placement of undercover investigators in workplaces and "controlled buys" of counterfeit, gray market or pirated goods. However, the facts in these cases need to be carefully considered since the courts have not ruled that *any* use of subterfuge by a private investigator constitutes dishonesty and fraud and the decision in *Wayne* dates back to 1962. Moreover, the California legislature was unable to pass broad anti-pretexting legislation as discussed below. It should also be noted that California's definition of "Dishonesty or Fraud" has also recently been broadened to include failure to provide for workers' compensation insurance or carry out the obligations imposed by the Unemployment Insurance Act.[14] Decisions or administrative rulings which similarly restrict investigation activities or techniques may exist in other states.

5.1.2 State Privacy Laws. In California, a plaintiff claiming violation of his or her privacy rights may bring claims under (i) the California Constitution; (ii) California's Privacy Act; and (iii) the common law tort of intrusion.

The California Privacy Act[15] outlaws secret wiretapping, eavesdropping, and recording of confidential communications without consent and any violation of this law also constitutes a violation of the Private Investigator Act. There are other invasion of privacy laws that may impede an investigator's activities, such as California's anti-paparazzi and anti-stalking laws.[16] California also has enacted anti-spyware legislation, which became effective on January 1, 2005.[17] The Act makes it illegal to knowingly or willfully cause the installation of software on a California end user's computer with the intent of using the software for "wrongful" purposes. Wrongful purposes include collecting personal information through intentionally deceptive means.

5.1.3 State Unfair Competition Laws. It is likely that a licensing violation by a private investigator would constitute an "unlawful…business act or practice" under California's Unfair Competition Law.[18] The law broadly prohibits "untrue or misleading" statements and provides punishments of six months' imprisonment and fines of $2,500. Private parties are afforded the remedies of equitable relief, including an injunction and restitution.

5.1.4 State Anti-Pretexting Laws. Pretexting is often used to describe the obtaining of telephone call records by fraudulent means but the term has a much broader meaning to private investigators. Pretexting is a technique used by investigators to obtain information through the use of a false identity, a false pretext or a "cover story". The

technique is used in cases involving lost or abducted children, identity theft, intellectual property theft and a wide variety of fraud cases.

As of March 2007, at least 15 states[19] had laws in place which prohibit pretexting for phone call record information. California enacted Senate Bill 202 in September 2006.[20] New York enacted its Consumer Communication Records Privacy Act the same month.[21] California's bill generally bans the use of deceit to obtain telephone call records and violations carry a fine of up to $2,500 for the first conviction and/or imprisonment for up to one year.[22] Under the California law, personal information obtained during violation of the law is inadmissible as evidence in any judicial or other proceeding except a proceeding involving violation of the law itself. A broader anti-pretexting bill that would have barred investigators from making "false, fictitious or fraudulent" statements or representations to obtain private information about an individual, including telephone calling records, Social Security numbers and financial information, failed to pass the California Assembly after determined lobbying by the motion picture industry, which argued that the broader bill would hinder piracy investigations.

5.2 Federal Prohibited Practices. Prohibited practices potentially impacting the activities of private investigators can be found in a variety of federal laws and regulations -- many of them fairly recently enacted and focused on privacy. The major statutes impacting the activities of private investigators are discussed below, but this listing is not exhaustive. For example, the Social Security Act prohibits misrepresentations that a person holds a social security number for any purpose.[23] Also, access to certain databases are restricted to law enforcement, for example the National Crime Information Center (NCIC) database.

5.2.1 Pretexting. Following hearings on the use of pretext to obtain telephone records in the Hewlett-Packard case, the Congress passed and the President on January 12, 2007 signed into law HR 4709, the "Telephone Records and Privacy Protection Act of 2006" which amended Title 18, United States Code, to prohibit the obtaining, in interstate *or foreign commerce*, of confidential phone records information from a telecommunications carrier or VoIP service provider ("covered entity") by: (1) making false or fraudulent statements to an employee of a covered entity; (2) providing false or fraudulent documents to a covered entity; or (3) accessing customer accounts of a covered entity through the Internet or by fraudulent computer-related activities without prior authorization.[24] This law also prohibits the sale or transfer of confidential phone record information and the purchase or receipt of confidential phone record information. Violations include a fine and/or imprisonment for up to ten years. There are enhanced penalties if a violation occurs while a person is violating another law, if the violation is part of a pattern of illegal activity or if the information obtained is used in furtherance of certain criminal activities. The Act provides for extraterritorial jurisdiction over offenses.

5.2.2 Other Privacy-Related Laws. A variety of other privacy-related federal law restricts how private investigation firms go about gathering information.

5.2.2.1 Gramm-Leach-Bliley Act ("G-L-B"). Title V of The Gramm-Leach-Bliley Act contains prohibitions on the disclosure of nonpublic person information and fraudulent access to financial information. Section 521 of the Act specifically prohibits obtaining customer financial information by making a false, fictitious, or fraudulent statement or representation to a financial institution or a customer of a financial institution or by presenting any document to a financial institution with knowledge that it is forged, counterfeit, lost or stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation.[25]

5.2.2.2 Fair Credit Reporting Act ("FCRA"). The FCRA regulates the activities of credit reporting agencies, those who furnish information to the credit reporting agencies and businesses who are users of credit reports.[26] Private investigation firms are required to certify the purpose for which the report is being obtained and that the report will not be used for any other purpose. If written instructions granting authorization are not obtained or the purpose is not associated with the extension of credit or employment purposes, then pulling a credit report on an individual is not permissible. For example, pulling the credit report of an individual to obtain information useful in litigation is not a permissible purpose under FCRA. Prior to December 2003, the FTC held the opinion that an investigation of employee misconduct constituted an "investigative consumer report" entitling the employee to all rights under FCRA, including prior consent and the furnishing of a copy of any report (oral and written) if the report resulted in an "adverse" personnel action. If a private investigation firm was retained to furnish the report, the firm would be a consumer reporting agency under FCRA. On December 4, 2003, the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") was signed into law.[27] FACTA amended the FCRA to exclude from the definition of consumer reports misconduct investigation reports and investigation reports into "compliance with Federal, State or local laws and regulations, the rules of a self-regulatory organization, or any preexisting written polices of the employer." It is important to note that only investigations of misconduct *related to the employment* are excluded from the definition of a consumer report and violation of an employer policy is only excluded if the policy *predates* and investigation and is in *writing*. Employers "negligent in failing to comply" with FCRA requirements are liable to an applicant or employee for actual damages, costs of a suit, and attorney's fees. In addition, an employer's "willful noncompliance," may result in punitive damages. Criminal penalties also may be imposed if a person obtains a credit report under false pretenses. In a recent case, the Supreme Court held that for a violation of FCRA to be willful, it must have been committed knowingly and recklessly.[28]

5.2.2.3 Electronic Communications Privacy Act ("ECPA"). The ECPA prohibits the interception of e-mail transmissions by unauthorized individuals or individuals working for a government entity but acting without a proper warrant.[29] The focus of the ECPA is unauthorized access by employees or corporate competitors seeking competitive intelligence.

5.2.2.4 Stored Communications Act. The Stored Communications Act prohibits intentional unauthorized access to a facility through which an electronic communication

service is provided or exceeding an authorization to access the facility.[30] Fines and imprisonment ranging from one year for a first offense to ten years for repeat offenses committed for the purpose of commercial advantage and certain other purposes. Civil actions by a subscriber, provider or anyone else who was aggrieved are also authorized.

5.2.2.5 Drivers Privacy Protection Act ("DPPA"). The DPPA generally prohibits a State department of motor vehicles and its employees and contractors, from disclosing any personal information about any individual obtained by such department.[31] The DPPA specifically permits disclosure of personal information for use by licensed private investigative agencies or licensed security services for any of the purposes permitted under the Act. These permissible uses include verification of information submitted by an individual (such as an employment application or background questionnaire) and use in connection with any civil, criminal, administrative or arbitral proceeding, including investigation in anticipation of litigation and the execution or enforcement of judgments. The DPPA also prohibits the making of a false representation to obtain any personal information from an individual's motor vehicle record.[32] Penalties authorized for violation of the DPPA include a criminal fine and civil liability, including punitive damages.

5.2.2.6 FTC Act. The Federal Trade Commission has authority, separate from the G-L-B Act to investigate and bring actions for unfair and deceptive practices under Section 5 of the FTC Act and has used this authority to prosecute pretexting cases involving consumer phone records.[33]

5.2.2.7 The 1996 Health Insurance Portability and Accountability Act ("HIPAA")[34] HIPAA established, among other things, mandatory rules governing the privacy of all patient identifiable health information (also referred to as "protected health information" or "PHI"), regardless of form. In response to a mandate in HIPAA, the Department of Health and Human Services issued regulations entitled *Standards for Privacy of Individually Identifiable Health Information*. For most covered entities, compliance with these regulations, known as the Privacy Rule, was required as of April 14, 2003. Covered entities are health plans, health care clearinghouses, and health care providers that transmit health information electronically in connection with certain defined HIPAA transactions, such as claims or eligibility inquiries. The Privacy Rule also permits disclosures to business associates. Business associates are persons or entities that perform certain functions or services on behalf of the covered entity that require the use or disclosure of PHI, provided certain arrangements to safeguard the PHI are in place between the covered entity and the business associates.

PHI may be disclosed only under conditions permitted by the regulations, including, for example, reasonable belief that use or disclosure will avert a health hazard or to respond to a threat to public safety, including an imminent crime against another person.[35] Investigators may violate the Privacy Rule if accessing PHI without a permissible reason.

5.2.3 Economic Espionage Act of 1996 ("EEA"). The Economic Espionage Act of 1996[36] contains a provision making criminal the theft of trade secrets carried out for purely economic or commercial advantage.[37] The penalties to individuals for theft of trade secrets under §1832 can be imprisonment for up to ten years and a fine of $250,000. Organizations can be fined up to $5 million. The Act also covers attempts and conspiracies to violate the EEA and, importantly, the government does not have to prove the existence of a trade secret, only that the defendant sought to acquire information that he or she believed to be a trade secret, regardless of whether the information actually met the definition of a trade secret under the EEA.[38] The definition of a trade secret under the EEA is very broad and includes, generally, all types of information, however stored or maintained, which the owner has taken reasonable measures to keep secret and which has independent economic value.[39] In light of the significant criminal exposure faced by individuals and corporations under this act, retention of a private investigation firm to conduct competitive intelligence gathering should only occur with the knowledge and approval of in house counsel and senior management with the investigator's activities closely prescribed. Sample guidelines for obtaining competitive intelligence are contained in Appendix IV.

6.0 OVERSEAS INVESTIGATIONS

Companies operating outside of the United States are very likely to be using the services of local private investigators either by engaging them directly of indirectly through a U.S. private investigation firm or U.S. or foreign law firm. In addition to fraud investigations within foreign subsidiaries, foreign investigation firms are often retained to conduct due diligence on prospective potential partners, investors, distributors and manufacturers and to respond to hotline tips on issues such as kickbacks and Foreign Corrupt Practices Act violations. Another major issue in which foreign investigators are active and can be useful is counterfeiting and piracy. Set forth below are brief descriptions of the status of regulation of investigators in major foreign markets.

6.1 China. The only entities that may legally conduct "investigations" in China are law enforcement agencies, predominantly the Public Security Bureau ("PSB"). There are other agencies that conduct investigations, but they coordinate with the PSB since it controls most of the records and files of everyone living and working in, or traveling to China. Executive Order No. 421[40] mandated that all corporations establish a dedicated Security Department with management and personnel having the requisite experience to carry out security and investigative tasks. Therefore, a proprietary corporate security department can also legally conduct investigations whether they involve internal or external threats. Executive Order 421 requires that once initial evidence developed during the investigation points to a potential criminal case, it must be reported to the PSB. In China, there are private investigative firms in virtually every municipality and city, but they usually operate under business licenses that state that their business is "market research." Although the PSB keeps a close watch on private investigation firms, they are more often than not owned and managed by former police officers.

There are only a handful of foreign risk management consultancies having business licenses stating "Market Investigation and Research." These licenses were issued years ago, but the Chinese government stopped issuing any business licenses that contain the word "Investigation" shortly after those first licenses were issued.

Given the above, China does not have a licensing process or regulations for private investigators or private investigation firms.

6.2 Hong Kong. Private investigators are not required to be licensed in Hong Kong and they are generally unregulated. The general rule in Hong Kong and Singapore is that if information is not publicly or commercially available in the open market, it is illegal to obtain the information.

6.3 Singapore. Private Investigators are required to be registered with the government and to have "close ties" to the Singapore Police.

6.4 Mexico. Private investigations in Mexico are illegal. Under Mexican law, investigations can only be conducted by law enforcement agencies. However, the federal and state laws for public safety consider certain "investigations services" as one of the services that Private Security Companies can conduct in Mexico. These "investigation services" include verification of information (partial backgrounds) and location of persons. Private security companies are required to be licensed and report to law enforcement agencies any criminal activity they uncover. Notwithstanding the limits placed upon them, private security companies and other companies that provide "investigation services" conduct all types of investigations, including obtaining information from criminal and tax records from various sources.

If the intention of conducting an investigation is to prosecute, the company that engages investigative services must keep in mind that information gathered during the investigation cannot be presented before the authorities as evidence, since it was not legally obtained; in these cases the attorney representing the prosecuting company provides the "investigating prosecutors" (Ministerios Publico) with the information that has been gathered to support the prosecution.

The laws of other Latin American countries, e.g., Brazil and Argentina, are similar to Mexico in that private investigators are not legal and investigations must be conducted by the authorities.

In house counsel should consider the risk associated with retention of a private security company to obtain information form records which are not public, including criminal, tax, financial and banking information, since the private security company may be using illegal means to obtain the information and may not be able to keep their sources confidential.

6.5 India. There currently are no laws regulating or providing for the licensing of private investigators but the possibility is under consideration at the central government level.

There are no laws prohibiting private investigations in India and courts are generally not concerned about the methods with which evidence was obtained. There are no centralized databases on individuals similar to those found in Western countries. For example, criminal records can be verified only at the local police station that has or had jurisdiction over the residential address(es) of the subject. If a subject has lived in numerous locations and had multiple employers, the task can be quite time consuming and should not be considered as "fool proof".

6.6 United Kingdom. The United Kingdom currently does not license private investigators but is considering legislation to require licensing; the government is having difficulty defining an "investigator". Nonetheless, there are many private investigation firms and they are largely unregulated.

The Data Protection Act[41] ("DPA") is considered by most investigators to be a serious source of liability and a major obstacle to obtaining information due to the restrictions placed on Data Controllers. The Act applies to "personal data" concerning identifiable living individuals. Data can be in paper or electronic form and must be handled in accordance with eight principles. The eight principles require that data must be:

- Fairly and lawfully processed;
- Processed for limited purposes and not in any manner incompatible with those purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than is necessary;
- Processed in line with the data subject's rights;
- Secure; and
- Not transferred to countries without adequate protection.

Processing may only be carried out where one of the following conditions has been met:

- The individual has given his or her consent to the processing;
- The processing is necessary for the performance of a contract with the individual;
- The processing is required under a legal obligation;
- The processing is necessary to protect the vital interests of the individual;
- The processing is necessary to carry out public functions; or
- The processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

The Information Commissioner is an independent body which enforces the Data Protection Act. The Information Commissioner has expressed the opinion that a private investigator is a Data Controller, which imposes significantly more responsibility and direct liability to a Data Subject under the DPA than if an investigator were to be deemed a Data Processor.

It is a criminal offense under the DPA to obtain information by deception ("Blagging") and investigators who violate the DPA by obtaining data "unfairly and unlawfully" face unlimited fines and imprisonment.

6.7 Middle East. Most of the Middle East should be considered a very risky environment to conduct investigations. Investigators generally advertise themselves as researchers and any investigation which could involve a royal family member could result in imprisonment for the investigator.

6.8 Russia. Private investigators are required to be licensed in Russia and there are laws protecting some personal data as well as laws that prohibit wiretapping. The use of "front companies" and undercover operatives in investigations is not specifically prohibited.

7.0 ETHICAL CONSIDERATIONS

7.1 ABA Model Rules 4.1 and 8.4(c). ABA Model Rule 4.1 prohibits a lawyer from knowingly making a false statement of material fact or law to a third person or from failing 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.

Model Rule 8.4(c) defines engaging in conduct involving dishonesty, fraud, deceit or misrepresentation as professional misconduct.

The ABA has considered the act of secretly but lawfully recording a conversation without the knowledge of the other party and found such conduct not to be deceitful and in violation of the Model Rules.[42] The opinion specifically did not address the issue of lawyers involved in deceitful but otherwise lawful conduct involving nonconsensual recording of conversations relating to criminal activity, discriminatory practices and trademark infringement.

The Utah State Bar has opined that the participation by a government lawyer in a lawful covert governmental operation that entails conduct employing dishonesty, fraud, misrepresentation or deceit for the purpose of gathering relevant information does not, without more, violate Utah's Rules of Professional Conduct.[43]

A few cases have addressed the use of pretext and similar deceptive practices and determined they were not in violation of the ethical rules. In *Apple Corps Ltd. v. International Collectors Society* a New Jersey court considered the actions of undercover investigators posing as customers to gather evidence of violations of a consent decree in a trademark infringement case.[44] The court found that Rule 8.4 (c) did not cover misrepresentations only of identity or purpose while gathering evidence and noted that courts, ethics committees and grievance committees do not condemn

such activity by undercover agents in criminal cases or by discrimination testers in civil cases.[45] The court also found that Rule 8.4 (c) should be interpreted in conjunction with Rule 4.1, which prohibits misrepresentations of material fact. The court concluded that only grave misconduct should be the target of Rule 8.4(c).

A New York case, *Gidatex, S.r.L. v. Campaniello Imports, Ltd.,* considered the activities of investigators seeking evidence of trademark infringement by secretly tape recording conversations with the salespeople of a terminated distributor in light of New York's version of Model Rule 8.4(c).[46] The court ruled that the purpose of New York's rule was to prevent parties from being tricked and that there was no violation of the rule because the investigators did not interview the salespersons or trick them into making statements they would not otherwise have made as part of the transaction.

A case which disapproved misrepresentation and contact with unrepresented parties is *Upjohn Co. v. Aetna Casualty and Surety Co*.[47] In *Upjohn*, investigators representing the defendant interviewed former employees of the plaintiff without identifying themselves as agents of defense counsel. The court stated that under Michigan's rules governing contact with unrepresented people, if the lawyer knows or should know that an unrepresented person misunderstands the lawyer's role in the matter, the lawyer is required to make "reasonable efforts to correct the misunderstanding." The court found that it was improper for investigators retained by counsel to misrepresent their identity or purpose in gathering information.

Other trademark related cases allowed evidence gathered under pretext but do not specifically address whether the ethical rules were violated.[48]

7.2 ABA Model Rule 4.2. ABA Model Rule 4.2 generally prohibits a lawyer from communicating about the subject of representation with a person the lawyer knows to be represented by another lawyer in the matter without consent of the person's lawyer. Some variation exists at the state level with regard to the definition of a represented party. While the Model Rule's definition appears to be very broad, some states such as New Jersey and Ohio have addressed the "represented" person for organizations. The Ohio rule prohibits communications with a constituent of the organization who supervises, directs or regularly consults with the organization's lawyer concerning the matter or who has authority to obligate the organization with respect to the matter or whose act or omission in connection with the matter may be imputed to the organization for purposes of civil or criminal liability. New Jersey's rule appears to limit the represented person for organizations to the litigation control group. In states that have adopted the Model Rule without modification, contact with even lower level employees who are directly involved in the matter that is the subject of representation could result in a violation of Rule 4.2 and the preclusion of evidence obtained through such contact.

Rule 2-100 of the California Rules of Professional Conduct prohibits a lawyer from "directly or indirectly" communicating "about the subject of the representation" with a party represented by another lawyer. If in-house or outside counsel is aware that another party is represented by counsel, retaining an investigator to communicate with

such party would be a violation of Rule 2-100. No violation of Rule 2-100 was found when a plaintiff's lawyer hired an investigator to interview a corporation's employees seven months before the plaintiff sued the corporation.[49] However, the court commented that a close question would have been presented had the investigator conducted the interviews on the eve of the filing of the lawsuit.[50]

The foregoing Model Rules apply to lawyers and any non-lawyers working directly for that lawyer.[51]

8.0 PRACTICAL CONSIDERATIONS

Outside counsel should consult the following checklist of considerations when planning investigations, retaining an investigation firm and conducting investigations in order to comply with legal and ethical obligations, conduct the investigation in a controlled and efficient manner and avoid missteps that could result in embarrassment to the corporation.

8.1 Initial Investigation Planning.

- Determine whether a trained investigator is needed (expertise, geography, contacts, relationships with law enforcement, etc.).
- Determine the information needed and its criticality.
- Determine the sensitivity of the investigation and whether or not the appropriate individuals and internal departments are involved.
- Determine an initial investigative strategy, keeping in mind the importance of the investigation and narrowly tailoring the investigation.

8.2. Before Retaining an Investigator.

- Determine whether to hire a law firm or private investigation firm.
- Determine whether an investigation firm should be retained by outside counsel.
- Obtain referrals of reputable investigation firms from colleagues, outside counsel or other sources such as AUSA's, Deputy AG's and District Attorneys.
- Confirm the firm's reputation for legal and ethical behavior.
- Confirm expertise in the desired field and geography of investigation.
- In the case of foreign investigators, confirm language abilities.
- Confirm the investigation firm's licensing status (including any license violations or suspensions) and the licensing status of proposed subcontractors. Understand what happens if the investigation crosses state lines. Some states grant limited reciprocity to out-of-state firms.
- Determine whether the investigation firm belongs to a professional association with a code of conduct or whether it follows its own code of conduct.[52]

- Seek references and check them.
- Confirm that no conflicts of interest exist.
- Have the investigator review and agree to comply with your company's Code of Business Conduct or specialized investigations guidance.
- Execute a non-disclosure agreement if you intend to share confidential information or work product with the investigation firm prior to formally engaging it.
- Conduct a face-to-face interview with the principal investigator, outlining the information sought or activities to be engaged in and oversight expectations.
- Review the initial investigative strategy with the investigator to confirm objectives, likelihood of success and compliance with law.
- Confirm the ethical limitations in your state and ensure that the investigator understands them.
- Do your due diligence before engaging investigators in countries where "investigations" are prohibited to ensure that the information gathering or "market research" will be conducted in compliance with national or local laws and police requirements.
- Determine if the firm will need to use independent contractors and, if so, where and for what activities.
- Develop a phased approach to the investigation, if appropriate.
- Determine whether investigators carry firearms. The presence of firearms generally should be considered to increase risk.

8.3. Retaining the Investigator.

- Retain the Investigation Firm under a Professional Services Agreement or detailed Engagement Letter which includes the following:
  - Scope of services, timeline and not-to-exceed budget, by phase.
  - Identity of lead investigator and other key individuals.
  - Protection of confidential information provided to the investigator and developed by the investigator; work product doctrine.
  - Representations and warranties relating to licensing, compliance with law, performance to best industry practices, compliance with client company's Code of Business Conduct and confidentiality.
  - No subcontracting without Client's express approval.
  - Indemnification.
  - Insurance (general liability, automobile, worker's compensation, errors and omissions).
  - Report form and frequency (oral and written)
  - Deliverables (reports, surveillance logs, photos, data, etc.).
- Clearly communicate expectations and boundaries to avoid surprises.

- Remember a lawyer's duty to inquire about the proposed sources of information and legality of techniques and be wary of an investigator's refusal to explain them.
- Keep in mind how the investigative techniques will appear to a jury or the media.
- Recognize that surveillance activities typically require at least two investigators if the subject is expected to be active and this can represent a significant cost if surveillance is extended.
- Recognize the difficulty of obtaining information in certain countries and discuss the timeline and budget with the investigator.

8.4 During the Investigation.

- Maintain regular and clear communications.
- Maintain control over activities.
- Avoid "fishing expeditions."
- Document each phase and stage of the investigation.

9.0 HYPOTHETICAL INVESTIGATIONS

Appendices I and II set forth two examples of intellectual property related investigations that counsel may encounter. A host of legal and ethical issues can immediately be identified and others may arise as the investigative techniques are developed and evolve. Gray areas will also appear in which counsel is required to weigh the need for investigative results against the law and ethical guidance that exists as applied to the facts as they present themselves. Careful consideration of the issues identified by the panel, including the clear prohibitions, gray areas and alternative approaches will aid counsel in managing a variety of investigations.

10.0 APPENDICES

Appendix I: Hypothetical Investigation-Suspected Trade Secrets Misappropriation

Appendix II: Hypothetical Investigation-Suspected Motion Picture Piracy

Appendix III: Sample Investigation Guidelines

Appendix IV: Sample Competitive Intelligence Guidelines

[1] *Recent Trends in Internal Investigations*, ACC Docket, April 2007
[2] *Leading Practices In The Use Of External Investigators To Aid In Corporate Investigations*, Association of Corporate Counsel, June 2007
[3] U.S. Dept. of Labor, Bureau of Labor Statistics.
[4] California Bus. & Prof. Code §§7512-73.
[5] California Bus. & Prof. Code §7521
[6] California Bus. & Prof. Code §7522(e).
[7] California Bus. & Prof. Code §7523(b).
[8] California Bus. & Prof. Code §7523(d).
[9] California Bus. & Prof. Code §7538(b) and §7561.4.
[10] *Wayne v. Bureau of Private Investigators and Adjusters*, 201 Cal.App.2d 427 (1962).
[11] *Redner v. Workmen's Comp. Appeals Bd.,* 5 Cal.3d 83 (1971)
[12] *Noble v. Sears, Roebuck & Co.*, 33 Cal. App.3d 654 (1973)
[13] *Id.* at 664-664.
[14] Cal. Admin. Code tit. 16, s 621.2
[15] California Penal Code §630, et seq.
[16] California Penal Code §647k. See also California Penal Code §502 covering unauthorized access to computers.
[17] Cal. Bus. & Prof. Code §22947, et.seq.
[18] California Bus. & Prof. Code §§17200, 17203.
[19] Arizona, California, Colorado, Connecticut, Florida, Georgia, Illinois, Maryland, Michigan, New York, Oklahoma, Rhode Island, Virginia, Washington and Wisconsin.
[20] California Penal Code §638.
[21] New York Communication Records Privacy Act (s.6723/A.12033) signed by the Governor on September 26, 2006, N.Y. Gen. Bus. Law § 399-dd (2006)
[22] The operative language of California's anti-pretexting law is typical and states "Any person who purchases, sells, offers to sell, or conspires to sell any telephone calling pattern record or list, without the written consent of the subscriber, or any person who procures or obtains through fraud or deceit, or attempts to procure or obtain through fraud or deceit any telephone calling patter record or list shall be punished …"
[23] 42 U.S.C. § 408(a)(7)(B)
[24] Telephone Records and Privacy Protection Act of 2006, Public Law 109-476, January 12, 2007, 18 U.S.C. 1039
[25] 15 U.S.C. § 6821.
[26] 15 U.S.C. § 1681, et seq.
[27] The Fair and Accurate Credit Transactions Act of 2003, (Pub. L. 108-159, 111 Stat. 1952)
[28] *Safeco Insurance Company of America v. Burr,* No. 06-84, June 4, 2007.
[29] 18 U.S.C. sections 2510-22.
[30] 18 U.S.C. sections 2701-11.
[31] 18 U.S.C. § 2721 et. seq.
[32] 18 U.S.C. § 2722.
[33] See *FTC v. Action Research Group*, Civil Action No. 6:07-CV-0227-ORL-22JGG (M.D. Fla., February 15, 2007).
[34] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (codified at 42 U.S.C. § 1320d-2 (note)); Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002).
[35] 46 CFR § 164.512(j).
[36] 18 U.S.C. §§ 1831-1839.
[37] 18 U.S.C. § 1832.
[38] *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998)
[39] 18 U.S.C. 1839.
[40] Internal Security Regulations for Corporations, issued on September 27,2004, effective December 1, 2004.
[41] Data Protection Act 1998.
[42] ABA Comm. On Ethics and Professional Responsibility, Formal Op. 01-422 (2001).
[43] Utah State Bar, Ethics Adv. Op. Comm. Op. No. 02-05 (2002)
[44] *Apple Corps Ltd. v. International Collectors Society*, 15 F. Supp.2d 456. (D.N.J. 1998).
[45] See also, David B. Isbell & Lucantinio N. Salvi, Ethical Responsibilities of Lawyers for Deception by Undercover Investigators and Discrimination Testers: An Analysis of the Provisions Prohibiting Misrepresentations Under the Model Rules of Professional Conduct, 8 Geo. J. Legal Ethics 791, 804 (Summer 1995).

[46] *Gidatex, S.r.L. v. Campaniello Imports, Ltd.*, 82 F. Supp2d 119 (S.D.N.Y. 1999).
[47] *Upjohn Co. v. Aetna Casualty and Surety Co*., 768 F. Supp. 1186 (W.D. Mich. 1990)
[48] See, e.g. *Louis Vuitton S.A. v. Spencer Handbags Corp*., 765 F.2d 966 (2d Cir. 1985); *Weider Sports Equip. v. Fitness First, Inc*., 912 F. Supp. 502 (D. Utah 1996); *Philip Morris USA Inc. v. Shalabi*, 352 F. Supp. 1067 (C.D. Cal. 2004); and *Cartier v. Symbolix*, 386 F. Supp. 2d 354 (S.D.N.Y. 2005).
[49] *Jorgensen v. Taco Bell Corporation,* 50 Cal. App.4th 1398 (1996).
[50] *Id.* at 1402-1403. 18 U.S.C. sections 2510-22.
[51] Model Rules of Professional Conduct, 2007 Edition, Rules 5.3, 5.7 and 8.4(a)
[52] See, e.g.,California Association of Licensed Investigators Code of Ethics.

APPENDIX I

Suspected Trade Secret Misappropriation

Your marketing people have received reports that a Chinese company is scheduled to break ground on a new facility employing process technology that is commonly known to be available to only three competitors worldwide. Your engineering people tell you that to successfully employ the technology, the Chinese company would need a combination of patented devices and the know-how and show-how required to integrate the devices, start up, and operate the facility. This know-how and show-how is a closely-guarded trade secret within your company. Successful operation of this facility has the potential to dramatically impact the world prices for the specialized commodity produced using this technology.

Your Chief Executive Officer and Vice President of Engineering are concerned that there is a leak of trade secret information from one of three sources: (1) a licensee of your technology in India; (2) a currently employed engineer; or (3) a former employee who held high- level technical position within your company. All are bound by NDA's.

As Senior IP Counsel, you have met with a licensed private investigation firm, briefed them on the issues and suspects and developed the following phased course of action. The objective of this course of action is to determine if there is evidence of contact between the company's current and former engineers and the Asian company or between your former licensee (or its employees) and the Asian company.

Phase 1

1. Conduct background investigations on the activities of the current employee and former employee to determine their recent activities or employers and whether they have traveled to Asia and made contact with the Chinese company.

2. Covertly prepare a "mirror image" of the current employee's laptop computer to determine if there is evidence of communication with the Chinese company.

3. Conduct a background investigation on the Indian licensee using an Indian private investigation firm to determine if there is or has been contact with the Chinese company.

4. Conduct a background investigation of the Chinese company and its plans for the new facility, including any news articles or industry publications and visit the site of the planned facility to gather information on permitting, the sources of technology and any partners involved in the project.

Phase II

1. Using a “Front Company” identity, visit the main offices of the Chinese company posing as representatives of an investment fund to determine if the company is interested in any foreign investment.

2. If successful in engaging the Chinese company, continue the dialog and seek assurances that the necessary process technology has been obtained and information regarding the sources of the technology.

What legal and ethical issues are presented in each phase of this proposed course of action?

Are there alternative ways of proceeding with the investigation and evidence gathering that avoid the legal and ethical issues?

APPENDIX II

Suspected Motion Picture Piracy

You are the Senior IP Counsel with brand protection responsibility for a major motion picture studio. You have identified an offer on Craigslist for bundles 10 movie DVD’s for $60. None of the movies listed have been released on DVD and some of them have not even been released to the theaters. The advertisement brags that “all screeners perfect video/audio quality” and invites prospective purchasers to bring their portable DVD player to confirm quality.

Typically, movies are pirated during advance screenings in theaters using “handycams” which produces a copy that is less than perfect. This advertisement seems to indicate that the seller has pre-release access to masters or access to a video and audio feed in a theater projection booth.

You have discussed this advertisement with senior management and been given approval to retain an investigator with the objectives of determining:

1. The quality of the DVD’s and how they were obtained;

2. The quantity that the seller has been selling;

3. The volume the seller can supply;

4. The seller’s associates and distribution chain.

During your initial discussions with the investigator, she has proposed the following investigative plan:

Phase I:

Reply to the Craigslist Ad and make contact with the seller using the pretext of a distributor who has lost his source of DVD’s and wishes to verify quality and discuss volume discounts.

Conduct an initial purchase of each pack of DVD’s offered by the seller.

Determine if Seller is able to consistently provide pre-release movies.

Determine the identity of the person via his e-mail address and conduct a background investigation if the name is not fictitious.

Confirm the quality of the DVD’s and whether “handycam” piracy can be ruled out.

Phase II:

Conduct a two-week surveillance on the Seller to determine volume of sales and associations with the objective of tracing his distribution network up the chain to the source of the high-quality content.

What legal and ethical issues are presented in each phase of this proposed course of action?

Are there alternative ways of proceeding with the investigation and evidence gathering that avoid the legal and ethical issues?

What techniques are legally available if Seller is receiving the high-quality content from his distributor or a third party over the internet to his home computer?

APPENDIX III

SAMPLE INVESTIGATION GUIDELINES

The following guidelines apply to our internal investigation of potential violations of law or XYZ Company Compliance policies:

1. When there is a basis to believe that there may have been a violation of law or an XYZ Company Compliance policy, we will exercise due diligence to collect and evaluate relevant facts about the issue and to determine whether or not a violation has occurred.

2. We will conduct investigations in accordance with all applicable laws.

3. We will treat all persons involved in an investigation with respect and fairness.

4. We will determine the extent of an investigation in large part by the seriousness of the issue and the nature and quality of information provided about a potential violation.

5. We will look into issues objectively and impartially and make no presumption at the outset of an investigation whether or not there has been a violation, or whether a person is guilty or innocent of allegations made against him or her. To this end, we will not assign an investigation to persons who have an interest in the outcome of the matter.

6. While investigating a potential compliance violation, we will work to understand all sides of the issue, including, where possible and appropriate, speaking with people whose conduct is at issue. We will consider all relevant facts, whether incriminating or exonerating.

7. We will handle investigations as discretely and confidentially as possible under the circumstances and expect everyone involved in or assisting the investigation to do the same.

8. We will expect full cooperation from our employees and from any others involved, including suppliers, vendors, contractors, and their respective employees. We will not tolerate any attempts to obstruct an investigation.

9. We will strive to complete investigations in a timely, cost-effective manner, while limiting any disruption to on-going business activities.

10. We will not tolerate retaliation against a person who, in good-faith, reports a known or suspected violation of law or XYZ Company policy or who participates in any part of an investigation.

11. Based on all of the collected facts, the appropriate management team will decide what action should result from the investigation. We will treat fact-finding and management decision-making based on the investigation results as distinct parts of the process.

12. We will document the steps taken during the investigation and the results.

APPENDIX IV

SAMPLE COMPETITIVE INTELLIGENCE GUIDELINES

Competitive Intelligence:

- Can Provide
  - information about competitors, actual or potential business partners, potential acquisition targets;
  - information about financial status, business history, legal issues & standing, technology, new products, marketing;
  - crucial information for strategic business decisions.
- But must be collected in a legal and ethical manner.
  - Properly conducted competitive intelligence is not industrial espionage.
  - Improperly gathered competitive intelligence can lead to disaster.

What We Must NOT Do:

- Use false pretenses, pretexts or surreptitious means to get information
- Ask for or use confidential information about competitors or other third parties
- Steal anything (e.g. competitor's documents on a desk in a customer's office)
- Use espionage techniques such as electronic or aerial surveillance, dumpster diving, etc.
- Offer anything of value, including XYZ Company information, as an inducement to disclose confidential information
- Seek confidential information from new hires about their prior employer

What We Should Do:

- Ask for information, as long as you are not knowingly inducing someone to breach an obligation of confidentiality
- Advise information sources that we do not want them to give us information they think is confidential or believe they should not disclose it

- Use public sources of information (e.g. government records, SEC filings, internet searches, public records searches, trade shows, industry surveys by reputable firms)
- Observe carefully and thoroughly in an unconcealed manner
- Ask Legal Counsel if you are uncertain whether an action is legal or ethical
- Contact the Director of Global Security or the Law Department if you believe it is necessary or appropriate to hire an outside investigator

When Using Outside Firms:

- We will be held responsible for actions of firms we hire
- Close oversight of planning and execution is a must-what to do and how to do it.
- Law Department must be consulted re: any potential legal issues (e.g. privacy laws, computer forensics)
- For outside investigators:
  - Must obtain approval from Global Security, which coordinates with the Law Department
  - Global Security maintains a database of experienced, reputable firms in different locations who subscribe to industry codes of ethics or have their own codes
- For other outside firms (e.g. investment banks)
  - need to ensure that they conduct themselves legally and ethically
  - consider building this commitment into engagement letters

Sample Code of Ethics for Competitive Intelligence:

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

From Society of Competitive Intelligence Professionals

Always Remember:

- Use good business judgment
- Ask:
  - Is it legal?
  - Does it follow company policy?
  - Is it right?
  - How would it look to those outside the Company?
- Ask if you are not sure what to do

Trends in Corporate Investigations

- Increased frequency (including international)
- Increased scrutiny of Investigators
- Increased regulation of Investigators
- Increased oversight by Counsel
- Increased cost/decreased effectiveness

Objectives – to define and determine:

- How Private Investigators are used
- How they conduct investigations
- How they are regulated
- What practices are prohibited
- What ethical issues confront the retaining lawyer
- How investigations can be conducted ethically, effectively and in compliance with law

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Internal Investigations

- Background investigations
- Undercover investigations
- Fraud investigations
- Forensic accounting
- Computer forensics
- IP theft investigations
- Workplace issue investigations

External Investigations

- Due diligence (M&A, JV partners, suppliers, distributors, manufacturers, offshore operations)
- Insurance fraud
- Competitive intelligence
- Debtor and asset searches
- Counterfeiting, piracy and gray market
- Trade Secret and other IP theft
- Economic espionage
- Litigation support

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

How do they do it?

- Overtly
- Covertly
  - Open and closed source databases
  - Using a pretext
  - Physical surveillance
  - Technical surveillance
  - Using "front companies"
  - Using undercover agents
  - Using their "contacts"

How are they regulated?

- Stringently, in a majority of states
- Exemptions: Attorneys, In-house investigators, insurance adjusters, sometimes others
- Unlicensed investigators
- Many small firms and individuals (43,000 in 2004; 26% self-employed)

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Prohibited Practices: <u>There are many</u>

- Private Investigator statutes and regulations
  - *Wayne v. Bureau or Private Investigators*
- State privacy laws
- State unfair competition laws
- State anti-pretexting laws-phone records
- Federal anti-pretexting law-phone records
- Federal privacy laws

Overseas Investigations

- "Investigations" may be illegal
- General absence of licensing requirements
- Obtaining non-public records-probably involves illegal activity at some level
- UK's Data Protection Act
- Middle East is particularly risky

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Ethical Considerations

- ABA Model Rule 4.1-False Statements
- ABA Model Rule 8.4(c)-Conduct involving dishonesty, fraud, deceit or misrepresentation
- Model Rule 4.2-Communicating with represented parties
- Model Rules 5.3, 5.7 and 8.4(a)-Acts by others

Case Law

- *Apple Corps Ltd. v. International Collectors*
- *Gidatex v. Campeniello Imports*
- *Upjohn v. Aetna Casualty*

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Practical Considerations

- Initial Planning
- Before Retaining an Investigator
- Retaining an Investigator
- During the investigation

Hypothetical 1 – Suspected Trade Secrets Misappropriation

- Permissible investigation of current employee
- Covert imaging of employee's hard drive
- Investigation of former employee
- Investigation of Indian licensee
- Investigation of Chinese company
- Use of "front company" and pretext to engage Chinese company

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Hypothetical 2-Suspected Motion Picture Piracy

- Use of pretext
- Determination of identity of pirate
- Surveillance of suspect