AFFORDABLE EDUCATORS LLC

601

# PI Blunders

COURSE INSTRUCTIONS

You are on Page 1 of this book.

Use your "Page Down", "Arrow Down" or scroll, to start reading.

## How to Search Book?

Use ***CTRL+F*** (Command F for Mac) or ***Go to INDEX*** on next page.

## Course Contents



*iPad and Tablet Users See DEMO & Links Above*



*- Since 1993-*


AffordableEducators.com
(800) 498-5100
orders@ceclass.com

PO Box 2048
Temecula, CA 92593

HOME

PI blunders

# Contents

PI blunders

# Preface

Private investigators who have never been sued or legally pursued, are sometimes lulled into believing that the way they do business must be working. Unfortunately, this ignores the real possibility that the ***same events of the past, that weren't a problem, can now become a problem***. It is a world of legal rights and little trust. The long-term client who you trusted, can change. Also, regulations change, industries change, economies change and no one can really keep up or control every aspect of their present business, let alone the future.

No one knows what life has in store, but if you have been a working PI for any length of time, you know you are prone to errors, some beyond your control . . . some, are actually small indiscretions that might start out as a favor for your client. As a business person you need to accept the fact that your business carries the risk that these problems could grow into something big. Before that happens, you need to find ways to manage and plan for these risks to minimize the fallout when a claim occurs. You will notice we said ***when*** a claim occurs not ***if***.

Your exposure can also vary depending on the type of work you do. Conducting internal investigations for employers, expert witness testimonies, skip tracing services or independent white collar crime investigations could represent lower levels of liability than might more controversial duties like surveillance. Then again, we will show evidence of PI blunders, even lawsuits, for seemingly small infractions like recordkeeping or a simple lack of communication with a client.

You might try to end run around potential conflicts by making friends with your clients, buying errors and omissions insurance, incorporating or using other means of asset protection, but you will always be at risk for the problems that ***fall through the cracks*** and rear their ugly heads at your doorstep. You have to plan for that day NOW. The purpose of this course is to help you do that by understanding the mistakes or blunders of other PIs and making a conscience effort to avoid them yourself.

Many issues we discuss on this course focus on laws. Of course, these laws may vary from state to state. You may even notice some of the court cases may be in a state different than the ones you practice. Or, they may be old and seemingly not relevant. Don't be fooled that these lawsuits don't apply to you. In many respects they can be used a precedent for court rulings anywhere in the United States.

Another thing . . . you might read about cases where a investigator defendant was let off or received a light penalty. Again, don't be fooled. If you are involved in litigation, much of the money and time you spend happens way before you get into court. By the time a jury or judge decides you are innocent or deserve a slap on the hand you will have written checks for tens of thousands of dollars and spent weeks in discovery, depositions or at your attorney's office. The best remedy is to avoid a lawsuit before it happens.

Before we get into the down and dirty blunders in the PI industry, let's start by looking at the deciding issues that establish your legal conduct and create agent liability . . . ***PI licensing and law***.

*NOTE: As we proceed on our journey, look for this symbol to denote PI Blunders you won't want to repeat.*

PI blunders

# PI Licensing & Law

## LICENSING

### *State Licensing & Permissible Activities*

States with no PI license requirements are the ***exception*** rather than the rule today. As of the writing of this course, only Alaska, Idaho, Mississippi, South Dakota and Wyoming allow investigators to work without a license. Since rules change, you would be wise to research unique requirements in each of the jurisdictions in which you practice to determine license rules and regulations. It may even be possible to request opinions from the states' attorneys general offices for particular situations.

The majority of states that do require PIs to be licensed focus on ***permissible activities*** such as:

- Overt investigations, in which investigators identify their roles and principals and do not otherwise mislead or deceive anyone.
- Public records searches.
- Physical observations, measurements, and the like.
- Protection of a person, if it is "incidental" to an investigation and if the investigator complies with the firearm and insurance requirements.
- Surveillance, even if covert, provided that investigators do not trespass or invade privacy.

### *Investigator Defined*

The ***definition of an investigator*** can be slightly different among varying jurisdictions. Typical examples of statutory definitions of an investigator that would require licensure include a person investigating:

- The identity, habits, conduct, movements, whereabouts, transactions, reputation or character of any person or organization.
- The credibility, honesty or integrity of witnesses or other persons.

- The location, disposition or recovery of lost or stolen property, missing persons, owners or heirs of property or heirs to estates.
- The origin of and responsibility for libels, losses, accidents, fires, or damages or injuries to persons or property.
- The conduct, honesty, efficiency, loyalty or activities of employees, persons seeking employment, agents, or contractors and subcontractors.
- The identity or location of persons suspected of crime or wrongdoing.
- 
- Evidence (or obtaining of evidence) to be used before any committee, board of award or arbitration, administrative or licensing body or officer, or in preparation for trial of any civil or criminal case.

## ***Exemptions & Exclusions***

Jurisdictions have differing exemptions and exclusions from their PI licensing requirements, and some offer no exemptions at all from licensure requirements. Examples of exceptions from PI licensure in various jurisdictions include attorneys, CPAs, government officials, individuals conducting genealogical research, computer forensics experts, insurance adjusters, expert witnesses and reporters.

Most states exclude someone performing an investigation on behalf of his or her employer, such as an internal auditor or company detective while others provide no such exceptions. Some states specifically exempt a person conducting computer forensic examinations, while other states specifically include them in the definition of an investigator requiring a PI license. Each investigator is responsible to ensure they're in compliance with the law, so you need to consult your legal counsel. Don't wait to be embarrassed on the stand or find yourself charged with a crime. ***Proactively investigate the necessity of licensure in the jurisdictions in which you practice***.

## ***Bonds***

Many jurisdictions require that the private investigator or his or her firm be bonded; the amount of required bond varies by jurisdiction and ranges from $2,500 to $100,000. A few states require liability insurance . . . some allow it in lieu of a bond.

## ***Expert Testimony***

If you're going to testify as an expert witness or fact witness, be sure that you're either properly licensed within that jurisdiction or specifically exempted from licensure requirements. Otherwise, opposing counsel can accuse you of violating the law during cross examination, or the judge may choose to disallow your testimony entirely. Either way, your case and professional reputation could be severely damaged

## ***License Disqualifiers***

Although you should refer to your particular state's disqualifiers, most states will disqualify you from applying for a PI license if any of the following conditions exist for you:

- Are under 18 years of age and are applying to be a private investigator, or private investigator associate (intern).
- Do not have three years of investigative experience
- Are not a citizen or legal resident who is authorized to seek employment in the United States
- Have ever been convicted of a felony, whether or not your conviction was subsequently set aside and your Civil Rights were restored
- Are currently under indictment for a felony, or named in an outstanding arrest warrant
- Have been convicted of any misdemeanors involving personal violence, misconduct with a deadly weapon, dishonesty or fraud, arson, theft, domestic violence, narcotics, or sexual misconduct within the last five years preceding your application
- Are on parole, community supervision, work furlough, home arrest, or release on any other basis
- Are on probation pursuant to a conviction for any act of personal violence or domestic violence
- Have been adjudicated mentally incompetent or found to constitute a danger to self or others
- Have a disability, which renders you incapable of performing essential functions of the job even with reasonable accommodation from an employer
- Have been convicted of acting or attempting to act as a security guard or private investigator without a license if a license was required

**Note:** Not all arrests will disqualify you from pursuing a career as a private investigator and eventually obtaining your license. Many of the country's top investigators committed minor crimes in their past, but this has not

stopped them from being effective at what they do.

## ***Fees & Penalties For Unlicensed Investigators & Others***

Regulations and fees from licensing PIs, give states the power to discipline and limit what non-sworn law enforcement personnel can do while conducting an investigation.

In most states that require PI licensing, anyone may file a complaint against an individual or firm conducting an investigation without a license. ***Penalties for practicing without a PI license vary, but in a few states the crime is a felony***. In one recent case, even a CPA providing forensic accounting services was charged with a felony for conducting an unlicensed investigation in Virginia.

Unlicensed persons who represent themselves as licensed or act as private investigators are committing a misdemeanor. ***Fines might be $5,000 and up to one year in jail***. In addition, anyone--presumably including a lawyer--who "knowingly" engages an unlicensed investigator or who conspires to have an unlicensed person operate as an investigator also commits a misdemeanor with the same penalties. Public prosecutors may seek civil remedies against unlicensed investigators, their coconspirators, and anyone who knowingly engages such investigators. The civil remedies include an injunction (for which prosecutors need not "show lack of adequate remedy at law or irreparable injury"), a civil fine of up to $10,000, and reimbursement of investigation expenses.

## ***Private Party Remedies***

While many jurisdictions may not have specific private rights of action for licensing violations, ***private parties who wish to purse an unlicensed investigator have three indirect remedies***:

- A ***licensing violation under unlawful business act or practices*** with equitable relief, including an injunction and, if appropriate, restitution.
- A ***move to exclude evidence gathered*** by an unlicensed investigator.
- A person who contracts with an unlicensed investigator might seek to ***avoid paying the investigator's fees*** on the ground that the contract is illegal.

# LAW

## *Privacy Issues*

Courts generally interpret a violation or invasion of privacy where:

One ***intentionally intrudes***, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

The form of invasion of privacy discussed here does not depend upon any publicity given to the person whose interest is invaded or to his affairs. ***Invasion of privacy consists solely of an intentional interference*** with a person's interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.

The invasion may be:

- ***Physical intrusion*** into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff's room in a hotel or insists over the plaintiff's objection in entering his home.
- It may also be by the ***use of the defendant's senses***, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires.
- It may be by some other form of ***investigation or examination into his private concerns***, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents.

***The intrusion itself makes the defendant subject to liability***, even though there is no publication or other use of any kind of the photograph or information outlined

## *Federal Invasion of Privacy*

The Fourth Amendment, which prohibits unreasonable searches and seizures, has been interpreted to imply a right of privacy. Beginning in the early 1960s, the United States Supreme Court decided a line of cases which

held that privacy is an implied right under the Fourth and Fourteenth Amendments. For example, in **Roe v. Wade** (1973), the Court addressed the right to privacy in the area of birth control and abortion.

In **Katz v. United States** (1967), the United States Supreme Court recognized a reasonable expectation of privacy for telephone conversations. The Court in that Fourth Amendment case indicated that the attorney-client privilege turns on whether the communication enjoys a ***reasonable expectation of privacy***.

Lower courts vary in the tests they apply to determine if there is a reasonable expectation of privacy.

In addition, Fourth Amendment protection of privacy could be lost simply because the investigating entity had a purpose for investigating that was completely independent of law enforcement, like **State of Utah v. Brenda Ellingsworth** (1998), where a workers compensation claim did not provide the defendant the privacy protection she was hoping for.

Similarly, in **United States v Howard** (1985), and **United States v Pervaz** (1997), the courts held that private investigations were made to ***benefit private interest and not law enforcement*** and not afforded protection under the Fourth Amendment.

***State Privacy Laws***

Some states have constitutional provisions which expressly provide citizens with a right of privacy pursuant to the following language:

***Every natural person has the right to be let alone and free from governmental intrusion into his private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.***

By these terms, investigations that do not closely align with law enforcement or some other state agency shall have a constitutional right of access to public records.

## *The Privacy Act of 1974*

The Privacy Act establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of ***personally identifiable information*** about individuals that is maintained in systems

of records by federal agencies. A ***system of records*** is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register.

The Privacy Act ***prohibits the disclosure of information from a system of records absent the written consent of the subject individual***, unless the disclosure is pursuant to one of many statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements. Additionally, with people granted the right to review what was documented on their name, they are also able to find out if the "records have been disclosed".. and are also given the rights to make corrections.

This Act ***limits the collection and transfer of personal data*** on individuals by government agencies. It provides that no government agency may disclose any record about an individual except pursuant to the written request of or with the consent of the person to whom the record relates. However, there are several exceptions in the Act; which allow disclosure to employees of the agency itself, to law enforcement officers, to the Census Bureau, or to either house of Congress. In addition, records of an agency may be produced pursuant to a subpoena.

Under this Act, an agency in possession of records is required to provide an individual with the information concerning that individual, upon his or her request, and is required to allow that person an opportunity to correct inaccurate information. The Act also provides that the government agency maintain only such information about an individual as is relevant and necessary to accomplish a purpose of the statute which authorized collection of the information. If the agency fails to keep accurate information, or fails to provide an individual with a copy of his record upon request, the aggrieved person may bring a civil action in Federal District Court and may recover attorneys' fees upon prevailing.

Of particular interest in the context of the Internet is the fact that the Privacy Act ***extends only to those records*** that specifically identify an individual based upon name, identifying number, or other personal identification feature, such as photograph, fingerprint, or voice print. Accordingly, the Act does not cover collections of information which do not identify that person based on a feature or attribute unique to that individual. For example, detailed information about a person's purchasing patterns and assets would not constitute a record under the Act unless that

information was retained in a record designated by an identifying attribute of the individual.

## ***Privacy Protection Act of 1980***

The **Privacy Protection Act of 1980** is legislation passed in the United States that protects journalists and newsrooms from search by government officials. The act ***protects "work products" and "documentary materials."*** A subpoena must be ordered by the court to gain access to the information

This Act limits the authority of federal law enforcement officers and employees to seize any work product materials possessed by a person reasonably believed to have a purpose to use those materials in a book, broadcast, or newspaper to be distributed to the general public, unless there is probable cause to believe that the person in possession of the materials has committed or is committing the criminal offense to which those materials relate. The Act includes a specific exception which allows the seizure of child pornography.

## ***Internal Revenue Code***

***All taxpayer records are deemed confidential***, and may only be produced with the taxpayer's consent or pursuant to a subpoena. A taxpayer may bring a civil action against any person who willfully or negligently discloses any tax return information.

## ***The Freedom of Information Act***

Passed in 1966, the Freedom of Information Act was originally designed to ***allow citizens access to government records*** and to prevent secret governmental activities. Amended in 1996, it expanded the definition of records to include electronically stored information. Records have also been defined as other media like audio recordings, videotapes and motion pictures.

The FOIA creates the presumption that the records of all federal agencies are open to the public. However, given the explosion of information readily available on the Internet and computer data bases, the state and federal courts now appear to be favoring privacy interests over openness to justify sealing information that once was considered public.

Under the FOIA, the government is required to give individuals the records they request unless the government asserts one many exemptions

permitted by the FOIA. Of those exemptions, the FOIA contains two exemptions that allow an agency to ***withhold information if it concludes that release would invade the privacy of individuals.*** This might apply in the case of personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Another exemption withholds ***records or information compiled for law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy***.

The FOIA also provides that a federal agency may delete from its published rulings and opinions identifying details, if necessary to prevent an unwarranted invasion of privacy. However, the opinion must explain the justification for the deletion. For all its promise, the FOIA appears to have fallen short of its original goal of providing full disclosure. The courts, including the United States Supreme Court, have given the FOIA a narrow construction and have given the exceptions to disclosure a fairly broad construction.

For example, in the **Dept. of Justice v. Reporters Committee for Freedom of the Press** (1989), the United States Supreme Court, relying on the personal privacy exemption, held that the disclosure of "rap sheets" (compilations of arrests, indictments, convictions, or acquittals) maintained on a centralized computer at the Department of Justice constituted an unwarranted invasion of privacy, even though the same information was publically available on paper from the original sources, such as local police departments. Finding that there was a stronger personal privacy interest implicated by the disclosure of a rap sheet generated by a computer than by scattered records found from a diligent search of courthouse files, county archives, and local police stations, the Supreme Court narrowly interpreted "public interest" and held that those seeking personally identifiable information from government records must show an intent to use the information to examine the workings of the government.

Thereafter, the Supreme Court continued to permit federal agencies to withhold personally identifiable information on privacy grounds. For example, the Supreme Court in **Dept. of Defense v. Federal Labor Relations Authority** (1994), held that the home addresses of government employees should not be disclosed to union organizers because the addresses did not relate to government operations and their release would not serve the public interest.

Other governmental agencies have also relied on the personal privacy exemption. For example, in **New York Times v. NASA** (1990), NASA cited the personal privacy exemption to justify withholding the cockpit tape

from the Challenger disaster. In addition, the Department of Education in **Garnett Satellite Information Network, Inc. v. Dept. of Education** (1990), relied on the personal privacy exemption to justify its refusal to release the names of persons who had defaulted on their student loans. Furthermore, the FBI in **Schmerler v. Federal Bureau of Investigation** (1990), invoked the privacy exemption to justify its refusal to disclose sixty-year-old records.

This trend towards relying on the exemptions of the FOIA has demonstrated how the presumption favoring disclosure originally embodied in the FOIA is becoming subservient to privacy interests. In reshaping the boundaries established by Congress, courts have restricted access to information that could shed light on government activities.

## ***The Fair Credit Reporting Act***

Checking an insured's credit history can result in vital clues for in unveiling fraud. A consumer credit report typically includes employment history, income, current indebtedness, payment history on credit accounts and loans, bankruptcies, lawsuits or judgments against the subject, and tax and other liens against the subject's property. Much of that information, however, is protected by the Fair Credit Reporting Act to ensure that consumer reporting agencies utilize reliable and accurate credit reporting practices while simultaneously maintaining the confidentiality of the consumer reports the consumer reporting agencies generate, by limiting access to those with a specific, limited, and legitimate interest in obtaining the information.

A ***consumer report*** is defined as any communication of any information by a consumer reporting agency that is expected to be used in whole or in part to serve as a factor in establishing the consumer's eligibility for "credit or insurance to be used primarily for personal, family, or household or employment purposes. An ***investigative consumer report*** is defined as a report which delves into the consumer's character, general reputation, personal characteristics, and mode of living; which is obtained through personal interviews.

The Act only permits disclosure of consumer reports to persons who intend to use the information for credit-granting, employment, insurance underwriting, governmental license or benefit eligibility, or in connection with a business transaction involving the subject of the report. The recipient of the consumer report is required to notify the consumer that it has obtained a report where he or she is being denied credit or where an investigative consumer report has been requested.

What relevance does this have to private investigations? Consider **Hovater v. Equifax, Inc.** (1987). An insured filed a first party property claim for loss of his residence by fire. After determining that arson caused the fire, insurance company investigators retained Equifax to obtain background information about Hovater in order to evaluate his claim. After learning of the report, Hovater sued Equifax for ***negligently releasing a consumer report*** for a purpose not authorized under the Act. The court held that a report, which an insurer procures from a credit reporting agency solely for use in evaluating the insured's claim for benefits under an existing policy of insurance, is not a consumer report that is governed by the Act.

Also, in **St. Paul Guardian Ins. Co. v. Johnson** (1989), a homeowner's insurer, suspicious of a theft loss, obtained a copy of the insured's pre-existing credit report for the purpose of obtaining information as to whether the insured owned the property claimed as stolen. Because the insurance company investigators obtained a copy of a pre-existing credit report the court held that the insurance company had violated the Act, even though the insurance company did not intend to use the report for a purpose under the Act.

In addition to the Federal Fair Credit Reporting Act, investigators need to be aware that many states have enacted statutes or rules which codify all or substantial portions of the Fair Credit Reporting Act. To avoid litigation regarding the appropriateness of obtaining a consumer credit report during the investigation of a claim, a written consent or authorization from the subject of the report should be obtained before the request for such a report is made to any consumer credit reporting agency.

## ***Federal Wiretapping Act / Electronic Communications Privacy Act***

As an amendment to the 1968 Federal Wiretap Statute, ***the Electronic Communications Privacy Act (ECPA)***, codified the common law tort of invasion of privacy as it relates to electronic communications. Whereas the Federal Wiretap Statute made it unlawful for one to eavesdrop on or intercept another person's oral and wire (telephone) communications, the ECPA broadened that statute's scope to protect ***all forms of electronic/digital communications, such as data transmissions between computers, paging devices, e-mails, video transmissions, and telephone voice communications.***

Generally, the ECPA ***prohibits any person (not just the government) from intentionally intercepting an electronic communication, or from disclosing the contents of any intercepted electronic***

***communication.*** This prohibition applies not only to those who seek to break into an electronic communications system (such as hackers) but also to those who own and operate such systems (such as Internet access/service providers and private network operators).

However, this prohibition does not prevent an employer or agent of a provider of an electronic communication service from intercepting, disclosing, or using the communication in the normal course of his or her employment while engaged in any activity that is necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service. Employers, for example, may monitor an employee for as long as the communication is business-related.

In **Epps v. St. Mary's Hospital of Athens, Inc.** (1986), an employer monitoring the conversation between two employees, reprimanded one employee who had criticized supervisors. Since this was in the ordinary course of business and the call took place during work hours, and it concerned supervisory employees and the work environment it was considered legitimate.

Also, in **Briggs v. American Air Filter Co.** (1980), an employer's monitoring of a business call, in which the employee revealed trade secrets to a business competitor, was within the ordinary course of business and justified because the employer had suspicions that trade secrets were being revealed, and he listened only long enough to confirm that fact.

The ECPA provides various levels of privacy protection depending on: (1) the type of system (public or private) where the communication is found; and (2) whether the communication is in storage or in transit. Typically, there are three main types of systems: a private network; a semi-public network or commercial services; and the Internet.

Private networks are essentially closed systems that operate within the same office. E-mail communications on a private network raise a reasonable expectation of privacy as seen in **United States v. Keystone Sanitation Company** (1995).

A right to privacy is similarly fairly clear on semi-public networks or commercial services provide e-mail services to individuals or entities for a subscription fee. Typically, access to those networks is password-protected. Computers send messages over a reserved telephone network to the commercial network. Stored on the commercial network, those messages are accessed via password by another member of the commercial service. Such transmissions are subject to a reasonable expectation of privacy per **United States v. Maxwell** (1995).

E-mail provided through the Internet typically uses ordinary telephone lines and intermediate computers to transfer information. Operated by Internet service providers, Internet e-mail may be stored temporarily in one or more computers. Once stored, the ECPA prohibits any person from unlawfully and intentionally accessing a stored electronic communication without authorization. ***Stored messages include*** those in the addressee's mailbox waiting to be picked up by the addressee, and records of private discussions between users. Thus, ***stored e-mail messages can be obtained only pursuant to a search warrant***

However, the ECPA does not provide users of a system with a right of privacy against the operator of the system, at least with respect to stored messages. Since a system can be configured to store all messages that pass through it, ***the system operator effectively has the ability to review all messages that pass through the system***. It is illegal, however, for a system operator to divulge the contents of any communication stored on the system (other than to the intended addressee and other limited exceptions).

With regard to the transmission of any voice or electronic communications, the ECPA prohibits unauthorized interception, use, or disclosure of such communications in transit. Therefore, the interception of private e-mail and other communications in transit requires a wiretap authorization per **Jackson Games, Inc. v. U.S. Secret Service** (1994). However, there are a limited number of exceptions. For example, no protection exists for communications that are "readily accessible to the general public" such as those in public chat rooms. Also, an Internet service provider may intercept an injurious message if necessary to protect "the rights of property" of the Internet service provider.

The ECPA provides for both ***criminal and civil remedies*** in the event of a violation. Appropriate relief in a civil action may include actual damages suffered by the plaintiff, profits made by the violator, and attorney's fees and costs.

## ***Stored Communications Act (1986)***

The SCA provides ***criminal penalties for anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided or … intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage*** in such system shall be punished ... ."

The SCA targets two types of online service, "***electronic communication services" and "remote computing services."*** The statute defines an electronic communication service as "any service which provides to users thereof the ability to send or receive wire or electronic communications." A remote computing service is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." Also describes conditions under which a public ISP can voluntarily disclose customer communications or records. In general, ISPs are forbidden to "divulge to any person or entity the contents of any communication which is carried or maintained on that service." However, ISPs are allowed to share "non-content" information, such as log data and the name and email address of the recipient, with anyone other than a governmental entity. In addition, ISPs that do not offer services to the public, such as businesses and universities, can freely disclose content and non-content information. An ISP can disclose the contents of a subscriber's communications authorized by that subscriber.

Conditions under which the government is able to compel an ISP to disclose "customer or subscriber" content and non-content information for each of these types of service:

- **Electronic communication service.** If an unopened email has been in storage for 180 days or less, the government must obtain a search warrant. There has been debate over the status of opened emails in storage for 180 days or less, which may fall in this category or the "remote computing service" category.
- **Remote computing service.** If a communication has been in storage for more than 180 days or is held "solely for the purpose of providing storage or computer processing services" the government can use a search warrant, or, alternatively, a subpoena or a "specific and articulable facts" court order (called a 2703(d) order) combined with prior notice to compel disclosure. Prior notice can be delayed for up to 90 days if it would jeopardize an investigation. Historically, opened or downloaded email held for 180 days or less has fallen in this category, on the grounds that it is held "solely for the purpose of storage."

## ***Computer Fraud and Abuse Act (CFAA)***

Another federal statute enacted to address data and communications privacy concerns is the Computer Fraud and Abuse Act. The Act has been amended a number of times—in 1989, 1994, 1996, in 2001 by the USA PATRIOT Act, 2002, and in 2008 by the Identity Theft Enforcement and Restitution Act.

In January 2015 Barack Obama proposed expanding the CFAA and the RICO Act in his *Modernizing Law Enforcement Authorities to Combat Cyber Crime* proposal. It failed on the grounds it would make many regular Internet activities illegal.

The Computer Fraud and Abuse Act (CFAA) was designed to protect information in computer data banks, including information held by financial institutions, a consumer reporting agency, or a credit card issuer. In addition, the CFAA prohibits certain actions when computers used by, or for the benefit of the U.S. Government or financial institutions (known as ***federal interest computers***) are involved, or when there is interstate computer access. The CFAA also prohibits intentional access to a federal interest computer which affects the ability of the government to operate that computer.

Intended primarily to prevent unauthorized access to computer networks to protect the privacy of the information and communications associated with those networks, the CFAA also protects those networks from acts of sabotage, including alteration of data and impairment of network operations and use. Authorizing the Secret Service to investigate any violation, the CFAA provides for a private cause of action for any person who suffers damage due to someone tapping into a computer system. The Act also provides for ***criminal penalties*** up to ten ***(10) years*** for a first violation and twenty ***(20) years*** for a subsequent violation.

## ***Computer Matching & Privacy Protection Act***

This Act (1988) is an amendment to the Privacy Act of 1974, discussed below. The amendment restricts the federal government's ability to keep track of people by matching information (such as social security numbers) regarding individuals that is maintained by different federal agencies.

## ***Telephone Consumer Protection Act of 1991***

Codified at 47 U.S.C. §227, this Act prohibits the use of unsolicited fax advertisements, and restricts the use of automatic dialer systems to make telephone solicitations, artificial or prerecorded voice messages, SMS text messages, and fax machines. It also specifies several technical requirements for fax machines, autodialers, and voice messaging systems—principally with provisions requiring identification and contact information of the entity using the device to be contained in the message. The Act also allows the creation of a data base of customers who specifically do not want to be called by telephone solicitors. This statute is not intended to preempt state laws, and the states are free to enact laws that provide greater protection.

## ***Cable Communications Policy Act***

Codified in 1984, this Act prohibits a cable service operator from collecting personally identifying information about a customer without the customer's consent. It also prohibits disclosure of the customer's identifying information, including, but not limited to, information about the customer's viewing habits.

## ***Children's Online Privacy Protection Act of 1998 (COPPA)***

The act, effective April 21, 2000, applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing to those under 13.

## ***Gramm-Leach-Bliley Act of 1999 (a/k/a Financial Services Modernization Act of 1999)***

This law became effective in November of 1999. It primarily affects the banking and finance industry. However, it also affects the interplay between the banking and insurance industries. More specifically, the Act permits financial holding companies to engage in insurance activities, and will pre-empt any state laws currently prohibiting that practice.

The Act creates a new mechanism for protecting non-public customer information. It provides customers with certain informational and non-disclosure rights with respect to the sharing of customer information between financial service organizations. Consumers must be provided an annual privacy disclosure concerning privacy policies and information sharing, and consumers must be provided with an opportunity to opt-out with respect to the transfer of that consumer's information.

The Act requires federal banking and securities agencies to adopt customer privacy regulations. The Act also specifically addresses the issue of "pretext calling" and identity theft, and provides for criminal sanctions for these type activities.

## ***Federal Records Act (1950, 2014)***

The Federal Records Act provides citizens with access to historical documents contained in the national archives. In particular, this Act provides that people shall have access to records of federal agency activity which affect that individual.

In November 2014, the Presidential and Federal Records Act Amendments of 2014 was signed into law by President Barack Obama. This bipartisan act, which followed the 2011 President's Memorandum on Managing Government Records, modernizes the Federal Records Act. The act expressly expands the definition of federal records to include ***electronic records*** (the first change to the definition of "Federal record" since the enactment of the act in 1950). The act also

- Grants the Archivist of the United States the final determination as to what constitutes a Federal record;
- Authorizes the early transfer of permanent electronic federal and presidential records to the National Archives, while legal custody remains with the agency or the president;
- Clarifies the responsibilities of federal government officials when using non-government email systems; and
- Empowers the National Archives to safeguard original and classified records from unauthorized removal

## ***Right to Financial Privacy Act (1978)***

This Act prohibits the federal government from obtaining access to the bank records of an individual or partnership of five people or less, unless the account holder consents, or the federal agent obtains a warrant or subpoena for the records. However, the Act permits the bank to disclose

records of persons suspected of engaging in illegal activity. Before the Act was passed, the United States government did not have to tell customers that it was accessing their records, and customers did not have the right to prevent such actions.

## ***Family Educational Rights and Privacy Act of 1974***

FERPA gives ***parents access to their child's education records***, an opportunity to seek to have the records amended, and some control over the disclosure of information from the records. With several exceptions, schools must have a student's consent prior to the disclosure of education records *after that student is 18 years old*.

The law applies only to educational agencies and institutions that receive funding under a program administered by the U.S. Department of Education. Other regulations under this act, effective starting January 3, 2012, allow for greater disclosures of personal and directory student identifying information and regulate student IDs and e-mail addresses.

Examples of situations affected by FERPA include school employees divulging information to anyone other than the student about the student's grades or behavior, and school work posted on a bulletin board with a grade. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.

This privacy policy also governs how state agencies transmit testing data to federal agencies. For example see Education Data Network.

This U.S. federal law also gave students 18 years of age or older, or students of any age if enrolled in any post-secondary educational institution, the right of privacy regarding grades, enrollment, and even billing information, unless the school has specific permission from the student to share that specific type of information.

FERPA also permits a school to disclose personally identifiable information from education records of an "eligible student" (a student age 18 or older or enrolled in a postsecondary institution at any age) to his or her parents if the student is a "dependent student" as that term is defined in Section 152 of the Internal Revenue Code. Generally, if either parent has claimed the student as a dependent on the parent's most recent income tax statement, the school may non-consensually disclose the student's education records to both parents.

The law allowed students who apply to an educational institution such as graduate school permission to view recommendations submitted by others as part of the application. However, on standard application forms, students are given the option to waive this right

## ***Video Privacy Protection Act (1988)***

Passed by Congress in 1988, the Video Privacy Protection Act, also known as the Bork Bill, was created after the **City Paper**, a Washington D.C. weekly, published the titles of Judge Robert Bork's video rentals when he was a Supreme Court nominee. The Video Privacy Protection Act makes it a crime to release individualized data about the videos any individual may rent or buy. In addition, this Act requires a warrant, a grand jury subpoena, or a court order establishing probable cause and formal notice to the individual to obtain such information.

## ***Driver's Privacy Protection Act (1994)***

The law was first introduced after an increase in opponents of abortion rights were found to be using public driving license databases to track down and harass abortion providers and patients. Prominent among such cases was physician Susan Wicklund, who faced protests and harassment including her house being picketed for a month

The Act sets forth a ***general prohibition on the release of information contained in state motor vehicle registration records***. However, the Act sets forth numerous exceptions. One of those exceptions, permits the release of motor vehicle information "For use by any insurer or insurance support organization, or by a self insured entity, or its agents, employees or contractors in connection with claims investigation activities, anti-fraud activities, rating or underwriting." This exception allows the insurance company's investigation to include records available from state motor vehicle registration departments.

The statute's constitutionality was upheld by the U.S. Supreme Court against a Tenth Amendment challenge in **Reno v. Condon** (2013).

## ***Anti-Phishing Laws***

Many states have enact laws that the act of posing as a legitimate company or government agency in an email, Web page, or other Internet communication in order to trick a recipient into revealing his or her personal information.

## ***Computer Spyware Legislation***

These types of laws prohibit an unauthorized person from knowingly installing or providing software that performs certain functions, such as

taking control of the computer or collecting personally identifiable information, on or to another user's computer.

## ***Cyberbullying Laws***

Cyberbullying is one or more acts of sexual harassment, hate violence, or intentional harassment, threats, or intimidation, directed against school district personnel or pupils, committed by a pupil or group of pupils. Bullying, including bullying committed by means of an electronic act, as defined, including a post on a social network Internet Web site, is a ground on which suspension or expulsion may be based.

## ***Online Privacy Acts***

Online privacy law require operators of commercial web sites or online services that collect personal information on consumers through a web site to conspicuously post a privacy policy on the site and to comply with its policy. The privacy policy must, among other things, identify the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information. The privacy policy must also provide information on the operator’s online tracking practices. An operator is in violation for failure to post a policy within 30 days of being notified of noncompliance, or if the operator either knowingly and willfully or negligently and materially fails to comply with the provisions of its policy. When collecting personal information electronically, agencies must provide certain notices. Before sharing an individual's information with third parties, agencies must obtain the individual's written consent.

## ***Public Official Online Privacy***

This law prohibits posting or displaying on the Internet the home address or telephone number of any elected or appointed official, as defined, if the official has made a written demand not to disclose his or her information. Entities receiving such a demand must remove the information immediately and ensure that it is not reposted.

# ***Pretexting***

One ethical pitfall that occurs with some frequency is ***pretexting, which is the use of false pretenses as a method of discovery***. Pretexting generally involves the use of information about an individual, such as a social security number, ***to impersonate the individual*** and mislead information providers into giving out additional information that would generally only be available to the authorized individual. Attorneys, and private investigators, when gathering facts, must avoid making false or misleading statements representing that they are authorized to obtain personal information when in fact they are not.

In general, when a business entity, such as a private investigator conducts any type of ***deception***, it falls under the authority of ***the Federal Trade Commission (FTC).*** This federal agency has the obligation and authority to insure that consumers are not subject to any unfair or deceptive business practices.

Some of the many federal statutes that might possibly apply to pretexting pretexting include:

- 15 U.S.C. § 45 (Unfair methods of competition unlawful; prevention by Commission): By relying on both 15 U.S.C. §45 and 15 U.SC. § 53 (False advertisements; injunctions and restraining orders), the Federal Trade Commission can sue pretexters for fraudulent, deceptive and unfair business practices.

- 15 U.S.C. § 6821(a) (Prohibition on obtaining customer information by false pretenses): This part of the GLBA makes it illegal to access bank account information by making pretext phone calls to a financial institution or its customers. 15 U.S.C. § 6821 also prohibits submitting false documents to a financial institution, to obtain nonpublic customer information.

- 18 U.S.C. § 1039 (Fraud and related activity in connection with obtaining confidential phone records information of a covered entity): This statute generally prohibits telephone record pretexting and the sale of illegally acquired telephone records.

- 18 U.S.C. § 1028 (Fraud and related activity in connection with identification documents, authentication features, and information): Both this statute & 18 U.S.C. §1028A (Aggravated identity theft), prohibit a broad range of frauds in connection with identification documents.

- 18 U.S.C. § 1341 (Frauds and swindles): Covers frauds which use U.S. mail. It and 18 U.S.C. § 1343 (Fraud by wire, radio, or television), are the ubiquitous federal fraud statutes.

- 26 U.S.C. § 7213 (Unauthorized disclosure of information): Prohibits the unauthorized inspection or disclosure of U.S. tax returns or return information. Subsection (a) (4), entitled "Solicitation", expressly covers the illegal sale/illegal receipt of tax return information.

- 42 U.S.C. § 1307 (Penalty for fraud): Among other things, covers misconduct like eliciting social security numbers through pretext calls to the U.S. Social Security Administration.

- 47 U.S.C. § 222 (Privacy of customer information): Section (c) (2) of this Act generally prohibits telephone record disclosure absent "affirmative written request by the customer, to any person designated by the customer".

- A private investigator or information broker engaged in pretexting could face a Federal Trade Commission lawsuit or even criminal indictment. In Federal Trade Commission v. Victor L. Guzzeta d/b/a Smart Data Systems, an information broker stipulated to a final judgment which enjoined him from pretexting. The 2001 press release "As Part of 'Operation Detect Pretext' FTC Sues to Halt 'Pretexting'" indicated this information broker was accused of pretexting for financial records.

Until recently, a number of statutes covered pretexting activities only with respect to certain records. For example, ***the Gramm-Leach-Bliley Act*** of 1999, 15 U.S.C. § 1681q, ***prohibited the use of pretexting to acquire personal financial information*** from financial customers or institutions. The Fair Credit Reporting Act, 15 U.S.C. § 1681q, enacted in 1968, barred individuals from obtaining consumer information under false pretenses from a consumer reporting agency. Enacted in 1914, the Federal Trade Commission Act, 15 U.S.C. § 45, prohibited unfair or deceptive acts or practices affecting commerce, which covered many aspects of pretexting but did not give the FTC authority to seek civil penalties in certain cases.

No law specifically banned the use of pretexting to obtain telephone records until Congress enacted ***the Telephone Records and Privacy Protection Act (TRPPA) of 2006***, 18 U.S.C. § 1039, making it a crime to knowingly and falsely obtain "confidential phone records information," punishable by a fine and up to ten years' imprisonment. Congress's findings supporting the

TRPPA describe pretexting as fraud on a material fact that persuades someone to disclose information: pretexting occurs when "a data broker or other person represents that they are an authorized consumer and convinces an agent of the telephone company to release the data." Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, § 2, 120 Stat. 3568 (codified at 18 U.S.C. § 1039). Even greater penalties may be assessed under state law against the use of fraudulent statements to obtain consumer and employee telephone records information, as is the case with California Penal Code § 638, enacted several months before the TRPPA. Section 638 subjects any person who attempts to procure telephone calling records through fraud or deceit to a penalty of a $10,000 fine and up to one year of jail time.

Rules of professional conduct regarding pretexting provide some guidance, but also leave a considerable grey area that cautions restraint. Ethics rules do not

## ***HIPAA Privacy Rules***

The HIPAA Privacy Rule establishes national standards to ***protect individuals' medical records and other personal health information*** and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections

## ***Legislation Allowing Exchanges Between Insurers***

During the course of a claim investigation, the exchange of information between insurance companies can be very helpful to the insurer investigating a suspicious or fraudulent claim. However, such an exchange raises the question of whether an insurance company may be held liable for an invasion of privacy when it shares information from its claim files with any other insurance company.

Some states have enacted statutes which allow insurance carriers to release claim files to other carriers under certain circumstances, without written authorization of the insured. Florida Statutes, for example, provide that: "an employee whose responsibility it is to investigate claims relating to suspected fraudulent insurance acts may share information related to

persons suspected of committing fraudulent insurance acts with other employees employed by the same or other insurers whose responsibilities include the investigation and disposition of claims relating to fraudulent insurance acts, provided the department has been given written notice of the names and job titles of such designated employees prior to sharing that information."

Also, Illinois has enacted an Insurance Information and Privacy Protection Act, which provides in part as follows: "Disclosure Limitations and Conditions. An insurance institution, agent, or insurance-support organization shall not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is:...(C) to an insurance institution, agent, insurance-support organization or self-insurer, provided the information disclosed is limited to that which is reasonably necessary: (1) to detect or prevent criminal activity, fraud, material misrepresentation or material non-disclosure in connection with insurance transactions...".

Along with permitting insurance companies to provide information to other insurance companies, the Insurance Information and Privacy Protection Act provides immunity to an insurer who releases information.

In addition to immunity statutes, common law privileges in some states provide significant and substantive protection for a wide range of communications, including information disclosures, that otherwise would create civil tort liability. This "conditional" or "qualified" common law privilege exists to promote the free flow of information to further a legitimate private or public interest. The condition on the privilege is that the publication not be abused or widely distributed. This privilege provides substantial protection for an insurer's disclosures concerning fraud investigations.

An example of this qualified protection can be seen in **Caswell v. Manhattan Fire & Marine Ins. Co.** (1968), where a fire destroyed a portion of Caswell's restaurant in DeFuniak Springs, Florida. After investigating that suspicious fire loss, the National Board of Fire Underwriters published a report to its member insurance companies that contained a detailed account of its investigation into the cause of the fire. In discussing whether the report was privileged, the court stated that a communication is privileged when made in good faith and both the communicating party and the receiving party have an interest worthy of protection in its subject matter. Further, the court stated that the National Board had an interest in warning all of its member insurance companies of potential risks in insuring the plaintiff against fire loss and that the member insurance companies would have a legitimate interest in that information.

Therefore, a libel action will not be successful if based upon information shared between two companies when both entities have a common interest in the information and the communication is reasonably calculated to protect or further such common interest.

## ***Sunshine in Litigation and Confidential Settlement Agreements***

When a claim or lawsuit is settled, it is not uncommon for the parties to ***agree to keep the terms and provisions of the agreement confidential*** for a variety of reasons. However, the use of confidential settlement agreements has been criticized in recent years, particularly with regard to manufacturers of dangerous products.

Many states have enacted statutes or court rules that limit a party's ability to shield settlement agreements in secrecy.

The right to incorporate a confidentiality provision into a settlement agreement is governed by ***sunshine acts*** which prohibit a confidential settlement agreement which has the effect of concealing a "public hazard." A ***public hazard*** is defined in this statute as "An instrumentality, including but not limited to any device, instrument, person, procedure, product, or a condition of a device, instrument, person, procedure or product that has caused and is likely to cause injury." Therefore, this Act would apply primarily to products liability cases.

Settlement offers and statements made during settlement negotiations are generally privileged from discovery. Also, states with mediation rules of procedure or statutes usually make all discussions held during a mediation conference confidential and non-discoverable.

# ALL CLAIMS DATA BASES

Insurance data bases containing information on claimants may represent the single most effective loss prevention weapon available to insurers in combating insurance fraud. Not only can they help uncover patterns of possibly fraudulent claims activity but they can also alert insurers when those patterns appear in their markets.

## *ISO ClaimSearch*

Claim Search is the property/casualty insurance industry's system for improving claims processing and fighting fraud.

Each year, participating insurers and other organizations submit tens of millions of ***reports on individual insurance claims***. ISO stores those reports in a single database that helps insurers, self-insurers, law enforcement agencies, and state fraud bureaus detect and prevent fraud, evaluate risk, and process meritorious claims.

The ISO ClaimSearch system furnishes ***essential data for researching prior-loss histories, identifying claims patterns, and detecting suspect claims.*** ISO's Internet interface lets users conduct broad and flexible searches of the data.

With data on casualty, property, and vehicle claims, ISO ClaimSearch® is the insurance industry's most comprehensive resource for claims professionals. The ISO ClaimSearch database contains information from the former Property Insurance Loss Register (PILR) and Index System (bodily-injury claims), as well as the vehicle information databases formerly administered by the National Insurance Crime Bureau.

Now, all those claims are part of a single database that lets you search all lines of business and all types of claims simultaneously submitting hundreds of thousands of claims daily.

The ISO ClaimSearch database has three major segments — casualty, property, and auto. Each segment contains comprehensive information on claims submitted by hundreds of insurers and other users.

## *All Payer Claims Database (APCDs)*

These are large-scale databases that systematically collect ***medical claims, pharmacy claims, dental claims (typically, but not always), and eligibility and provider files from private and public payers.*** The first statewide APCD system was established in Maine in 2003. By 2008, five states (Kansas, Maine, Maryland, Massachusetts, and New Hampshire) had passed legislation and established APCDs. By the end of 2010, four additional states (Minnesota, Tennessee, Utah, and Vermont) did the same. Since 2010, state interest in APCDs has grown at a steady pace. Currently, more than 30 states have, are implementing, or have strong interest in APCDs.
Unfortunately, there are recent legal cases that may limit ERISA plans (most qualified pension plans) from submitting their health care claims data for use in the state's all-payer claims database (APCD).

## *Medical Index Bureau (MIB)*

The Medical Information Bureau (MIB) is a membership organization in which serves as a ***data bank of medical information*** for approximately

650 different insurance companies. MIB's members reportedly write 99% of the individual life policies and 80% of the health and disability policies sold in the U.S. and Canada. MIB maintains medical information on individuals, and member companies report significant consumer medical information to the MIB.

## ***LexisNexis Risk Solutions***

***Lexis Nexis*** is in the business of collecting and selling the information that commercial organizations, government agencies and nonprofits use to profile individuals, businesses and assets with data and analytic products.

The company is known for selling information for insurers to assess risk and streamline the underwriting process in 99% of all U.S. auto insurance claims and more than 90% of all homeowner claims. LexisNexis C.L.U.E.® Auto, is an underwriting database for the U.S. auto insurance market and represents a 99.6% industry contribution.

Formerly ChoicePoint and Database Technologies.

## ***Proprietory PI Databases***

Private investigators have access to databases others do not, such as TLOxp, IRB Search and CLEAR. All of these data bases essentially do the same thing, each one just has more up to date info than the other or more data.

PI blunders

# Fraud

## *Fraud vs Abuse*

Each year, fraud and abuse cost corporations, insurance companies and government billions of dollars. What is the difference between fraud and abuse?

*Abuse Defined*: Abuse is any practice that uses the system in a way that is contrary to either the intended purpose of the system or the law. This includes some behavior that is not criminal and some that is, most significantly fraud.

*Fraud Defined:* In the simplest terms, Fraud occurs when someone knowingly lies to obtain some benefit or advantage, or to cause some benefit that is due to be denied. If there is no lie, there may be abuse but it is not fraud.

The ***difference boils down to the person's intent***. Both activities have the same effect: they consume valuable resources. It is the intent that creates a fraudulent situation.

When fraud has been committed, the powers to be can seek federal criminal conviction, suspend licensing and/or impose monetary penalties. Abuse is considered a lesser offense, happening when people do not follow proper coding and billing guidelines. When abuse is committed, jurisdictions usually recovers payments made and impose civil monetary penalties can be imposed.

## *Some Forms of Abuse*

Merely filing an insurance claim that is not warranted or violating the rules of industry, in the absence of fraud (a lie) or kickbacks, may be abuse but it may not be criminal. Noncompensability per se does not constitute fraud unless the specific elements of fraud are present. For example,

***overtreatment by a physician*** might represent only a difference in opinion; although it could appear excessive and possibly abusive, it does not necessarily constitute fraud. Typical abuses of the system also include magnification of complaints or disability that fall short of an outright lie, or an overutilization of benefits. For example, soft tissue injuries give rise to subjective complaints that cannot be either proven or disproven.

The presence or absence of a specific, provable lie is the deciding factor. To separate fraud from abuse, it is necessary to look for the lie or misrepresentation, whether written or oral.

For example, ***returning to work while receiving temporary disability payment might be abuse***, ***or it might be fraud, depending upon the circumstances***. As the law now stands, claimants have no legal obligation to advise anyone when they return to work, nor do they have an obligation to certify their continuing disability status. If temporary disability payments continue when the claimant has returned to work--and no one ever asks the claimant "are you working?"--there is an abuse of temporary disability benefits, but there is no lie and therefore no fraud.

However, using the same example, if someone, such as the adjuster or the doctor, specifically asks the claimant "are you currently working?"--and the claimant replies "no" and thus lies, and that lie is relied upon to determine the amount and payment of temporary disability--there is fraud.

## ***Kickbacks***

Though not legally a fraud, offering or accepting ***kickbacks*** for the referral or settlement of an insurance claim for example, is a reportable and highly prosecutable crime. ***Kickbacks indirectly feed the problem of fraud*** and, as a result, cause damage to our society and our economy. Consequently, the legislature has determined that both fraud and the kickbacks that can contribute to it are punishable criminal acts; a single fraudulent transaction can be punished by up to 5 years in prison.

## ***Some Forms of Fraud***

In separating criminal fraud from abuse, remember these *key elements*:

- There is always a false representation--the lie.
- The lie must be intentional or knowingly made.
- The lie must be made for the purpose of obtaining a benefit the claimant is not due, denying a benefit that is due, or obtaining insurance at less than the proper rate.

- The lie must be material, that is, it must make a difference: "If the truth had been told, would you have done anything differently?"

Some common forms of fraud include:

### Insurance Fraud

Insurance fraud involves individuals who make false claims to receive insurance money or insurance companies who refuse to honor legitimate claims.

### Corporate Fraud

Corporate fraud includes issues like theft of information, compromised customer information, and a damaged reputation.

### Financial Fraud

Tax evasion, public corruption, health care fraud, telemarketing fraud, and terrorist financing all fall under Financial Fraud.

### Identity Theft

With identity theft, investigators will look for faulty loan or credit card applications, false withdrawals from bank accounts, dishonest use of calling cards, and using an alternate name to receive benefits.

### Internet Fraud

Internet fraud occurs when criminals attempt to take advantage of victims via the internet. This includes theft of personal information or fraudulent transactions that result in the significant loss of money.

### Corporate Slip and Fall

This type of fraud involves individuals who purposely organize a fall while inside a store in order to file a claim. They will go as far as to throw water on the floor in order to ensure a slip.

### Transit Fraud

This kind of fraud occurs when passengers on buses, subways, or streetcars don’t remain seated or hold rails and fall when the vehicle stops. There are also cases in which individuals allow their feet to be run over or stand in the way of the mirror.

### Ticket Fraud

With ticket fraud, a person will purchase tickets for a sporting event or concert that aren't legitimate. Often these tickets have already been used or don't exist.

### Mechanical Repair Fraud

Often a mechanic will call for fixes that are overpriced or not necessary.

### Expense Claim Fraud

When employees pocket runover business expenses they are committing fraud. Often, individuals will claim to stay in hotels costing $200 a night when in reality, they stay in cheap motels and keep the remainder of the money.

### Theft of Inventory

With theft of inventory, investigators will look into whether employees steal products or order more than the store needs. Sometimes employees will claim products are expired when they aren't so they can take the items home.

## ***Investigating Fraud***

Fraud continues to evolve and affect financial and institutions and personal lives in general. The opportunities and need to investigate fraud are also growing exponentially.

Today's fraud investigators need to have both a strong technical and business background as fraud schemes continue to become more complex. If you look at mobile devices, personal computers, laptops and all the complexities of evidence, organizations need people who can in fact analyze this and understand what this means in the context of a fraud investigation.

Investigators need to understand ***when files were written, what certain registry keys mean and what certain files on the system mean***, to give a few examples. And those same pros need to see incidents from the business side as well, being able to understand and translate that meaning to the technical side.

Sometimes it's an organization that claims it is a victim. They will need your assistance in figuring out ***how it happened***. In other cases, they've actually gone through the entire scheme, but they want an outside party to

help them ***quantify the loss***. In other cases, you will get calls where you are told they ***think they have a problem***.

One of the things that come up, and one of the dangers, is that organizations call and say, "We've already done a lot of the work and ***we couldn't find anything***. Can you come back and examine what we've already reviewed?" Sometimes the evidence, when we're talking about electronic evidence, has been altered because the organization hasn't necessarily relied on the proper mechanisms to analyze this evidence. One of the biggest obstacles is gaining access to the information that is need, and sometimes it's not necessarily an obstacle. It's just the complexity of the systems. Just think of how organizations manage their accounting systems, their payroll and their accounts payable. What information is available to review? It is a challenge in the beginning to get a grasp on all of the information that you can use, how you can use it and then converting this information.

One of the things that we see a lot of today is ***intellectual property theft***. Organizations have a lot of information that is of extremely large value to them. It can be ***client lists***. It can be ***documents***. It can be ***formulas***. It can be ***source code***. It can be just about anything that gives value to an organization.

Financial Investigator Jean-Francois Legault describes a particular instance:

*We were called in by an organization telling us that they suspected that an employee had in fact stolen a copy of all the source code that was developed by the organization; and this organization was a software developer. This code was all that they had as value for the organization. What we did is we actually seized this person's computer at work. We performed forensics, examining bit-by-bit copy of the person's hard drive. We maintained a chain of custody throughout this entire process and then we went on to analyze the forensic image of this computer to find that the person had uploaded all of the company's source code using automated scripts. He was doing it on a regular basis. He uploaded all this information online so that he could download it from home. We were able to, extremely quickly, within about 24 hours, establish how the information was transferred out of the organization, where the information went and we were able to identify what to do for this not to happen again. That was a successful one on the technical side.*
*On the financial fraud side, a lot of the work as I mentioned is in support of financial fraud investigations. So let's get back to the example I used earlier, where we had to convert these reports back to electronic format. That took quite a bit of time to get done, but once we had this information,*

*we were able to identify using analytics. That is using statistical analysis of the data that we had. We were able to identify all of the regular transactions which had been performed by a part within the organization, and since this organization was processing hundreds of thousands of transactions a week, we really had to rely on electronic analysis. Had we not been able to do that, we would still have people flipping through reports right now. That was a successful one from the standpoint of taking a large set of data and bringing it down to results, which were easily presentable to the stakeholders involved.*

## ***Recognizing Fraud***

Recognizing fraud is part of an investigator's job. Not knowing it is fraud could be it a blunder. Let's looks at some classic fraud scenarios:

***Staging A Death Scam*** **--** Before the days of computers and desktop publishing systems, staged deaths appeared more in fiction than in fact. Certainly, there were highly-publicized cases of people whose private planes went down in supposedly-impenetrable swamps or forests, people who later turned up alive long after hefty insurance claims had been paid. One case involved a scenario worthy of a Hollywood film. A young man, the rather never do well son of a prominent family, went off to Australia to make a life--and a fortune. He married there and fathered a child, gradually establishing renewed contact with his family back in the States. Then came a message from Australia: the young man had fallen overboard from a ferry crossing from the mainland to an island and had drowned. His grieving family sent plane fare to the widow and child, welcoming her into their midst and giving her a home.

Imagine their surprise when she told them that, far from being penniless, she was the beneficiary of a multimillion dollar life insurance policy which their son had only recently taken out. Since the job he had held in Australia did not pay much, his parents were impressed that he had invested so much in protection for his wife and child. When confronted alone, the wife, who had born the burden of suspicion from the start, confessed their scheme. Under his clothing, her husband had worn a survival suit that enabled him to stand the frigid waters and to breath until he could safely emerge on land. He had gone to a hide-out which they had set up, one stocked with all the provisions he would need. And there he had stayed, growing his beard and mustache, while his wife played out her part of the charade

The insurer was not so impressed. At first they suspected suicide, but found that they could not prove that to be the case. After a long investigation, they reluctantly paid the claim, but kept the case open. It

was a good thing they did. The wife banked the money and settled down into life in her new home. Months passed, and then the wife told her in-laws that she wished to go back to Australia where she had been born. This seemed a natural enough wish.

But when the young woman went to the bank and asked for a transfer to a bank in Australia, the bank complied with the insurer's request that they be notified if she made such a move. An insurance investigator then tracked her. Sure enough, not long after she and the child arrived in Australia, a man appeared in her life. Although his hair was a different color and he wore a beard and mustache, and weighed more than the dead husband had, the investigator felt certain that this man and the dead man were one and the same.

***Death Certificate Anyone?*** -- Desktop publishing has made it possible for people wishing to stage a death to produce authentic-looking copies of death certificates. And there are officials in some Caribbean and African countries who will accept a fee for certifying that a death has occurred. In a highly transient world, it becomes increasingly difficult to use the old procedures when an insured dies.

For example, an insurance investigator was asked to check out a life insurance claim for the death of a nine year old child who was supposed to have died in a taxi accident in a West African nation, where he was staying with his grandparents while his parents established themselves in New York. The policy was new, which was the first sign that something might be wrong. When an investigator went to the grandparents' home in the West African town, the child was playing in the front yard. A local official had signed the death certificate in return for a fee. In Los Angeles County, what look like official death certificates are sold on the streets for anywhere from $500 to $1000.

***Last Minute Change of Beneficiary*** -- Consider the situation described in a 1984 court case (Crobons vs Wisconson National Life). Here, even the agent was part of a last minute fraud to replace the name of a legitimate beneficiary with an unnamed beneficiary.

The case began as an ordinary life insurance sale between agent and client. Years later, however, the client became gravely ill and lapsed into a coma. Some family members soon realized that the beneficiary of the insured's policy was a relative whom they did not approve. The agent agreed to come to the hospital and change the beneficiary.

The agent's big mistake was agreeing to witness a change in beneficiary knowing full well that the client was in a coma. After death, the damaged beneficiary filed an action against all parties, including the agent. The beneficiary designation was eventually reversed.

***Slip & Fall Family*** -- A family in Las Vegas staged a variety of "slip and fall" and auto accidents in Illinois, Wisconsin, and Ohio. Eight family members admitted to collecting ONE MILLION DOLLARS in false claims. A man, working alone and using more than 24 false names, claimed to have staged more than 200 fake accidents across the country over a twenty year career of defrauding insurance companies with false claims. An insurance investigator assembled a paper trail of 71 slip-and-fall claims that had been paid to him by more than 50 different insurers and business, claims ranging from tripping on torn carpet to slipping on water to being bumped by cars backing out of store parking lots. Caught and charged with insurance fraud, this man could get twelve years in prison, as well as being fined $750,000 for each count of insurance fraud.

***Slip and fall scams*** are favorites of those out to get insurance benefits fraudulently, and some of its users go to great lengths to stage fake falls. Some squirt the floor with water from a hidden bottle- others have put fake blood up their noses with a syringe so that their claim of a broken nose will be more believable.

***The Fake Break Scam*** -- ***A less than ethical person has recently broken his or her arm***, which is in a cast. ***An accomplice removes the cast***, soaks the limb, then ***both go to the hospital for treatment, setting the stage for a false claim***. Or, an old back injury might be added to a new injury to increase the size of the claim.

Some false claims come from people who have pulled items from store shelves so that they fall on top of them and cause an "injury" for which they can claim benefits. This is the ***Yank Down scam***. Or people on the lookout for opportunities for false claims find a broken or obstructed sidewalk or stairway, and then stage a fall by tripping. And there are always those who ***Chew and Sue***, claiming they have found broken glass in their salad, bone in the soup, etc.

***The Auto Ring*** -- More elaborate are cases of staged auto collisions, which involve more than one person. In fact, so profitable are such collisions that rings are formed to do nothing but stage them. The National Insurance Crime Bureau describes the seven steps of a staged auto collision: first, the ringleader, who is usually a corrupt attorney or doctor, hires a "***capper***," the person who will actually coordinate the collision and recruit people to

claim injury as a result of it. Second, the capper promises financial rewards to get passengers involved. Third, the group makes a script of the details of the collision and the injuries they will claim. Fourth, the accident occurs, Fifth, the capper sends the cooperating passengers to an unethical attorney who will represent them in their claims. Sixth, the lawyer sends the passengers to an unethical medical provider who will inflate medical expenses for injuries which may not exist. Seventh, the attorney gets the insurer to agree to an out-of-court settlement for the victims involved. The resulting payment is divided among the people involved.

***Staged Auto Fraud*** -- Auto accidents can be staged by just driving a car off the road: after such an accident, the driver can claim that another auto forced him or her off the road. A man in Pennsylvania formed a group which included his wife, his father-in-law, his sister-in-law, two close friends and his baby sitter whose sole purpose was insurance fraud. For years this group ran cars into trees and poles, slipped and fell, lost valuables, and were robbed. They took in more than TWO MILLION DOLLARS from a multitude of insurance policies, making their biggest score from a single auto accident from which they collected $495,651 from 13 insurers. The ringleader bragged to a friend that every time he went to the hospital because of his accident-caused bad back, he made $80,000.

Nor is fraud in the health and accident field restricted to patients. There is only a certain amount of money that can be made filing fraudulent individual claims, There is far greater amount to be made forming fraudulent insurance companies and other such scam like these:

- A British citizen based in Atlanta used several insurance and reinsurance operations to take in an estimated $72 million in premiums for health, disability, and business insurance from 5,500 policyholders, and then refused to pay out claims.

- A man in Maryland build a complicated network of almost 50 insurance companies and sold spurious medical malpractice insurance to hundreds of doctors.

- Two brothers operated hundreds of medical clinics and mobile labs in Southern California that offered free physicals to get patients to come in. They then billed insurers for thousands of dollars per patient for serious medical problems which did not exist, and may have gotten as much as ONE BILLION DOLLARS from these false claims.

- A large national chain which operates psychiatric hospitals was charged with admitting thousands of patients to its institutions who did not

require hospitalization, and then treating them at inflated prices.

- A network of 100 in the New York metropolitan area, which included free-lance claims adjusters, employees of insurers, as well as policyholders, used staged accidents and inflated claims to defraud insurers of $43 million dollars before they were caught.
- One hundred seven defendants, including medical providers, police officers, lawyers and alleged bus passengers, formed a ring which staged bus accidents and then had people hop on, claiming injuries.

- A California firm set up "self-funded" health insurance plans from small businesses. It collected millions in premiums, moved the money into personal accounts, and left unpaid claims totaling $10 million.

***Hold Up Fiasco*** -- Joseph Francis Brooks, 46, orchestrated a hold-up with his cousin Pierre Lamont Taylor so that Taylor could file a false workers' compensation claim with his then-employer. On August 14, 2002, their elaborate plot was brought to fruition. Taylor was working for United Parcel Service (UPS) when the "assailant" approached him, firing a bullet into his right leg. Taylor reported the made-up ordeal to UPS and filed a claim with Liberty Mutual Insurance, UPS' workers' compensation insurer. In November 2004, Liberty Mutual doled out a lump sum disability payment of $250,000 to Taylor, who shared the wealth with Brooks.

A former friend of Taylor's tipped off Liberty Mutual to the scam, and Taylor eventually confessed to Maryland State Police. During the confession, Taylor said that he and Brooks arrived at the idea from "watching television." Brooks pled guilty to one count of conspiracy to commit insurance fraud, for which the court imposed a five-year suspended sentence and 18 months of probation.

***Swoop and Squat*** -- The swoop automobile cuts in suddenly in front of the squat car, forcing it to stop quickly to avoid hitting the swoop car. But the car behind the squat vehicle usually can't stop, and hits the squat victim from the rear.

***Drive Down --*** An innocent driver is trying to merge into traffic, and gets a signal from another driver that he or she will yield, and allows the victim of the scheme in. The innocent driver takes the signal as meant in good faith, and merges into traffic ahead of the signaler's car. That driver immediately smashes his or her car into that of the victim, and then denies that he or she ever signaled the innocent driver to merge.

Or a driver will drive a damaged car, and then claim it was damaged by someone who hit it and ran. Less effort is required by those who set up paper accidents: in these cases, a car owner whose vehicle is already damaged files an accident report with his or her insurer. The ***Drive Down*** is a scam that depends upon an opportunity presenting itself.- the driver wishing to set up an accident gets into a dual left turn lane at a high traffic intersection, and, if a driver in the inner lane drifts into the outer lane, the other driver sees to it that the two vehicles collide.

***Phantom vehicle scam*** -- In this one, a person creates phony documents to prove ownership of a vehicle, often a luxury car, or a classic antique. He or she then purchases insurance for the vehicle, and later, claims it has been stolen. One example of this scam involves a man who claimed that his entire collection--nine vehicles in all--had been stolen. The nine classic cars had been in a storage facility, or so he claimed. His insurer paid him $270,000 for the claim, and he then went on to make the same claim with a second insurer. Perhaps elated by his success, he over-stated his case, claiming this time that the tools had been stolen as well as the cars. But the receipts he submitted to prove the number and value of the tools were fake--upon closer investigation, the insurer determined that some of the information on the cars was also made up.

***Switching Drivers*** -- This occurs when the person driving a vehicle involved in an accident either does not have a driver's license, or has a record of accidents. The legal (and premium) consequences of being responsible for an accident are worse for the true driver than for a passenger who has a driver's license and no record of accidents. Before the police arrive, the driver and passenger switch places. Even when there are witnesses, it is sometimes difficult for people to accurately remember who was driving when they are excited or upset by the accident itself. And, if the people involved in this fraud keep to their stories, it is unlikely that witnesses' reports will be believed.

How does this defraud insurers? Simply because the vehicle premium one pays is based, in part, on one's record as a driver. If a person who has been in many wrecks is able to conceal this from the insurer, he or she will not be paying a premium commensurate with the amount of risk he or she represents, and is thus cheating other members of the insurance pool.

***Fake Fur*** -- Another popular scam is for a woman to wear a fake fur to a large party in a private home, and to call the hostess the next day claiming that when she went to retrieve her valuable mink, someone had taken it and left the fake fur in its place. Since the hostess can hardly be expected to remember exactly what each guest wore as she arrived, the hostess will

not be able to prove that the guest did not in fact wear a valuable coat, and will file a claim for the lost coat's value. Meanwhile, the mink coat is safely in its owner's closet, along with the fake that makes the scam work.

***Lost Rent*** -- In the aftermath of Hurricane Opal, a real estate agent claimed loss of rent for a property that had been destroyed. Although the sale had not yet been closed, the property had been sold: closure took place some three days after the storm occurred. Because the agent had been the owner when the hurricane hit, she worked with the adjuster to determine the amount of loss. The monies involved would be paid to the new owner, who could then make repairs. When the new owner received a copy of the claim, she noticed that the real estate agent had included several thousand dollars in lost rent.

There were two things wrong with this claim. First, the property had not been rented, and second, even if it had, the monies would not belong to the former owner. The new owner called the insurer to tell them that this part of the claim, as well as the part that listed physical damages, were incorrect. The physical damages had been over-stated: all in all, the claim was fraudulent to the extent of about $3,000.

***A Dead Horse*** -- This fraud involves the hired killing of expensive race horses who are literally worth more to their owners dead than alive. Astonishing as it might seem, one man made a living for nearly ten years by killing animals their owners needed to get rid of in a way that would make the insurance on them pay.

***Roping*** -- The process whereby a private detective creates a situation which ***causes a claimant to perform some physical activity*** so that the PI can then videotape or photograph the claimant. This practice is highly unethical.

PI blunders

# PI Ethics

## *In a Nutshell . . .*

Many PIs believe that ethics and the law are the same. It is important to realize that ***ethics are not laws***, ***yet they can be guided by laws***. Proof of this exists in the fact that you can be unethical yet still operate within limits of the law. And, laws are growing in numbers every day. The courts attempt to legislate protections from those without values or with values in opposition to what most of us would consider right and wrong. We have more laws than any one lawyer can ever know. And more and more lawyers seem to be necessary to handle the litigation that results from what seems to be a trend in "making others pay".

***Being ethical*** is indeed professional but the gesture goes beyond the mere compliance with law. It ***means*** being ***completely honest concerning ALL FACTS***. It means more than merely NOT telling lies because ***an incomplete answer can be more deceptive than a lie***. It means more than being silent when something needs to be said, because saying nothing can be the same as a lie.

## *A Moral Compass*

During times of fundamental change, values that were previously taken for granted may be strongly questioned. These are the times when the attention to business ethics is critical. Leaders, workers and agents must sensitize their actions -- they must maintain a strong moral compass.

John Kennedy Jr's last flight went wrong because he lost sight of land. In the growing dark around him, the horizon line became blurred and he became disoriented eventually flying his place right into the ocean.

***When nothing is stable or dependable, you also can lose your own sense of moral direction.*** When it happens, you start accepting ambiguity as real. You begin making up your own rules. You cut corners.

This is exactly how things started going bad at Enron. Accountants simply made-up their own accounting standards. They lied, cheated and waffled because it was to their economic advantage. Over time, they began justifying their unethical behavior as acceptable.

How can you keep this from happening to you? You can have a strong, unfailing sense of what is right and stay focused on it at all times. It's called ***integrity***. When you have it, it allows others to trust you, even when things go bad.

Kim Cameron, Professor of Organizational Behavior at the University of Michigan, says that it is not enough to simply encourage ethical behavior, honesty and integrity because these concepts in themselves imply an ***absence of harm***. A ***strong moral compass means that you strive behave in ways where self-interest is not the driving motivation***."

Too soft and fuzzy for you? Well take note, Kim's research proved that businesses with high scores on virtuousness significantly outperformed those with low scores. ***It pays to have a strong moral compass!***

Certified Fraud Examiner ***Dawn Lomer*** says there are ethical implications when you are obtaining and digging through personal information, but those often depend on who you work for and your position.

If you're an auditor or an accountant in a financial institution, you're more than likely not allowed to misrepresent yourself. Private detectives, law enforcement, intelligence officers… we use subterfuge and guile all the time; they are considered official resources of the trade, she says. At the same time, you have to have a moral compass, she adds. ***If you're a smart investigator and you've been doing it long enough, you know when to stop***.

## ***Confidentiality***

Some confuse the confidentiality with privacy. Privacy demotes the right to be left alone and control information about oneself. Confidentiality concerns the communication of private information and personal information form on person to another. If you surreptitiously collect information, you are ***intruding*** on an individual's privacy. If you pass on information without permission, you are ***violating confidentiality***.

The ***key ingredients of confidentiality are trust and loyalty***. As a PI, you gather personal and confidential information from and for your clients. You must be willing to take responsibility for handling this sensitive information. For instance, do you take measures to secure client data? Do

you unknowingly publicize a client's address, phone or e-mail address, exposing them to unwanted mail? Do you forward e-mail messages and attachments without reading them? Share passwords? Neglect to change your own password?

In a nutshell, it takes a combination of legal, technological and individual actions to preserve confidentiality.

## ***Some Things PIs Should Not Do***

If you know what side of the road to drive on you have the ability to recognize right from wrong. But, if no one ever told you to drive on the right side of the road you might not know it was wrong. Violating ethics is to know be told something is wrong and doing it anyway. So, an ethical PI needs to know what he cannot do first.

PINow.com did an excellent job in taking this further to describe exactly what a PI cannot do . . .

### Operate Without a License (If Required in That State)

Some states have extensive licensing laws for private investigators. In California, for example, an investigator must complete 6,000 hours of paid investigative work under a licensed investigator over the course of three years (or fewer hours over a shorter period of time depending on relevant advanced degrees and law enforcement background), get fingerprinted, submit an application packet, and pass the California Private Investigator Examination before they can work as a licensed private investigator.

### Impersonate Law Enforcement

In most states, private investigators cannot carry a badge, wear a uniform, or use any logo or phrasing that could imply that the investigator is a police officer or federal official. This prevents private investigators from misleading individuals about their association with government agencies. In some cases, private investigators will wear badges and uniforms that indicate they are private investigators, and they will often work in conjunction with local law enforcement or federal officials.

### Break the Law

In addition to limitations on how information can be obtained and other investigation techniques, a private investigator cannot harass a subject, trespass on private property, use bribery, hacking, pretexting (impersonating the individual whose records they are trying to obtain), or

other deceitful methods for obtaining information, and cannot break the law on behalf of their client or investigative purposes.

### Participate in Unethical Practices

An unethical practice would put an individual in danger, include obtaining information for non-investigative purposes, or using unscrupulous methods. One example would be locating an individual and providing that person's information to a stalker or person who might put that person's safety at risk. Another would be looking up information on former classmates or friends for personal purposes outside of an investigation.

### Trespass

A private investigator cannot enter a property, house, or building through illegal means, including breaking and entering. Though trespassing laws vary from state to state, in some jurisdictions the investigator must have permission from the owner before entering a property. Some private investigators in states like Illinois will be allowed an exemption to trespassing laws if they are working as a process server to serve legal documents.

### Enter Your Home or Place of Business Without Consent

A private investigator cannot enter your residence or business without consent, and if asked to leave must do so immediately. In line with this, they cannot use forced entry or lock picking to get inside.

### Tamper with Mail

Tampering with, opening, or destroying another person’s mail is a federal offense.

### Wiretap a Phone Without Consent

According to federal law, private investigators are prohibited from wiretapping, or monitor phone conversations, without consent from at least one of the individuals, depending on the state. 38 states in the United States, as well as the District of Columbia, have statutes that require one party to consent to the recording of a conversation, while the remaining 12 states require consent from all individuals involved in the recording. In many cases, a warrant is required to legally tap a phone, and private investigators will sometimes work with local police enforcement in order to avoid breaking any local or federal laws.

### Film a Subject Through a Window to a Private Home

Investigators are generally allowed to film exchanges and interactions that take place in public, but they cannot film the interior of private property through an open window.

### Record a Conversation of Which No Party Has Knowledge

Depending on the jurisdiction, in order to legally record a conversation at least one person involved must be aware that they are being recorded. In some states, both parties must be alerted ahead of time. A private investigator can, however, eavesdrop on a conversation that takes place in public or is naturally loud enough to hear.

### Place a GPS Tracker on a Vehicle Without Consent

GPS trackers can only be placed on vehicles with the consent of an owner. For example, if a husband wants to put a tracker on the car his wife drives, he can only do so if the car is in his name, not hers. An employer cannot place a GPS tracker on an employee's private car, but they can place a tracker on a company-owned vehicle, provided they have gone through the proper steps of consent.

### Hack Into a Social Media or Email Account

Hacking of any sorts just isn't what a private investigator does. Some investigators have software that allows them to access information about profiles, like when photos were posted and pulling data on where the person was at the time, but a private investigator will not attempt to gain access to a social media account that belongs to another person.

### Run a License Plate Without Reason

A private investigator cannot run a license plate unless they have a legal reason to do so. This means that a private investigator will generally run a license plate only for investigative purposes (i.e. when attempting to locate a person or conducting a background check) or for future use in a court proceeding.

### Run a Credit Check

As a credit report is considered private information, a private investigator must have written consent from the individual in order to run a credit check. If granted consent, a private investigator must also have a legal purpose for running a credit check before doing so.

### Obtain Protected Information Without Consent or Legal Purpose

Although they can find the location of the information, which can be helpful in asking for a subpoena, private investigators cannot obtain federally or state protected information without consent of the individual or a subpoena. These restrictions apply to various documents, including:

- **Bank Accounts**
  A private investigator can identify the location of bank accounts associated with a specific individual, but does not have access to specific information about these accounts. Unless they have obtained permission from the account holder, a private investigator must be granted a formal demand such as a court order to legally access the files.
- **Financial Records**
  Account-specific information, like transaction history, can't be obtained without either a court order or permission from the card or account holder.
- **Phone Records**
  Through legitimate investigative methods, an investigator can find out what carrier or person is associated with a given phone number, but because phone records are considered private and protected by both federal and state statutes, a private investigator cannot obtain those records without a court order or subpoena.

### Make a Legal Arrest

In the U.S., private investigators are not authorized to make an arrest. However, in some countries (the U.S. and Canada included) certain circumstances allow an individual not associated with law enforcement to make a citizen’s arrest. Some states require written consent for a private investigator to make a specific arrest, while other jurisdictions only authorize citizen’s arrest when the individual is endangering the public, or when a federal offense is witnessed. Citizen's arrests are rare in the investigative field. Some states will allow a private investigator to serve an arrest warrant under special circumstances.

### Obtain Cell Phone Records Without a Warrant

An investigator cannot access cell phone records without a warrant or consent of the individual who holds the records. In most instances, a private investigator can get comparable evidence through other methods.

*NOTE: This list is not meant to cover every circumstance and laws vary from state to state.*

## ***Consequences***

When things go bad, someone will pay the price. In previous material we covered penalties, fines and even jail sentences for violations of laws and licensing.

Beyond these issues, there is an important consequence of wrongdoing that every PI needs to keep in mind.

- Unethical / illegal actions may lead to suspension of or other action against the private investigator's license.
- Evidence obtained as a result of misrepresentation, illegal or unethical actions might be excluded in civil proceedings.
- Victims of torts may seek damages against investigators.
- Victims of intentional torts may seek damages against attorneys or others hiring the investigators.
- Victims of negligently supervised or entrusted investigators may seek damages from attorneys or others hiring the investigators.

PI blunders

# PI Liability & Insurance

## LIABILITY

The **Civil Code** in most states affords every person a qualified right against an ***investigator's tort liability***, i.e., it appears that ***anyone can sue a private investigator*** for a real or alleged wrongdoing, ***no investigator-client privilege or private investigator work product doctrine*** exists to provide PIs immunity from a claim.

Investigators may be liable for torts such as fraud, trespass, invasion of privacy, battery, and false imprisonment. Likewise, investigators may be liable for violating statutes such as the Uniform Trade Secrets Act. Other persons may be vicariously liable for any of this wrongdoing by retaining an investigator, especially if the investigator had advertised his or her capabilities for working undercover.

Further, in the absence of a client's consent, an investigator, in most states, ***shall not divulge***, except as he or she may be required by law, any information acquired to law enforcement officers. Thus, investigators have a ***duty of confidentiality***, but case law expressly leaves open the question of whether this duty creates any corresponding privilege against discovery. So, without the certainty of a privilege, private investigators face the possibility that their work product and communications with clients might be discoverable. Can you see some conflicts developing here?

However, some say investigators are not entirely vulnerable in this area. There are two grounds for objection to discovery that investigators may be able to utilize. First, an investigator (or the investigator's client) may assert a constitutional privacy objection. Second, while investigators might not have their own protections, investigators retained by lawyers might avail themselves of the lawyers' protections. Investigators retained by lawyers in litigation ***may assert the attorney work product doctrine to prevent disclosure of the lawyer's or the investigator's "impressions, conclusions, opinions, or...theories."*** Similarly, communications between a lawyer's client and an investigator who is the lawyer's agent may be protected by the lawyer-client privilege.

Lawyers retaining investigators face their own set of prohibitions and risks. For example, a lawyer may not compensate an investigator by "directly or indirectly" sharing fees from the lawyer's client. Also, lawyers must be careful not to violate professional conduct rules, which prohibit a lawyer from "directly or indirectly" communicating "about the subject of the representation" with a party represented by another lawyer.

A violation of such a rule can occur if a lawyer engages an investigator to communicate with a party that the lawyer knows to be represented by another lawyer.

In **Jorgensen v. Taco Bell Corporation**, the court of appeal found no violation of these rules when a prospective plaintiff's lawyer retained an investigator to interview a corporation's employees seven months before the plaintiff sued the corporation. The court expressly rejected the corporation's argument that the lawyer "should have known" that the corporation "would be represented" or had "house counsel." However, the Jorgensen court implied that a closer question would be presented if the investigator had conducted the interviews "on the eve of the filing of the lawsuit" and that a lawyer would violate the law if the lawyer hired an investigator to communicate with a represented adversary or represented witness after filing suit.

# INSURANCE

Trusted Choice.com does an excellent job in describing the types and need for PI insurance.

The right insurance for private investigators will vary from one business to another. If you are a PI, you may need a number of different insurance policies to completely cover your risks. For starters, most PIs require the same general types of insurance as any business:

- **General liability:** Covers your risk of bodily injury or property damage to another person or business in the course of doing business.
- **Property coverage:** If you own your building, you may need this coverage to protect your business property.
- **Auto liability:** Commercial vehicle insurance will protect you whether you drive a business vehicle or drive a personal auto for business.
- **Workers compensation:** You may be required to carry this coverage, whether or not you have employees. It provides protection

against job-related injury or illness suffered by you or one of your employees. Laws vary by state.

In addition, depending on the type of work you do and whether you hire employees, you may need a number of specialized coverages, such as:

## ***Assault & Battery Coverage***

Protects you if you are ***accused of physically harming another person***. Some private investigator work can involve situations where physical confrontation may be necessary. For example, you may face this risk if you are involved in any of the following:

- Executive and celebrity protection
- Retail store security
- Hotel security
- Investigating domestic issues

In order to get the proper protection, you will need for your insurance company to amend or waive the assault and battery exclusion in a standard general liability policy. Only a company specializing in private investigator liability insurance will consider taking this step.

## ***Care, Custody & Control Insurance Coverage***

Some of the work done by private investigators involves ***guarding or securing property***. For example, a department store might hire you as a PI if it is experiencing substantial inventory shortages and suspects that some of its employees are to blame. As the private investigator hired to look into the situation, you would have access to the entire store. A difficult insurance situation can arise if you inadvertently cause damage to some of the store's property while looking for evidence.

A standard general liability policy excludes liability for property in the "care, custody or control" of the insured. Your insurance carrier could well exert this exclusion in this scenario. The solution is to work with your insurance agent to create an amendment to the basic policy, providing a sub-limit for property damage otherwise excluded by the care, custody and control provision.

This is highly technical work and you need a knowledgeable agent who specializes in commercial coverage to help you through this and other concerns pertaining to private investigator insurance coverage.

## ***Invasion of Privacy Coverage***

Claims of "invasion of privacy" are a definite professional risk for private investigators.

## ***Fidelity Bonds***

This coverage protects you against the deeds of unscrupulous employees.

## ***A Word On PI Errors & Omissions Insurance***

A great deal of the work done by private investigators involves researching information or developing data that will be used by others to make significant decisions, such as choices regarding hiring or firing, marriage, contracts, or whether or not to do business with another party.

As a private investigator, you may find yourself responsible for a financial loss by another person or business in a number of ways. For example, you may face this risk if:

- You do ***an inadequate job of researching*** a given situation;
- You provide information that results in a poor decision by a client;
- You neglect to provide critical information that results in a client's choice of a contractor, who then does not perform quality work.

These situations ***will not be covered by a general liability policy*** because there is no bodily injury or property damage involved. Only a professional liability policy will protect you in this situation. "Errors and omissions" or "E & O" risks are inherent in any business that provides consulting services or provides information and advice, and this is particularly true of PIs.

Professional liability for private investigators may be one of the most important coverages you can buy to protect yourself against liability risks.

PI blunders

# PI Blunders

The line between legal responsibility and misconduct is often thin. Few investigator can say they have never "crossed the line". . . went out on a limb for a client . . . looked the other way or fudged just a little when serving a client.

These indiscretions, hopefully tiny and few in number, usually lead to nothing. But when something goes wrong an agent's biggest fear comes true. . . a lawsuit for breach, professional misconduct, trade practice violations, trespass, invasion of privacy and much more.

Anyone involved in one can tell you its a living nightmare. Beyond the financial liability, victims are dragged, kicked and punched through the legal maze known as our "justice system". It is the domain of judges, attorneys and plaintiffs, a place no one cares to revisit. If you are worried about this happening to you, this section of the course will be really important to you.

If you think it can't happen, you should know that a portion of the PI population is sued each year, and nearly three-fourth's of these claims are "frivolous", virtually beyond your control. The longer you stay in the business and the more expertise you develop, the bigger the target you become. YES, the litigation explosion is coming to a neighborhood near you and it might just end up on your door-step.

The reason this threat is greater now than ever before is a matter of public record.  Everyone wants a big payday.  Even insurance companies are fighting back, evolving from an almost cavalier attitude in settling nearly every claim, to a wholesale frenzy for standing firm . . . taking plaintiffs to trial. Of course, this has come at the great expense and frustration of every personal injury attorney who liked the old methods of settling a claim . . . before trial, but hated the big battles and courtroom antics glorified in "LA LAW". For the more lucrative cases, attorneys are pushing back. Others are looking for greener pastures . . . directions where there is less resistance.

Even if you are lucky enough to avoid a claim for now, ***every time another PI is sued, it gets closer to you because our court system makes legal decisions based on precedents***. Litigation experts believe this system is destined to expand liability to higher and higher levels because each decision in the chain sets the stage for the next step of expansion.

This, coupled with the willingness of judges and juries who sanction the expansion of legal theories in our courts, means that liability gets closer and closer to you for smaller and smaller violations. As a matter of fact, you will learn from these pages that you can be held responsible for matters related to the fact that you are a licensed and your client is not!

You will also learn that the root of most conflicts lies in the inability to understand statutory and fiduciary duties. Don't panic if you suddenly discover that you have made some of these same mistakes . . . most investigators are guilty of something. However, don't believe that because you haven't been sued you are in the clear. Thanks to our legal precedent system, ***seemingly innocent events of the past are potential big problems today***. To survive it all you need to justify your actions, manage your errors and plan ways to avoid making them in the future, i.e., you must change the way you do business.

There are many suggestions and guidelines that accrue from reading about the mistakes of others. However, don't depend on this book to be a universal solution for avoiding litigation or handling your own defense, rather it is a big, bright WARNING BEACON. Study it, learn from it, but get legal advice before taking any action to reduce or defend a possible conflict.

Now that we know a little about laws and ethics, let's delve into some specific issues . . . even blunders . . . that PIs have made. Knowing what others did wrong provides a valuable lesson toward moving in a better direction.

## UNLICENSED INVESTIGATORS

As we said in the beginning, the majority of states that do require PIs to be licensed focus on ***permissible activities*** such as:

- Overt investigations, in which investigators identify their roles and principals and do not otherwise mislead or deceive anyone.
- Public records searches.
- Physical observations, measurements, and the like.

- Protection of a person, if it is "incidental" to an investigation and if the investigator complies with the PIA's firearms and insurance requirements.
- Surveillance, even if covert, provided that investigators do not trespass or invade privacy.

Unlicensed persons who represent themselves as licensed or act as private investigators are committing a misdemeanor and may be jailed (up to one year) and fined ($5,000 or more). In addition, such as a lawyer who ***knowingly engages*** an unlicensed investigator or who conspires to have an unlicensed person operate as an investigator also may have committed a misdemeanor with the same penalties.

Public prosecutors may seek civil remedies against unlicensed investigators, their coconspirators, and anyone who knowingly engages such investigators.

Civil remedies include an injunction (for which prosecutors need not "show lack of adequate remedy at law or irreparable injury"), a civil fine ($10,000 or more) and reimbursement of investigation expenses. Civil actions by private parties who have been wronged can also be pursued as unlawful business practice, an exclusion of evidence the unlicensed individual obtained and a rescinding of all investigator fees.

This does not imply that unlicensed individuals are prohibited from performing any investigative tasks. A ***licensed manager***, for example, can direct, control, charge, or manage unlicensed personnel. However the manager is ***legally responsible for the good conduct...of his or her employees or agents*** and only the licensee, manager, or other person authorized by them may submit a written report...to a client.

But, not everyone plays by the rules. Here are some PI Blunders that focus on unlicensed activities:

## ***False Representation***

A former police officer decided to use a Colorado address as his base of PI operations. (At the time, Colorado did not have a PI license requirement.) He ***falsely identified*** himself as a licensed private investigator and posted

fake reviews of his various businesses on "investigator for hire" websites as well as referral sites. The unlicensed individual used ***these fabricated reviews to mislead potential clients*** into believing his business had nationwide offices and investigators, when in fact, he operated out of a small office in California with less than

five employees . . . most were family members. By the time the dust settled, he pleaded guilty to 17 felony counts of grand theft by false pretense, 11 felony counts of fraudulently using an access card, two felony counts of identity theft, four felony counts of possession of a firearm by a felon in his office stemming from a conviction for stalking, six felony counts of obtaining services through false pretenses, one felony count each of perjury by declaration, computer access and fraud, and possession of ammunition by a prohibited person in his employ, one misdemeanor count each of unlawful representation as a private investigator, engaging in the business of private investigation, and doing business without a valid license with sentencing enhancements for aggravated white collar crime over $100,000 and property damage over $65,000.

## ***Consultants Not Acting As PI's***

Beyond the statutory exemptions, some case law holds that at least some experts, consultants, and others performing investigative work also need not be licensed. However, these decisions are neither recent nor fully developed.

In **Kennard v. Rosenberg**, two licensed chemical engineers and a retired city fire inspector sued Nate Rosenberg to collect their professional fees. Rosenberg had been indicted for arson of his nightclub. His lawyer ***retained the fire inspector after the inspector*** had stated that he was not licensed and "acted only in the capacity of consultant or an expert." The lawyer also ***retained the engineers who conducted tests***, examined photographs, prepared court exhibits, and--along with the inspector--attended the preliminary hearing and consulted with the lawyer.

When all the work was done, the lawyer refused to pay the consultants. His defense for not paying the three was that the PIA (Private Investigator Act) for their state required them to be licensed as private investigators. The trial court rejected this defense, and the court of appeal affirmed. The appellate court, announcing that ***"none of the [three experts/consultants] were engaged in the private detective business,"*** reasoned that the engineers were licensed engineers and thus "***were authorized to make investigations in connection with that profession***...." Moreover, the court continued:

The private investigator license law was not intended...to place a limitation on the right of professional engineers to make chemical tests...and to testify.... A physician, geologist, accountant, engineer, surveyor or a handwriting expert, undoubtedly, may lawfully testify in court in connection with his findings without first procuring a license as a private detective,

and...a photographer may be employed to take photographs of damaged premises for use in the court without procuring such a license. Thus, experts--particularly in recognized, forensic disciplines--may be retained to investigate matters in litigation without being licensed as investigators.

## ***Unlicensed Surveillance Is Authorized***

In **Mason v. Peaslee**, Russell Mason, an unlicensed sound engineer, sued his client Margaret Peaslee after she refused to pay his fees. For eighteen years, Mason had taped "meetings..., speeches,...and personal conversations" for corporations, attorneys, individuals, and law enforcement agencies--"in many instances" without the subjects' knowledge. Peaslee requested Mason to install recording devices in her husband's office to determine if the husband was "dishonest and secreting money" or "a sex pervert." Mason did so. The trial court granted a nonsuit on the ground that the contract was illegal, because Mason lacked an investigator's license.

On appeal, the court of appeal reversed the decision on two grounds. First, the ***state may not demand a PI license from someone who is "engaged" in a low frequency of action*** as part of an investigation. The trial court "could not draw the inference that [Mason's] ***work in recording conversations for others was done in such a manner as to constitute doing business as a private investigator***...." Second, the court noted that ***Mason did not personally "conduct any investigation***...." Indeed, according to the court, "Mason...merely furnished to [Peaslee] the devices with which she could carry out her own investigation and...in operating the devices he acted not as an investigator but as one employed by [Peaslee] to render technical aid to her in operating the devices which she had rented from him."

The Mason court seemed to hold that (1) an investigator need not be licensed to conduct a one-time investigation, and (2) merely furnishing and operating surveillance equipment is not an investigation. Mason's holdings, though, appear unsound. For example, if the word "engage" connotes "frequency," then, using the same logic, an unlicensed person could perform dental surgery on one occasion, because dentists' licenses are required only for persons who "engage in the practice of dentistry...." Unsurprisingly, no court has ever cited Mason's interpretation of the law and it ***would be risky for unlicensed investigators or anyone contemplating retention of an unlicensed investigator to rely on it***.

## ***Unlicensed Investigators Can Do More Than Licensed PIs?***

In **Wayne v. Bureau of Private Investigators**, a case that had more to do with a licensed PI lying about his identity, the courts concluded that persons exempt from the PI laws enjoy not only freedom from licensing, but, ironically, perhaps greater latitude than licensed investigators in undercover investigations. To be sure, exempt persons still must avoid torts and statutory violations, but Wayne holds licensed investigators to higher standards. For example, Wayne suggests that the law's "dishonesty or fraud" language could--at least in part--encompass silence, does not expressly require that the victims' reliance be reasonable, and does not mention damages. By contrast, actionable fraud excludes misrepresentations by silence except in limited circumstances, requires that the reliance be reasonable, and requires actual damages. Thus, in Wayne, as well as in the typical types of scenarios in which businesses use undercover investigations, exempt persons might have been able to conduct the investigations, even if licensed investigators could not. In sum, exempt persons might be able to investigate in ways that avoid tort or statutory liability, but licensed investigators must also reckon with Wayne.

# INVASION OF PRIVACY

The right of privacy, as an independent and distinctive legal concept has two main aspects: (1) the general law of privacy, which affords a tort action for damages resulting from an unlawful invasion of privacy, and (2) the constitutional right of privacy which protects personal privacy against unlawful governmental invasion. The general law of the right of privacy, as a matter of tort law, is mainly left to the law of the states.

***Invasion of privacy*** consists solely of an ***intentional interference*** with a person's interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.

The invasion may be by ***physical intrusion*** into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff's room in a hotel or insists over the plaintiff's objection in entering his home. ***Or***, it may also be by the use of the defendant's senses, with or without mechanical aids***, to oversee or overhear the plaintiff's private affairs***, as by looking into his upstairs windows with binoculars or tapping his telephone wires.

***Other examples of invasion of privacy*** may also be by some other form of investigation or examination into his private concerns, as by ***opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents.*** The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined.

Most states have common law, constitutional, and statutory protections against the invasion of privacy. The statutory protections are numerous and scattered, ranging from an antipaparazzi law (banning certain photography of "personal or familial activity"and an antistalking law to a ban on the use of a "telescope, binoculars, camera,...or camcorder" to view the interior of a "bedroom, bathroom,...or the interior of any other area in which the occupant has a reasonable expectation of privacy." To complicate matters further, federal privacy statutes also exist. Let's look at how these laws create issues for investigators.

## *PI Found Guilty of Trespass*

**Miller v Miller** (1994) centers on a divorce case between Terry and Annette Miller. Following an initial separation, the wife moved out of their home which was titled only in the husband's name. The couple's separation agreement provided that plaintiff Terry Miller had sole possession of the Buck Lane house. In February 1992, the couple attempted a reconciliation during which defendant Miller moved back into the Buck Lane residence. This reconciliation attempt failed and she moved out after a few days. Plaintiff has testified in his affidavit and in a previous criminal trial that the couple agreed that he would have exclusive possession and control of the Buck Lane house and that defendant Miller would not return unless she was invited or he was present. She returned her key.

In February 1993, defendant Annette Miller ***hired Gary Brooks, a private investigator to install a surveillance camera to be placed in the residence***. Brooks hired defendants Massaroni and Hite to assist. Brooks also contacted a locksmith who met defendants Miller, Brooks, and Massaroni at the house and made a key to the house. When ***plaintiff was not home***, ***the investigators entered the house that was not titled to the wife (unauthorized), altered the wiring (neither was a licensed electrician), and installed a hidden videotape camera in the bedroom ceiling***.

A suspicious pile of dirt on the floor prompted the husband to engage his own private detective who helped him locate and remove the camera and videotape. They watched the videotape which showed pictures of plaintiff in his bedroom, getting undressed, taking a shower, and going to bed. The tape also showed defendants Brooks and Hite in plaintiff's bedroom. After discovering the camera, plaintiff became fearful for his life, moved out of his house temporarily, and carried a loaded shotgun in his car. He suspected he was being investigated by federal officials and went into hiding. Later, defendants Miller, Massaroni, and Hite went to the house to change the videotape and discovered that the camera and tape had been removed.

In mid-February 1993, defendant Miller, representing herself as a resident, asked the local post office to hold the mail for 2400 Buck Lane. Afterwards, she regularly picked up plaintiff's mail at the post office, sorted through and discarded portions of it, and placed the remainder in plaintiff's mailbox. ***Defendant investigator Massaroni picked up the mail for her once***. Postal employees discovered that defendant Miller was not living at the house and contacted plaintiff.

This was the final straw. The plaintiff filed a suit asking for declaratory judgment and compensatory and punitive damages for invasion of privacy, intentional infliction of emotional distress, trespass, and damage to real property. Plaintiff later amended his complaint adding investigator Massaroni and asserting additional claims for invasion of privacy.

Plaintiff alleges that ***defendants invaded his privacy by their intentional and highly offensive intrusion upon his seclusion, solitude, or private affairs. In his first and eighth causes of action, plaintiff asserts that defendants violated his privacy by breaking into his home, installing a hidden video camera in his bedroom, and taking pictures of him while in his bedroom. He asserts that they performed these acts wilfully, intentionally, maliciously, and in reckless disregard and indifference to his privacy rights.*** In his seventh cause of action, plaintiff asserts that defendants Miller, Massaroni, and Brooks Investigations, Inc., through its agent Massaroni, wilfully, intentionally, and maliciously invaded his privacy ***by intercepting and opening his mail without authorization.***

Because the couple agreed, in a written separation agreement, that plaintiff would have sole possession of the Buck Lane premises. The couple tried a reconciliation, but it didn't work. After the reconciliation attempt failed, plaintiff instructed defendant Miller (the wife) not to enter the premises without his consent.

To prove trespass, a plaintiff must show that the defendants intentionally, and without authorization entered real property actually or constructively possessed by him at the time of the entry. The ***essence of a trespass*** to realty is the disturbance of possession. If plaintiff had the right of possession at the time of the entries and if defendant Miller had no such right, any entries made by her without plaintiff's consent, or by the other defendants, constitute trespass. This is true even if defendants entered the premises with a bona fide belief that they were entitled to enter the premises.

# CONFIDENTIALITY

## *Can A PI Contact An Opposing Attorney?*

Is it illegal for a PI to have contact with a subject who has an attorney? Is it harassment? Also, if they do, is it the PI's attorney who gets 'punished' by losing his license rather than the PI? If the subject doesn't have an attorney when he comes into contact with the PI, couldn't he just go get an attorney and indicate he had been harassed by the PI?

The legal system has gone to great lengths to protect and enhance the institution and ***confidentiality of the lawyer-client relationship***. The reason that it is illegal for a PI who is working for Attorney A (and A's client) to have contact with Attorney B's client is this institution and confidentiality.

Why might an attorney be accountable for his/her PI contacting the client of an opposing attorney?

The legal idea behind this is simply that the boss is ultimately responsible for the employee's actions. In states where PIs are licensed, it may indeed be the case that both the attorney and the ***PI would be punished for intruding on another attorney-client relationship*** (one needs to check if this is the case with that state's PI licensing statutes or that state's attorney's ***code of professional responsibility***.

Could a person hire an attorney after being contacted by a PI, and then claim harassment? A person ***cannot retroactively create an attorney-client relationship***, but anyone can claim harassment by another third party. For the sake of a story, could a character talk to a PI, then afterward realize they said too much and not want what they said to that PI be admissible as evidence? Again, this character couldn't retroactively claim attorney-client privilege, but that character might accuse the PI of harassment, which would cast doubt on the reliability of that prior interview

as evidence. In other words, a lawyer wouldn't want to "dirty up" their case with evidence of an interview that has serious concerns about its reliability.

## ***PI Talked With A Witness He Should Not Have***

A good case to illustrate problems that occur when interacting with opposing counsel is **United States v. Smallwood** (2005). The initial Smallwood case involved a drug dealer (Smallwood) who was represented by a court-appointed attorney. ***Investigators recorded a telephone interview with a critical prosecution inmate-witness, without the knowledge or consent of that witness or his appointed counsel***. At issue, therefore, is whether an investigator hired by a lawyer must abide by an attorney's ethical obligations in not to (i) communicate with a person known to be represented by opposing counsel regarding the subject of the representation, or (ii) electronically record a conversation with a third party without the full knowledge and consent of the other party. The court who hired the investigator, refused to pay the PI's bill until the ethical issues were resolved.

Here's the background: The court-appointed (defense) attorney retained the investigative services of a PI to conduct normal backgrounds and interviews. Shortly before trial, the court appointed attorney learned that her client in another case and an inmate at the regional jail, knew a prime witness (at the same jail) who was scheduled to testify against Smallwood. The inmate told the attorney that the witness had approached him with offers to sell information that the inmate might use to testify as a government witness, and thus receive a reduced sentence. Concerned that the witness might attempt to offer false testimony against Smallwood, the court appointed attorney made the decision to send the Investigators to speak with the inmate. It did not seem improper, because she also represented the same inmate.

The Investigators traveled to the jail where they met with the inmate and learned that the witness inmate had repeatedly tried to sell to other inmates information concerning a variety of criminal activity that might be used to win government assistance in obtaining a sentence reduction. The inmate asked what to tell the witness in case he wants a quick answer. The investigator said to delay him...pretend you have to ask your uncle for the money.

In view of this conversation, the Investigators decided to contact the defense attorney as soon as possible to discuss an appropriate course of action. Yet, before they could do so, the inmate and witness called the

investigator asking to speak to the "uncle" (which of course was the investigator). The PI taped the conversation but did not disclose who he was or who he worked for until the call was over.

During the Smallwood trial, the court-appoint defense attorney used the tape to impune the testimony of the witness who was testifying against Smallwood. The prosecutor, who was using the testimony of his witness to nail Smallwood, cried fowl as the investigators spoke to his witness without permission.

The court denied payment of the investigators pending ethical hearings. At these hearings, the court discussed the fact that a defense attorney would not be allowed to interview, much less tape record, a prosecutor's witness without permission. And ***an investigator for the defense should be bound by the same rules***. It also doesn't matter that the witness initiated the conversation . . . it's still wrong.

The court determined that ***an investigator or other assistant has an affirmative duty to learn and abide by a lawyer's ethical obligations; he may not simply claim ignorance of these duties and proceed to act with impunity***; instead, investigators or other assistants should seek direction from their lawyer-employers when presented with areas of ethical ambiguity or uncertainty.

In the end, the PI lucked out as the court said the defense attorney did not order the PI to have subsequent conversations with the witness . . . it just happened. So, it was clear that neither the lawyers nor the Investigators knowingly engaged in any improper conduct. And significantly, the investigators' itemized statement reflects that the interview with witness was a comparatively small portion of the services the Investigators performed on Smallwood's behalf. Accordingly, the PI got paid his nearly $7,000 fee.

## ***No Contact Rules***

How far can an investigator go in making undercover interviews? Sometimes it comes down to how much and the type of contact is acceptable. **Gidatex v Campaniello** (1999) is a classic case where no contact rules were put to the test.

*Summary by Roy Simon is a Professor of Law at Hofstra University School of Law and Director of Hofstra's Institute for the Study of Legal Ethics*

Suppose you represent a furniture manufacturer of high quality designer furniture in a suit alleging trademark infringement, Lanham Act violations, and unfair competition. You want to prove that the defendant, a furniture store, is engaging in "bait and switch" tactics by advertising your client's brand and then palming off" furniture made by other manufacturers as equal in quality to your client's products. Practically speaking, the only way to prove that the store is "palming off" is to catch sales clerks in the act. But how do you do that? May you ethically send undercover investigators to the defendant's store posing as customers? May the investigators secretly record their conversations with the sales clerks? Will the secret recordings be admissible in evidence at trial?

In **Gidatex, S.R.L. v. Campaniello Imports, Ltd**. (1999), "Where the Facts Parallel Our Hypothietical," Judge Shira Scheindlin answered "yes" to all of these questions. But lawyers should tread carefully over this ground. The Gidatex decision seems narrowly direct to situations where (a) the only way to obtain the necessary evidence is by using undercover investigators, and (b) the public policy in deterring the defendant's conduct is strong Judge Scheindlin found these criteria satisfied in the particular factual and legal context of the Gidatex case, which involved trademark litigation. In other types of cases — for example, in typical personal injury cases, divorce matters, or routine breach of contract suits — the rational for Judge Scheindlin's holding might not apply.

**Amusing Facts**

The facts of the *Gidatex* case were amusing. Gidatex owned a federally registered trademark, "Saporiti Italia," for a brand of furniture. The defendant, Campaniello, a well-known store on 57th Street in Manhattan that sells designer Italian furniture, had been a licensed sales agent of Saporiti Italia furniture for 20 years, until Gidatex terminated Campaniello's agency in 1995. When Campaniello continued to use the Saporiti Italia trademark in its advertising after its termination, Gidatex sued Campaniello for Lanham Act violations, trademark infringement, and unfair competition. At trial, Gidatex sought to prove that Campaniello engaged in "bait and switch" tactics by luring customers into its showrooms with signs and advertisements bearing the Saporiti Italia trademark, and then selling them furniture produced by other manufacturers. To prove the store was "palming-off" or "passing-off," Gidatex's counsel hired private investigators to pose as interior designers visiting Campaniello's showrooms and warehouse. Before the complaint was filed, a private investigator visited the Campaniello store and secretly tape-recorded conversations with a sales clerk. When the investigator asked for Saporiti Italia furniture, the

sales clerk informed him that the company "doesn't exist anymore…it dissolved." The conversation continued as follows:

**Investigator:** So that company doesn't exist anymore then?
**Sales Clerk:** No.
**Investigator:** Okay, So would I be getting [] the same quality?
**Sales Clerk:** Oh absolutely. Absolutely.
**Investigator:** Would I be getting the same, I mean, if I guess the same workmanship?
**Sales Clerk:** Oh absolutely.
**Investigator:** What happened, they changed or something?
**Sales Clerk:** Well, they had a fight. The two brothers I guess.
**Investigator:** Okay. So where would I be able to get the Saporiti then?
**Sales Clerk:** Well there is one brother. Saporiti Italia as it existed doesn't exist anymore.
**Investigator:** So, there is no place to get their furniture?
**Sales Clerk:** As far as I know.

After the complaint was filed, two investigators visited Campaniello's warehouse, where they observed two Campaniello delivery trucks and a fork-lift displaying the Saporiti Italia name. They also observed Saporiti Italia furniture on sale at the warehouse. They also visited the retail store again, where the sales clerk told them that the Saporiti Italia name "is no longer there…We have very few Saporiti items in the store…These two brother[s] that were working together, but they spit. And now the second brother is doing this other line. But it is still Saporiti …The quality and everything is still the same.

Before trial, Campaniello moved for an order *in limine* precluding Gidatex from offering the testimony and reports of Gidatex's investigators and the secretly-obtained tape recordings of their conversations with Campaniello's sales clerks. Campaniello claimed that Gidatex's investigators had user their "superior legal knowledge" to trick Campaniello's sales clerks into making statements to support Gidatex's case under the Laham Act, and that Gidatex's use of undercover investigators violated ***no contact rules.***

**No-Contact Rule**

The stated purpose of the no contact rule "is to preserve the proper functioning of the attorney-client relationship." Under the circumstances presented her, Gidatex's investigators did not intrude upon Campaniello's attorney-client privilege or attempt to use superior legal knowledge to take advantage of Campaniello's salespeople. Neither investigator was an attorney and neither attempted to interview party witnesses.

The investigators posed as interior designers — typical Campaniello customers… While it might have been annoying and time-consuming for Campaniello sales clerks to talk with phony customers who had no interest in buying furniture, the investigators did nothing more than observe and record the manner in which Campaniello employees conducted routine business… There was no risk that Campaniello's low-level employees would disclose, or were even aware of, any information protected by the attorney/client privilege.

**Preventing Dishonesty & Fraud**

An attorney is prohibited from engaging in conduct involving "dishonesty, fraud, deceit, or misrepresentation." It's not a crime in New York for a person to secretly record his or her own conversations with another person, but is hiring investigators to pose as consumers a ***misrepresentation***? Some ethics committees have said that using undercover investigators is unethical, since such conduct involves deceit or misrepresentation. Nevertheless, the court refused to find a violation, calling the use of undercover investigators "an accepted investigative technique."

The policy interests underlying the prohibition on misrepresentations by attorneys are (a) to protect parties from being tricked into making statements in the absence of their counsel and (b) to protect clients from misrepresentations by their own attorneys. The presence of investigators posing as interior decorators did not cause the sales clerks to make any statements they otherwise would not have made. There is no evidence to indicate that the sales clerks were tricked or duped by the investigators' simple questions such as "is the quality the same?" or "so there is no place to get their furniture?"

**Court Applies Three-Pronged Test**

The court then focused on the policy interests expressed by trademark and unfair competition law.

These ethical rules should not govern situations where a party is legitimately investigating potential unfair business practices by use of an undercover investigator posing as a member of the general public engaging in ordinary business transactions with the target. To prevent this use of investigators might permit targets to freely engage in unfair business practices which are harmful to both trademark owners and consumers in general. Furthermore, excluding evidence obtained by such investigators would not promote the purpose of the rule, namely preservation of the attorney/client privilege.

Enforcement of the trademark laws to prevent consumer confusion is an important policy objective, and undercover investigators provide an effective enforcement mechanism for detecting and proving anti-competitive activity which might otherwise escape discovery or proof. It would be difficult, if not impossible, to prove a theory of "palming off" without the ability to record oral sales representations made to consumers. The court next noted that even if inappropriate contact and misrepresentation applied here, Campaniello had not established any violations. The court considered but rejected the three-part test used in the Second Circuit to determine whether lawyers have violated rules):

(1) Did counsel communicate with a "party"?
(2) If so, did counsel know that the party was represented by a lawyer in this matter?
(3) Finally, did counsel "cause" the communication to occur?

Under this test, whether Gidatex's lawyer violated no contact "turns on ***whether the sales clerks were parties, whether they were represented by counsel at the time of the communication, and whether [the lawyer] knew they were represented by counsel at that time."***

Applying this test, the court said that a corporate employee is "a party" if "(1) he/she had high-level managerial responsibility and was capable of binding the corporation; or (2) his/her acts or omission maybe be imputed to the corporation for the purposes of civil or criminal liability; or (3) his/her statements may constitute an admission by [the corporation]."

In *Niesig v. Team I* [76 N.Y.2d 363, 373 (1990)], the New York Court of Appeals has defined "party" to include: Corporate employees whose acts or omissions in the matter under inquiry are binding on the corporation (in effect, the corporation's "alter-egos") or imputed to the corporation for purposes of its liability, or employees implementing the advice of counsel. All other employees may be interviewed informally.

**(1) Sales Clerks Were Considered To Be NO CONTACT RULE Parties**

Campaniello's sales clerks are "low-level employees with no management responsibilities whatsoever" and therefore would not generally be considered parties under no contact — but Campaniello argues that ***Gidatex intends to offer the clerks' statements regarding Saporiti Italia furniture as admissions*** that Campaniello itself is involved in a "palming-off" scheme. ***As a result, the sales clerks are "parties" that***

***the investigators should NOT have interviewed. It was a violation of the NO Contact Rule.***

**(2) Were Defendants 'Represented' By Counsel?**

An organization "should be considered a party anytime it has specifically retained counsel to represent its interests regarding the subject of representation or has specifically referred the matter to house counsel." Gidatex stuck by its "technical argument" that Campaniello had not yet specifically retained counsel to represent it in this trademark infringement dispute. It is true that when the investigators visited Campaniello the first two times, Gidatex had not filed its trademark infringement case and Campaniello had not yet retained its current counsel. Nevertheless, "after years of related litigation between Gidatex and Campaniello, it is unrealistic to conclude that [plaintiff's lawyer] did not know that Campaniello was represented by counsel." Accordingly, the conduct of Gidatex's counsel "technically satisfies the three-part test generally used to determine whether counsel has violated the disciplinary rules."

**(3) Did Counsel 'Cause' Communication to Occur?**

This element was so obvious from the facts that the court did not separately address it. The plaintiff's attorneys had already freely acknowledged that they hired the investigators.

In sum, the facts satisfied all three prongs of the Second Circuit test for a violation. Nevertheless, the court concluded as follows:

[Plaintiff's attorney] did not violate the rules because his actions simply do not represent the type of conduct prohibited by the rules. The use of private investigators, posing as consumers and speaking to nominal parties who are not involved in any aspect of the litigation, does not constitute an end-run around the attorney/client privilege. Gidatex's investigators did not interview the sales clerks or trick them into making statements they otherwise would not have made. Rather, the investigators merely recorded the normal business routine in the Campaniello showroom and warehouse. Even if the rules had applied, and even if the plaintiff's attorney had violated them, the court would not have suppressed the evidence. "[A] court is not obligated to exclude evidence even if it finds that counsel obtained the evidence by violating ethical rules… New York State courts will admit evidence procured by unethical or unlawful means in violation of the NYSBA Code of Professional Responsibility." Here, "the remedy of preclusion would not serve the public interest or promote the goals of the disciplinary rules." Accordingly, the court denied defendant's motion to exclude the evidence obtained by the undercover investigators.

**Exercise Caution**

The *Gidatex* decision is a thoughtful, nuanced, careful analysis of the issues raised by an attorney's use of undercover investigators wielding concealed recording equipment. Given its legal and factual context, the *Gidatex* decision is probably right. But attorneys should not take it as a general statement of the law regarding undercover investigators and secret tape recordings. Other authorities in New York and elsewhere have also addressed the subject of secret taping, and some of these authorities have labeled it unethical.

For example, in N.Y. State 328 (1974), the ethics committee concluded that except in special situations, it is improper for a lawyer in private practice to record a conversation with another attorney or any other person without first advising the other party Even if secret electronic recording of a conversation with one party's consent is not illegal, the Committee said, it offends the traditional standards of fairness and candor that should characterize the practice of law. In ABA 337 (1974), relying on DR 1-102(A)(4), the ABA's ethics committee also concluded that no lawyer should record any conversation without the poor consent or knowledge of all parties to the conversation.

More to the point, in ABA Informal Op. 1320 (1975), the ABA ethics committee opined that a lawyer would be acting unethically if the lawyer asked an investigator to tape his conversation with a sales clerk when the investigator knew that the recording was being made but the clerk did not. (In some jurisdictions, recording a conversation without the consent of both parties is a crime, not just an ethical violation.) In N.Y. State Op. 515 (1979), the Committee said that a lawyer in private practice may under certain circumstances counsel a client concerning conversations to be recorded without notice or consent, but the Committee stressed that the permissible circumstances were narrow. And in N.Y. City Op. 1995-10 (1995), the City Bar's ethics committee flatly stated that a lawyer "may not ethically record telephone or in-person conversations with opposing counsel without first advising him or her that the inquirer intends to record the conversations."

Of course, some ethics committees have concluded that secret taping, in itself, does not violate any ethical rules as long as the taping is lawful where it is undertaken and the lawyer makes no affirmative misrepresentations as to whether the conversation in question is being recorded. [*See,* N.Y. County 696 (1993); Arizona 90-2; Kentucky E-279 (1984); Oklahoma 307 (1994); Oregon 991-74; Utah 90 (1989).] But a

lawyer who follows those authorities — or the*Gidatex* holding — is taking a risk. Unless all other avenues of gathering the information are closed off, a lawyer should avoid undercover investigators and secret taping.

## ***Ex Parte Contact***

In **McCallum v CSX Transport**, defendant CSX says that plaintiffs' counsel and investigator made ***improper ex parte contacts*** or with its employees after this lawsuit was filed. As a result, it seeks an order disqualifying plaintiffs' out-of-state attorney and law firm from further representation in this action, a protective order preventing plaintiffs from using at trial any statement given by a CSX employee, an order prohibiting further *ex parte* contacts by plaintiffs' counsel and/or their investigators, and an order granting CSX reasonable expenses and attorney's fees for bringing this motion

The CSX case began as a negligence issue where a minor boy, playing under a train trestle, was injured by a loose strap from a CSX railcar. Plaintiffs have alleged, among other things, that CSX, by and through its agents, servants and employees, was negligent in failing to inspect, maintain and operate the train properly and in failing to warn plaintiffs, to observe its own operating rules, and to eliminate the risk caused by dragging steel bands.

Through its investigator, the plaintiff's investigator allegedly violated the appropriate rules on professional conduct by interviewing some of the defendant's employees after this lawsuit was filed. The Court further found that ***the investigator may have misled some of the employees concerning whom he represented, his role in the process, and the nature of the situation between the plaintiffs and the defendants by minimizing the fact that the investigator was trying to find evidence which would prove the interviewees' employer was negligent.***

Defendant CSX contends that plaintiffs' counsel ***violated no contact rules by INTERVIEWING people who had a direct connection with the events of the accident.*** This includes the member of the train crew whose train car allegedly caused the accident and the employee at the train yard through which the train traveled, which was the last point wherein the train could have been inspected with respect to loose band problems. Both made statements with respect to banding indicating that it was a problem and such testimony may be harmful to defendant CSX's case. CSX complains that the three people responsible for rebanding were also directly connected with the accident. Finally, defendant asserts that plaintiffs'

interviews with the other employees were improper because such interviews could constitute admissions pursuant to as being statements made by a party's agent or servant concerning a matter within the scope of the agency or employment.

The Court agreed with the defense and, among other things, directed that (1***) the investigator be removed*** and not further participate in the case, (2) plaintiffs were required to identify all interviewed employees and produce copies of all interview notes, (3) plaintiffs' counsel and investigators were forbidden to contact any other CSX employee except through counsel of defendant, and (4) the Court assessed reasonable attorney's fees against plaintiffs' law firm for defendant's having had to bring the motion.

## ***Witness Tampering***

A San Francisco private investigator who works with criminal defense attorneys was indicted on a felony count of ***dissuading a witness***, a charge stemming from his alleged efforts to scare off a star witness in an attempted murder case. The investigator faced a $75,000 bail and up to three years in state prison.

In another incident, a gang of ***investigators*** and associates in Brooklyn were charged with illegal gun possession, ***soliciting, intimidating and tampering witnesses in a case***. All faced up to seven years in prison. The district attorney Brown used various investigative techniques, including court-authorized eavesdropping, controlled telephone calls, the subpoenaing of telephone records and listening to recorded telephone calls to unmask the illegal activities. Specifically, it is alleged that the investigators and other defendants engaged in acts intended to instill a fear in the witness and several members of his family that they might be physically injured if he or they testified or cooperated with the district attorney's office. At other times, it is alleged that the defendants offered to confer benefits on people, including the witness, in order to influence their testimony or keep them from appearing.

# MISREPRESENTATION / PRETEXTING

As we have previously defined: Pretexting generally involves the use of information about an individual, such as a social security number***, to impersonate the individual and mislead information providers into giving out additional information that would generally only be available to the authorized individual***. Attorneys, and private investigators, when

gathering facts, must avoid making false or misleading statements representing that they are authorized to obtain personal information when in fact they are not.

***A Story:*** *In the celebrated 1939 novel and 1946 movie The Big Sleep, Los Angeles private detective Philip Marlowe was retained by General Guy Sternwood to investigate Arthur Geiger, after Geiger had requested payment of some suspect promissory notes. Marlowe's investigation included two visits to Geiger's book shop on Hollywood Boulevard. On the first visit, Marlowe pretended to be interested in buying books; on the second, he pretended to have a book to sell. In neither visit did Marlowe disclose that he was an investigator or that General Sternwood had retained him. Under Wayne v. Bureau and its progeny, Marlowe might well have violated the law and risked discipline and civil liability. The fictional Philip Marlowe could ignore such risks. Nonfictional investigators and lawyers cannot.*

Violation of pretexting laws can be swift and substantial. The pretexter may be required to give back any money or profits made from their illegal act. In cases of egregious violations, there are criminal options available through the Department of Justice.

Who could be liable? If the person who hired the pretexter had no idea how the information was going to be acquired or didn't specifically know that pretexting was going to be used, then they may not be charged. PIs who hire out all or parts of their investigation may be brought to a higher standard***. A PI should not simply rely on a subcontractor's word, but should know how information will be acquired.***

## *Pretexting Techniques: Part Of Investigations?*

In the course of such investigations, investigators may explicitly or implicitly misrepresent who they are, may misstate the purpose of their visit, questions or interviews, and may secretly tape record, photograph or videotape others during the visits (to the extent such secret recording is permitted by law). As we have suggested, ***not every act of interviewing is pretexting***. Further, some feel that ***if pretexting were outlawed, an unintended consequence would be the loss of undercover investigators to detect theft in the workplace or seek out identities of drug dealers***.

Consider the following, ***somewhat acceptable, form of pretexting***: A client once hired a PI to find out whether a former employee who was

starting a rival business planned to illegally copy the firm's manufacturing techniques. The investigator who befriended the former employee at a trade show and worked to develop a relationship. After several weeks, the two men went on a fishing trip together, during which the former employee offered the investigator a job with his new firm and revealed that he had his former employers' trade secrets. The company used that information to sue the former employee with the investigator as the star witness.

The Investigative & Security Professionals for Legislative Action (www.ISPLA.org) suggest many other ***examples where pretext investigations may be required***:

- A brand owner suspects that its products are infringed upon or counterfeited and therefore hires private investigators to visit some stores or showrooms, speak to salespeople, determine who the owner of the store is and ascertain the scope of the infringing or counterfeit activity;

- Before or after commencing an action against an infringer or counterfeiter, a brand owner hires private investigators to take pictures of a store window displaying infringing or counterfeit goods, to buy infringing or counterfeit goods and to speak with sales representatives in order to assess how they present the products to consumers;

- Before or after commencing an action against an Internet infringer or counterfeiter, a brand owner hires private investigators to contact the online seller, exchange communication with the seller and purchase infringing or counterfeit goods to ultimately identify the seller and ascertain his or her domicile; or

- After commencing an action against an infringer or counterfeiter, discovery is difficult and a brand owner has difficulties getting the requested documentation. The brand owner, therefore, hires an investigator to visit defendant's stores, speak to defendant's salespeople and record conversations with defendant's low-level employees in order to gather evidence as to defendant's representations to consumers regarding the infringing or counterfeit goods.

Use of pretexts extends well beyond the investigation of trademark infringement and counterfeiting cases:

- A ban on such use would make all in-plant and internal survey style undercover investigations illegal, for posing as either an employee or as one other than an investigator would be a pretext.

- All "sting" operations would be illegal and the use of pretense in attempting to track down the location of thieves and their illegally gotten gains taken from the clients of investigators would be a crime.

- Retail loss interrogations would be restricted as many recognized interrogation techniques involve subterfuge or some limited pretext when questioning a suspect.

- Retail testing operations or the use of "Mystery Shoppers" would be illegal, as operatives would be posing as customers.

- Investigators conducting surveillance, who are approached by a neighbor inquiring as to the reason for their presence, would be unable to use a simple pretext to explain their presence in order not to alert the subject of their surveillance.

There is also some precedent for coming down on pretexting practices that might be considered widespread and blatant. Such was the case when the ***U.S. Attorney's office in Seattle indicted at least ten investigators hired by attorneys and others to obtain confidential information by pretext.*** As a large scale operation, private investigators offered and obtained confidential information for as many as 12,000 individuals involved in bankruptcies, law suits, divorces and collection efforts nationwide. Services were utilized by attorneys, insurance companies and collection companies to investigate the backgrounds of opposing parties and witnesses, and to uncover assets or income for satisfaction of debts, according to the indictment.

The alleged defendants collected information via pretext from the I.R.S., Social Security Administration, various State Unemployment Insurance Departments, private financial institutions, banks, pharmacies and hospitals. The alleged defendants fraudulently posed as the individuals about who information was sought. Clearly obtaining confidential information from entities like the IRS or Social Security is protected by specific laws

Bottom line? ***Professional investigators should not violate the law to obtain information, and that should be clearly explained to every potential client***.

***The principle intent of a legitimate pretexting interview is to limit the discussions between the investigator and the target to matters that would normally be addressed in the transaction under investigation.***

## ***Other Pretexting Violation Examples***

Simply ***using a pretense to determine whether or not a subject is at home or place of employment would be illegal***. Such practice is common in holding visual electronic surveillance of subjects in workers compensation claims and personal injury litigation.

***Calling a bank to determine if a check will clear if you don't actually have a check*** or you are trying to discern whether there is money in that account.

If you ***use false pretenses to get a bank to give you a consumer's address*** or get a consumer to give you the name of his bank, it is pretexting.

## ***John Lennon's Image***

A case from New Jersey illustrates what are likely the outer limits of what a court is willing to define as an ethical misrepresentation in the context of gathering facts in aid of litigation. In **Apple Corps Ltd. v. International Collectors Society**, Yoko Ono's counsel hired investigators to investigate whether a postage stamp company was violating the terms of a settlement agreement with John Lennon's estate concerning stamps bearing the rock star's image.

The investigators posed as consumers and placed orders by phone with the stamp company for products not authorized under the settlement agreement. The stamp company sold the products to the investigators, which was the critical piece of evidence showing the stamp company's violation of the settlement agreement. After the plaintiffs sought a contempt order and injunction, the stamp company motioned for ***ethical sanctions against plaintiff's counsel***, claiming their behavior was

deceitful. The *Apple Corps* court held that the phone calls did not violate ABA, New York or New Jersey ethics rules prohibiting fraud and deceitful conduct, although the investigators did not identify their purpose in calling.

The ***Apple Corps vs International*** court held ***lawyers and their investigators DO NOT violate pretexting laws when they "act as members of the general public, transact ordinary business and engage with low-level employees of a represented corporation to detect violations of the law.*** To what extent the conduct approved in Apple can be generalized to all cases is open for debate. Arguably, undercover investigative acts that verge on pretexting, such as those undertaken by the *Apple Corps* attorneys, appear to be accepted only in those narrow areas where courts or ethics boards have expressed some approval, as in the contexts of housing discrimination and trademark disputes, where the potential violations would otherwise not easily be detected or proven.

## ***Posing As A Chiropractor***

In yet another case, that seems to contradict the Apple Corps case, an Oregon court decided that a pretexting scenario ***did violate*** misconduct rules prohibiting "fraud, deceit or misrepresentation." **In re Gatti**, (2000). Gatti, a lawyer, sought to investigate whether Comprehensive Medical Review (CMR), a company that conducts claims reviews for State Farm Insurance Company, employed unqualified reviewers and used an improper cost-cutting formula to determine whether to grant medical coverage for chiropractic services.

Gatti, ***posing as a chiropractor***, called a reviewer who worked for CMR to ask questions about his qualifications. Then Gatti called a CMR executive and falsely stated that he himself had performed medical examinations, was interested in working as a CMR claim reviewer, and had been referred to CMR by both State Farm and the chiropractor-reviewer Gatti had called. The court held that the Oregon Bar could prosecute Gatti based on a disciplinary rule ***prohibiting knowingly misrepresenting one's identity with the intent that it be acted upon, in circumstances where disclosing one's real identity would have influenced the recipients' conduct***.

In response to the *In re Gatti* decision, which met with a critical response from the state bar, ***Oregon adopted a new professional rule***, now Rule 8.4(b***), permitting attorneys to supervise lawful covert activity in the investigation of violations of law or rights, where the supervising lawyer in good faith believes there is a reasonable***

***possibility of unlawful activity.***

The differences in conduct engaged in by Yoko Ono's attorneys and Gatti are important. One conclusion to be drawn is that an investigator's failure to identify her true objectives is acceptable if she is acting as a member of the general public, doing something that members of the public typically can do in relation to a particular transaction. In such a situation, the investigator is not lying to the investigation target, nor is she tricking the target into acting differently or giving out information that would not otherwise be given in such a situation.

However, where an investigator lies about his identity or poses as someone else in order to mislead the target into disclosing information that would otherwise be withheld, then such activity is treated as violative of the rules of professional conduct

## Private Investigator Indicted

A private investigator accused of ***posing as a journalist*** to gain access to the reporter's private telephone records is ***another example of illegal pretexting***.

The investigator was accused of ***using the Social Security number of the journalist***, who has not been identified***, to gain illegal access*** to the phone logs.

The PI was also accused of conspiring to illegally obtain and transmit personal information on directors, journalists and employees of a large company to learn the source of boardroom leaks to the news media.

Six years later, after a lot of attorney fees, the PI was sentenced to three months in jail.

The company that hired the investigator was also sued by the attorney general for engaging in unfair business practices. A $14.5 million settlement was reached.

## *Unsavory "Information Broker" Subcontractor*

When a prestigious private investigations firm was hired to investigate the key witness in a major corruption case, they ***subcontracted some of the work, to an unlicensed out-of-state "investigator" who had a spotty past, including a record***. The woman, according to court documents, used information

provided by the licensed PI firm to impersonate the witness and illegally gain access to his phone records. The witness became concerned that someone had hacked his phone when he received a text message from his carrier, informing him that his account information had been changed. He alerted prosecutors, who began an investigation. They ultimately learned that the subcontractor had contacted the phone company and used information about the witness to route his phone records to an email account she had set up. According to the "investigator: she was routinely hired by PI firms throughout the United States to conduct similar activities.

While no action was taken against the unlicensed individual, the PI firm was investigated and eventually raided by the district attorney's office to obtain evidence.

## ***Plausible Deniability***

Why do PIs use information brokers? In his book ***Analysis of the PIA and Case Law***, Los Angeles lawyer John Caragozian claims that private ***investigators who subcontract with information broker or subcontractors do so to insulate themselves from potential criminal culpability.***

"Private investigators have no more rights to access people's personal information than any other citizen, beyond what a reporter has or any other citizen has," Caragozian said. "If it would be illegal for a private person to do something, chances are it's illegal for a private investigator to do it."

It creates ***plausible deniability***, said Chris Jay Hoofnagle, director of information and privacy programs at the Berkeley Center for Law & Technology. Practices such as pretexting were at the forefront of a 2005 push to get the federal government to establish stricter rules surrounding the dissemination of a consumers' personal phone records.

The more distance created between the private investigators and subcontractor, the more plausible the deniability, said Stan Goldman, a criminal law professor at Loyola Law School.

## ***Someone Died***

In 1999, 20-year-old Amy Boyer of New Hampshire was killed in a murder-suicide by an obsessed former classmate who ***got her address*** from an Internet-based investigations firm that had obtained it by calling Boyer and ***pretending to be an insurance company*** verifying her address for a refund.

# ***The Investigator Had To Settle***

There is no doubt that private investigators may perform a useful and valuable function—and may even find that needle in a haystack. But they also come with great risks. Those risks played out recently in an antitrust class action currently pending against Uber and its co-founder and CEO, Travis Kalanick: **Meyer v. Kalanick** (2016)

In *Meyer*, the plaintiff sued Uber claiming that "surge pricing" and other aspects of Uber's business model resulted in antitrust violations. In addition to conventional fact-finding, Uber hired a private investigation company to dig up facts about the plaintiff and his counsel.

To do so, the ***investigator called and emailed Meyer's and Schmidt's acquaintances and colleagues under false pretenses and inquired about their most personal information***, including issues relating to their employment, finances, family life and motivation for bringing the suit, none of which was actually relevant to the issues in the underlying action. After learning of the investigation, Plaintiff's counsel sought to take discovery of Uber's information and the court agreed. The judge also did not allow Uber's work product and crime-fraud exception objections.

Further, the court also ***cited the investigators' lack of a license and investigator recorded phone calls with his sources without their knowledge*** or consent, some of whom lived in Connecticut and New Hampshire, where it is illegal to record calls without consent of both parties on the call. The court specifically admonished this behavior . . .

> *"It is a sad day when, in response to the filing of a commercial lawsuit, a corporate defendant feels compelled to hire unlicensed private investigators to conduct secret personal background investigations of both the plaintiff and his counsel. It is sadder yet when these investigators flagrantly lie to friends and acquaintances of the plaintiff and his counsel in an (ultimately unsuccessful) attempt to obtain derogatory information about them."*

Ultimately, the court (1) prohibited the use of any of the information obtained from the investigator in any manner; (2) and enjoined Uber and the investigator from undertaking any further personal background investigations of anyone involved in the litigation through the use of false pretenses, unlicensed investigators, illegal secret recordings, or other unlawful, fraudulent, or unethical means. Though inclined to issue monetary sanctions, the court did not ultimately rule on that issue because

Uber and ***it's investigator reached an agreement to pay plaintiff a reasonable (though publicly undisclosed) sum***.

The court finished its opinion with a warning:

> *"Potential plaintiffs and their counsel need to know that they can sue companies they perceive to be violating the law without having lies told to their friends and colleagues so that their litigation adversaries can identify 'derogatories.' Further, the processes of justice before the Court require parties to conduct themselves in an ethical and responsible manner, and the conduct here fell far short of that standard. As the Supreme Court long ago stated, 'courts of law' have inherent 'equitable powers . . . over their own process, to prevent abuses, oppression, and injustice,'* Gumbel v. Pitkin*, 124 U.S. 131, 144, 8 S. Ct. 379, 31 L. Ed. 374 (1888). This Court will not hesitate to invoke that power if any further misconduct occurs."*

## ***Dirty DUI***

A private investigator admitted that ***he hired female decoys to assist in determining if a "target" male, usually the husband of his female client in a custody or support case, would drink alcohol in a quantity sufficient to exceed the legal limit*** to drive an automobile. Once the "target" male had been observed to consume this amount of alcohol likely to exceed the legal limit to drive, the hired female decoys would leave the establishment and ask the target to follow them home. In some cases, the PI would tip off local police to stop, test and arrest the target.

The PI and his associates would lure the target with a concocted story about doing a TV show on their business or life experience.

An associate coined the phrase "***dirty DUI scheme***" to describe the practice. A number of the arrests and convictions resulting from the practice have been expunged and overturned, along with apologies from the senior deputy district attorney.

The PI was eventually arrested on sorted issues, including embezzlement, second-degree burglary and conspiracy, as well as drug-related charges. He is currently in prison until 2019.

# ***Bad Faith***

One of the early pretexting cases that is cited often is **Wayne v Bureau of Private Investigators and Adjusters** (1962). Wayne accumulated quite a history of misrepresentation over dozens of insurance investigations. In most cases, Wayne posed as someone he was not and ***did not disclose that he represented an adverse party*** to gather facts for his insurer clients. Here are few noteworthy examples:

On or about April 14, 1957, Wayne visited the home of one Kenneth G. Bell for the purpose of obtaining a statement from said Bell regarding an automobile accident in which Bell had been involved. Respondent was engaged for this purpose by a party whose interests were adverse to Bell. Prior to giving a statement, Bell asked respondent in substance, 'Are you National?,' (Bell's insurer). Respondent did not affirmatively reply that he was 'National' but represented himself as an investigator, and ***did not disclose to Bell that he represented an adverse party***. Respondent was aware that said Bell probably would not give a statement to him if respondent revealed that he was acting on behalf of an adverse party. Bell believed that respondent represented his insurer, and thereupon gave respondent a statement about the accident.

"On or about January 10, 1959, Wayne visited the home of Mr. and Mrs. Jack Weinstock for the purpose of obtaining a statement from them regarding an automobile accident in which Mrs. Weinstock had been involved. The respondent was engaged for this purpose by a party whose interests were adverse to the Weinstock's interests. Said Weinstock asked respondent for identification, and respondent identified himself as an investigator, and ***did not disclose to Weinstock that he was acting on behalf of an adverse party***. Respondent was aware that the Weinstocks probably would not give a statement to him if respondent revealed that he was acting on behalf of an adverse party. Said Weinstocks believed that respondent represented their insurer, and gave respondent a statement about the accident.

On or about July 16, 1958 one Terry Arnold, an employee of Wayne, visited the home of Ronald D. Garrahan for the purpose of obtaining a statement from him regarding an automobile accident in which Garrahan had been involved. Said Arnold was then acting in the course of his employment by respondent on behalf of a person whose interests were adverse to Garrahan. In accordance with respondent's instructions as to the manner and method of obtaining statements***, Arnold identified himself as the investigator 'assigned to***

***check the accident'***, ***and did not disclose to Garrahan that he was acting on behalf of an adverse party***. Said Garrahan believed that Arnold represented his insurer and gave Arnold a statement about the accident.

In about August, 1957, Wayne telephoned the home of one George Mathias and arranged an appointment with said Mathias for the purpose of obtaining a statement about an automobile accident in which Mathias had been involved. Respondent ***introduced himself on the telephone as 'the investigator checking out the accident'***. He then visited the home of Mathias at the appointed time, where ***he was aware that he was received as a representative of Travelers Insurance Company***, the insurer of Mathias. Respondent was not a representative of said company, but was instead a representative of a party adverse to Mathias, and concealed this from Mathias. Respondent knew that he probably would not obtain a statement from Mathias if he revealed that he was acting on behalf of an adverse party. Said Mathias, believing that respondent represented his insurer, gave respondent a statement about the accident.

On or about August 21, 1958 one John Kroh, an employee of respondent, visited the home of Leonard Goldberg for the purpose of obtaining a statement from him regarding an automobile accident in which Goldberg had been involved. Said Kroh was then acting in the course of his employment by respondent on behalf of a person whose interests were adverse to Goldberg. In accordance with respondent's instructions as to the manner and method of obtaining statements, ***Kroh identified himself as an 'independent investigator assigned to check your accident', and did not disclose to Goldberg that he was acting on behalf of an adverse party***. Said Goldberg believed that Kroh represented his insurer and gave him a statement about the accident.

As a result of these activities, the investigator's license was suspended for 90 days, of which the execution of 60 days of said period was stayed for two years and he was also placed on probation.

Wayne objected to the decision and commenced a lawsuit to force a trail. However, the appellate court, after reviewing the facts, denied his request, sided with the Bureau by issuing the following:

"That petitioner's (Wayne's) conduct and the conduct of his employees, as set forth in the findings of fact of the Order and Decision of the Bureau of Private Investigators and Adjusters constituted acts of fraud and dishonesty

committed in the course of petitioner's business as a licensed Private Investigator and Adjuster within the meaning of section 7553.2 and former section 7551 of the Business and Professions Code of the State of California.

"Petitioner (Wayne) received a fair trial and a fair hearing and was afforded due process of law and the equal protection of the law at all stages of the administrative proceedings;

While there was no evidence submitted that concluded Wayne and his employees committed acts of fraud the essence of "fraud and dishonesty" is that appellant or his employee did not disclose that he was acting on behalf of an adverse party. The facts as found show that appellant's standard procedure is to identify himself as "the investigator checking out your accident." He does not reveal whom he represents because he is aware that he probably will not be given a statement if he fully identifies himself. "He does not actively misrepresent that he is from an interviewee's insurer, and instructs his employees not to do so. Respondent [i.e., Wayne] has interviewed about 10,000 persons for plaintiff's attorneys since receiving his license in 1953. There has been no complaint that his investigation reports were not true reports of his interviews." (Emphasis added.)
The main question for this court to determine is whether the acts and conduct of petitioner constituted dishonesty or fraud as those words are used in the statutes in question.

The court went on to say that: "Dishonesty may very well be something less than criminality. In other words, ***fraud and dishonesty extend beyond acts which would be criminal***. The term dishonesty 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 petitioner (Wayne) was acting as he did to the end that he would gain a benefit to himself and those companies or persons whom he represented to the disadvantage of the interviewees or the insurance carriers of the interviewees. It was not a simple or casual omission to tell the exact and whole truth on a single occasion, but to the contrary was a ***studied course deliberately to mislead the unwary and by telling part truths thereby to deceive the interviewees into believing that petitioner in some respect represented their agents or principals***. There was the disposition to deceive, betray and mislead the interviewees. In other words, there was ***a lack of complete integrity***.

# ***PI Deception?***

**Redner v Workmen's Compensation Appeals Board** (1971) is a worker's compensation case involving a company driver who handle heavy freight for an electrical supply company. His injury on the job was assessed by doctors to be a 57 percent disability. Investigators for Workers Compensation were brought in to see what, if any, additional capacity the insured may have.

In early July 1968 a person who told applicant that his name was Robert Hendry ***befriended the injured applicant*** and invited him to his ranch for the following weekend; applicant accepted. Hendry drove applicant to this ranch; there Hendry gave a small party, serving very little food but a great number of mixed drinks. The guests became inebriated. Hendry suggested that the party go horseback riding, and applicant joined the others in doing so.

During the riding and saddling of the horses, ***Chavez concealed himself in Hendry's barn and took about 350 feet of film***. The motion picture shows applicant saddling, riding, walking, and unsaddling a horse. Thereafter, on the next day applicant rode again. Unobserved by the riding party, Chavez took more motion pictures of applicant's activities. ***On the basis of the film, the insurance carrier ceased payment of temporary disability compensation on August 6, 1968, and refused to provide further medical care for applicant.***

On September 25, 1968, the insurance carrier asked Dr. Crandall to view the film of the horseback riding. Although he had not examined applicant for nine months, Dr. Crandall concluded that applicant "does not show the slightest evidence of any residual disability and should be able to perform gainful occupation satisfactorily, as evidenced by the films of July 18 and 19, 1968." On September 28, 1968, Dr. Perlson also viewed and described the motion picture films. Having examined applicant only once seven months previously, the doctor reported to the insurance company: "As a result of viewing the above films, it is my feeling at this time that this employee is not physically or mentally incapacitated in any way as a result of the alleged injuries sustained by him on April 25, 1967."

On June 3, 1969, Dr. Coulter, a neurological surgeon, examined applicant, reviewed the medical reports, and concluded that applicant had become "disabled from his usual employment as a truck driver, however, he is able to perform gainful employment at duties which do not require repeated bending and lifting, in fact the patient is working and has been doing light

tasks since September 1968 at Big Bear, California.... I would recommend that he avoid occupations in which repeated bending and lifting objects over fifty pounds is required, and that because of the slight objective weakness in his right lower extremity that he avoid occupations which require climbing ladders or to heights."

The injured worker appealed his case to the Workers Compensation Appealls board. The appeals board also viewed the film and issued its opinion (relying entirely upon the motion picture evidence): "We are satisfied that the activities depicted in said motion pictures are inconsistent with any permanent disability as a result of the within injury, and we will find, therefore, that this injury caused no permanent disability." The appeals board relied upon the reports of Dr. Perlson and Dr. Crandall to determine that temporary disability ceased on September 25, 1968 (the date of Dr. Crandall's report). It continued, "We are also satisfied that the injury herein has not caused the need for any further medical treatment as implied by Joseph Perlson, M.D., in his report of September 28, 1968." The injured worker appealed again with his counsel asking why the film was never entered as evidence, even though many decisions were based on its content. The appellate court eventually concluded that the board erroneously relied upon the motion picture evidence. Further, and this is important, even if the motion picture evidence had been offered in a timely fashion at the referee's hearing, ***the referee should have refused to rely upon because the carrier obtained it by fraudulent inducement***.

The record contains uncontradicted testimony by applicant that the private investigator induced applicant's intoxication and subsequent horseback ride in order to obtain a film of this activity. The carrier thereafter attempted to profit by this questionable conduct.

The referee recognized that a film is a reasonable method to determine a person's activity level. However, ***when the insurance carrier or its private investigators have deceitfully induced applicants to perform acts for the hidden camera which they would not otherwise have committed it should not be admissible. And, the carrier should not profit from its own deceitful conduct***. ***The investigators feigned friendship and concealed their employer's identity in bringing about applicant's inebriation and effectuating his horseback ride***.

Nothing in the record so much as suggests that in the absence of the fraudulent inducement applicant would have taken the ride. Indeed, the referee found ***that the carrier fraudulently obtained the film by means of a violation of applicant's right.*** Thus, the appeals referee refused to consider the two medical reports to the extent that the described

or relied upon the tainted film on the basis that evidence obtained by fraud and deceit in violation of the rights of the applicant is not "best calculated to ascertain the substantial rights of the parties and carry out justly the spirit and provisions" of the workmen's compensation laws.

# KIDNAPPING

In general, a parent who intentionally interferes with the parental rights of the other parent is liable in tort -- **Leonard Karp & Cheryl Karp, Domestic Torts** (1989 & Supp. 1999). Likewise, one ***who assists a parent in taking exclusive possession of a child (read PI) in contravention of the rights of the other parent may be criminally or civilly liable.*** See generally **Annotation, Kidnapping or Related Offense by Taking or Removing of Child by or Under Authority of Parent or One in Loco Parentis** (1983 & Supp. 1999).

As many of the cases below will bear out, ***the claim of kidnapping against a private investigator complicit in a child abduction case, and therefore against the attorney or the spouse, will rise or fall on whether the parent has a right to custody of the child***.

## *PI Was A Decoy*

Consider **State v Stocksdale** (1975). The mother brought the child to her parents' home. The father hired ***a private investigator who then acted as a decoy at the front door*** of the maternal grandparents while he, the father, slipped in the back and took the child. The court held that, in light of the prosecution's unwillingness to proceed with kidnapping charges, it could go no further. The court further opined, however, that the ***private investigator*** and the father ***could together be charged with conspiracy to kidnap***, and public policy mandated against a holding which would encourage or support the movement across state lines of people engaged in the business of resolving custody disputes by child snatching.

## *Investigator Restrained Father*

With **Offenhartz v. Cohen** (1990), it was alleged that when Sara Offenhartz was 12 years old, after her parents had separated, she was with her father in New Jersey when her mother and a private investigator hired by her mother's attorney, Jeffrey Cohen, "attempted forcibly to place Sara in a car against the girl's will. ***The investigator, it is asserted, restrained Sara's father during this episode***.

It is this event which forms the nucleus of Sara's complaint against her mother's lawyer that he was behind this 'assault' and attempted 'abduction' and accordingly should pay damages in the amount of $10 million." The court determined that, because Sara's mother had the right to custody, she had the right, through her agents, to go get Sara and have her placed in a car to be brought back to New York. The court further concluded, '"New York does not recognize any liability on the part of an attorney to a non-client third party for injuries sustained as a result of any attorney's actions in representing his client absent fraud, collusion, or a malicious or tortious act' (see, Michalic v. Klat). As concluded above, the allegations fail to state any tort claim, and while the now-adult plaintiff still clearly believes that the claimed 'abduction' was malicious, it is clear that the facts do not objectively state any cause of action as against the attorney based upon advice he allegedly gave his client."

## ASSAULT & BATTERY

## *False Imprisonment & Assault*

This **Armes v Campbell** (1980) case arises out of a custody dispute between Rita Campbell, the paternal grandmother of Jason Campbell, and Linda Sweet, the mother of the child, who hired Jay J. Armes, ***a private investigator, to assist her in obtaining physical possession of Jason***. Following a divorce between the parents, Ken and Linda Campbell, they entered into a written agreement giving Linda custody of a daughter of the marriage and Ken custody of their son, Jason. Subsequently, Ken entered into an agreement with his parents in which he relinquished custody of Jason to the grandparents. After Linda remarried, she decided to locate her son, and she came to El Paso in December, 1977, with her brother and brother-in-law and hired Mr. Armes to assist her.

On December 21, 1977, Rita Campbell received a telephone call while at work, supposedly from the Judge in Oklahoma who granted Ken and Linda's divorce, advising that she would be arrested for kidnapping. Actually, the Judge had died more than two years prior to this telephone call. About 10:00 p. m. on December 21, 1977, Mrs. Campbell received another telephone call at her residence, advising it was from a deputy sheriff who claimed he had a warrant for her arrest. In fact, there was no warrant for her arrest. Mrs. Campbell got Jason out of bed and decided to drive to her husband's place of employment. Shortly after leaving her house, she said she was followed by a pick-up truck with Oklahoma license plates.

Later, she was ***followed by a car driven by investigator Armes*** . She testified he finally succeeded in ***forcing her to pull over*** to the curb on Dyer Street. She said at that time he told her

she was under arrest for kidnapping and, when she started to leave, he told her: "Don't run! We'll get you." After a ***high speed chase*** down War Road, the engine in Mrs. Campbell's car exploded, and she was again required to stop, this time on Sun Valley Road. The pick-up then stopped in front of her car, and Mr. Armes' car was stopped directly behind her car. She sought help on her "CB" radio. When the City police officers arrived, she was very upset. After the officers reviewed the papers provided to them by both the mother and grandmother, they took Jason and gave him to Linda and she left.

The ***jury found Mr. Armes did falsely imprison Mrs. Campbell by preventing her from leaving Sun Valley Road, using his car to block her vehicle after a high speed chase. He also committed an assault upon her by chasing her on War Road, and that his conduct caused property damage to her vehicle***. The jury assessed the damages at $650.00 for the car, $2,000.00 for false imprisonment, $3,000.00 for assault, and found exemplary damages of $7,500.00 for false imprisonment and $12,500.00 for assault. Judgment was entered on this verdict.

# DEFAMATION

## *PI Qualified Privilege*

Lawyers are given an absolute immunity for statements made in the course of judicial proceedings so that they may exercise unfettered judgment in their clients' interests. Courts have opined, however, that investigators should be limited to a ***qualified privilege***, being held liable for otherwise defamatory statements the investigator knows to be false, or utters in reckless disregard of its truth or falsity. The litigation privilege is not limited to statements made in a courtroom during a trial; "it extends to all statements or communications in connection with the judicial proceeding." Other court decisions say the privilege also extends to preliminary conversations and interviews.

*A **qualified privilege of immunity from defamation** does not mean someone (witness or investigator) can say anything they want before or during a trial. The privilege is granted in order for witnesses to have free exchange of information to say what they need to say to get to the truth. However, **saying something that he knows is not true can mean the investigator's protection of the privilege could be lost**.*

Consider **Harris v Hawkins** (1994). Linda Hawkins was involved in an automobile accident that left her physically and mentally disabled. On July 14, 1987, Hawkins had another automobile accident that worsened her condition. Hawkins filed lawsuits against the two responsible parties. Those

matters were consolidated for discovery and trial and a jury returned a verdict in favor of Hawkins for over $400,000.

Hawkins's complaint included allegations that the investigator-defendants for the insurance company defamed her during their investigation. ***Three allegations were especially troubling***: (1) Investigator-defendants ***contacted her personal trainer and asked how long he had been having an affair with her***; (2) Investigator-defendants twice ***contacted her minister to say she was committing insurance fraud***; and (3) Investigator-defendants ***contacted her housekeeper*** and ***asked her how much money Mrs. Hawkins was paying her to lie.***

In the end, the court determined that ***the investigators' statement about the wife's alleged infidelity could be cause for further action against the PIs in another trial.*** The remaining statements were fortunately granted privilege in this case as they were made in the course of judicial proceedings.

# ENTRAPMENT

## *Lured To Commit Embararrassing Acts*

A private investigator hired by a Police Officers' Association, was sentenced to one year in county jail and three years probation for trying to entrap two city councilmen in embarrassing and illegal acts.
In a tense election year, a city council was embroiled in a battle with the city's public employee unions over their efforts to crack down on spiraling public employee pension costs and push the outsourcing of city services. The investigators were hired to dig up damaging information about the councilmen ahead of the election.
.
A civil lawsuit alleges the union, their law firm and the ***investigator***

***engaged in a scheme to follow and illegally entrap one or more councilmen and accuse him of driving under the influence. Another, who is married, was entrapped into a compromising position with woman planted at a bar.***

# SURVEILLANCE

## *GPS Tracking*

In 2012, the U.S. Supreme Court (**United States v Jones**) ruled that the installation of a GPS tracking device onto a suspect's car constitutes a search — and therefore could require a warrant. Of course, this case applied mainly to police, leaving the issue of private investigators silent.

Most states, however, have laws on the books that ***prohibit the use of "slap and go GPS" tracking devices by PIs or individuals***. The law in its simplest form, looks something like this…

***No person shall use a tracking device to determine the location or movement of another person without the consent of that person being followed.***

Placing such a device on a vehicle that you do not have an ownership interest in, however, could be ***a trespass to chattels*** and you could be liable in tort for financial damages.

Penalties for a ***first offense*** might be a fine not less than five hundred dollars ($500), or imprisonment for not more than six months, or both. For a ***second offense***, the fine might be not less than seven hundred fifty dollars ($750), or imprisonment for not less than thirty days nor more than six months, or both. For the third offense and all subsequent offenses, not less than one thousand dollars ($1000) or imprisonment for not less than sixty days nor more than one year, or both.

Typical state ***exclusions***, which allow some GPS tracking, include:

- The owner of a motor vehicle, including the owner of a vehicle available for rent, who has consented to the use of the tracking device with respect to such vehicle.
- The lessor or lessee of a motor vehicle and the person operating the motor vehicle who have consented to the use of a tracking device with respect to such vehicle.
- Any law enforcement agency, including state, federal, and military law enforcement agencies, who is acting pursuant to a court order or lawfully using the tracking device in an ongoing criminal investigation, provided that the law enforcement officer employing the tracking device creates a contemporaneous record describing in

detail the circumstances under which the tracking device is being used.

- A parent or legal guardian of a minor child whose location or movements are being tracked by the parent or legal guardian.
- When the parents of the minor child are living separate and apart or are divorced from one another, this exception shall apply only if both parents consent to the tracking of the minor child's location and movements, unless one parent has been granted sole custody, in which case consent of the noncustodial parent shall not be required.
- The Department of Public Safety and Corrections tracking an offender who is under its custody or supervision.
- Any provider of a commercial mobile radio service (CMRS), such as a mobile telephone service or vehicle safety or security service, which allows the provider of CMRS to determine the location or movement of a device provided to a customer of such service.
- Any commercial motor carrier operation.
- Any employer that provides a cellular device to employees for use during the course and scope of employment.

Some states have also carved out another ***special exemption for professional (licensed) private investigators*** and their supervised employees. GPS tracking can be allowed in these states under circumstances such as the following:

- The professional investigator or the employee of the professional investigator is working on behalf of a client who is the restrained party under a protective order.
- The professional investigator or the employee of the professional investigator knows or has reason to know that the person seeking his or her investigative services, including the installation or use of a tracking device, is doing so to aid in the commission of a crime or wrong.

This is a rapidly changing area of the law. You should consult local counsel when planning to use GPS tracking in specific jurisdictions.

## ***PI Escapes GPS Rules***

A New Jersey appeals court ***approved the use of GPS tracking devices*** to spy on cheating spouses. In this case, a New Jersey wife installed a GPS tracking system in the SUV she shared with her husband so that the private investigator she hired could track her husband’s whereabouts.

Through the use of the GPS device, the investigator was able to track the husband to his lover's home. The ex-husband then sued the private investigator for violating his privacy.

The court found that the installation and use of the GPS tracking device in the shared vehicle was not an invasion of the husband's right to privacy, because the GPS unit only tracked his movements in public areas, where he had no expectation of privacy.

A fact that influenced the court in this case is the fact that the husband and wife maintained joint ownership of the vehicle. Had the husband owned title in his own name, the outcome could have been different.

## ***Trespass To Take Video***

A somewhat older, landmark workers compensation case (**Mclain v Boise Cascade** - 1975) exposes the liability investigators might have in trespassing on private property to take surveillance videos.

The plaintiff in this case filed a back injury claim against his employer Boise Cascade. Boise hired investigators to gather information on his condition. Mclain (the plaintiff) was ***unaware he was being taped until a workers compensation hearing***. After the hearing he filed a lawsuit against Boise and the investigators for ***invasion of privacy and one for civil trespass.*** Plaintiff demanded general and punitive damages for invasion of privacy and nominal and punitive damages for trespass.

Plaintiff lived on a large square lot containing slightly more than two acres. of the east boundary of plaintiff's tract and west of the row of walnut trees from which some of the film was taken. One investigator testified that he Over a period of time, two investigators took 18 rolls of movie film of plaintiff while he was engaged in various activities on his property outside his home. Some of the film showed plaintiff mowing his lawn, rototilling his garden and fishing from a bridge near his home.

Some of the film of plaintiff was taken from a barn behind plaintiff's house, which apparently belonged to a neighbor. Other film was taken while plaintiff was fishing from a bridge on the near the northeast corner of plaintiff's property. The remaining rolls of film were taken from a point near some walnut trees at the southeast corner of plaintiff's property.

There was a barbed wire fence a short distance west stayed east of the fence and did not know that he was on plaintiff's land. He testified, however, that he crossed over a fence under the bridge near the northeast corner of plaintiff's property in order to get to his vantage point near the

walnut trees. He probably trespassed on plaintiff's property when he crossed the fence, but that does not appear clearly from the record. On one occasion, when an investigator was near the walnut trees, he was seen by plaintiff.

Investigators did not question any of plaintiff's neighbors or friends and limited their activities to taking pictures while plaintiff was engaged in various activities outside his home. Plaintiff testified that these activities could have been viewed either by neighbors or passersby on the highway. Plaintiff further testified that he was not embarrassed or upset by anything that appeared in the films.

The court determined that the following legal issues:

- The law well establishes that ***one who seeks to recover damages for alleged injuries must expect that his claim will be investigated and he waives his right of privacy to the extent of a reasonable investigation***.
- If the surveillance is conducted in a ***reasonable and unobtrusive manner*** the defendant will incur no liability for invasion of privacy.
- The surveillance and picture taking were done in such an unobtrusive manner that ***plaintiff was not aware*** that he was being watched and filmed. The plaintiff conceded that his activities which were filmed could have been observed by his neighbors or passersby on the road running in front of his property.
- Undoubtedly ***the investigators trespassed*** on plaintiff's land while watching and taking pictures of him, but it is also clear that the trespass was on the periphery of plaintiff's property and did not constitute an unreasonable surveillance "highly offensive to a reasonable man".
- We think ***trespass is only one factor to be considered*** in determining whether the surveillance was unreasonable. Trespass to peer in windows and to annoy or harass the occupant may be unreasonable. Trespass alone cannot automatically change an otherwise reasonable surveillance into an unreasonable one

In the end, the trial court dismissed the privacy cause of action and submitted the trespass claim to the jury after withdrawing from their consideration the claim for punitive damages. The jury returned a verdict for plaintiff for $250.

# ***Investigators Were The Cause Of New Injuries***

The **Unruh v Truck Insurance Exchange** (1960) is an interesting case involving a worker's compensation claim. On March 31, 1960, plaintiff injured her back while working for an employer insured under the workmen's compensation laws by defendant Truck. Subsequently she underwent four surgeries on her back and her condition deteriorated, causing extreme pain and requiring treatment. Investigators were hired by the insurers to investigate the accident claim and at all times they "had knowledge of plaintiff's physical and mental condition and medical history."

The PIs placed the plaintiff under surveillance and actually ***befriended her.*** Unfortunately, the ***investigator did NOT represent his capacity and his intentions toward the plaintiff***." On specified dates, for the purpose of obtaining motion pictures of plaintiff, the ***investigators enticed and cause the plaintiff to conduct herself in a manner beyond her usual and normal physical capabilities*** ... In particular defendants enticed plaintiff to visit Disneyland where she was filmed crossing a rope bridge and a barrel bridge. While she was on the bridge, ***the PIs willfully and intentionally violently shook and disturbed the bridges which allegedly caused additional physical harm to the plaintiff insured***. ,

Upon learning of "the ruse and deception" practiced on her by defendants, plaintiff allegedly suffered a physical and mental breakdown requiring hospitalization. This breakdown was proximately caused by defendants' negligent exhibition of the films described, and by defendants' negligent failure to properly control their agents and employees "as to the limit, scope and manner of their investigation," and as to "the possible risk of injury to plaintiff therefrom."

As a proximate result of the above conduct of defendants, plaintiff sustained "injury to her nervous system and person," in the sum of $500,000 general damages, and special damages for medical and other expenses and wage loss, past and future, in sums to be determined.

Additional allegations included theories of assault, conspiracy and intentional infliction of emotional distress whereby plaintiff sought punitive damages of $2,000,000.

After submission of doctor reports, the court agreed that new treatment for physical and psychological injuries were justified. The issue of punitive damages would need to be settled by a separate trial for malpractice."

# ***Malicious Investigation***

Before leaving on a weekend trip to California, Jack Hires secured his home in Sparks and asked his neighbor, Doug France, to maintain the swimming pool. Soon after reaching his destination, Hires received a telephone call from France who told him that his house had been "robbed." Hires immediately returned to Sparks. He found extensive damage to the residence and furniture. In addition, several items had been stolen.

Some major back and forth between the insurer and Hires ended up in the ***insurer refusing to pay the full value*** or replacement of certain items in the house. Hires had already replaced his furniture and experienced major financial difficulties because of these purchases and repairs. So, legal counsel was hired.

Republic's conduct with regard to its investigation of the burglary was an issue at trial. At one point, for example, the investigation concluded that, because of the large amount of vandalism associated with the burglary, the perpetrator might have been a ***member of the Hires family or someone with a great dislike for the family***.

Republic, in fact, conducted a full neighborhood investigation into Hires' possible involvement in the burglary. ***Part of the investigation concerned Mrs. Hires' alleged extramarital activities and possible involvement in the burglary***. Hires testified that, prior to the investigation, he enjoyed a very close relationship with people in the neighborhood. After the investigation, he perceived a change in his neighbors' attitude toward him and his family.

About eighteen months after the burglary a lawsuit was filed (**REPUBLIC INS. CO. v. HIRES** - 1991). Republic again investigated the incident. An investigator was again employed by Republic's attorney. The ***investigator asked people involved in the case if they had been involved in a relationship with Mrs. Hires***. This investigation was conducted throughout the neighborhood. Also, pursuant to the investigator's request, the Sparks Police Department reopened the investigation, but closed it again upon verification of information previously received.

Hires suit against Republic alleged breach of contract, misrepresentation, bad faith, negligence and invasion of privacy. The jury awarded Hires $410,000 in compensatory damages and $22.5 million in punitive damages.

On appeal, the court held the previous ruling saying "it is clear that Republic was ***guilty of oppressive behavior***. However, evidence showed that the net worth of Republic was approximately $172 million. We conclude that $22.5 million is a larger sum than is necessary in this case to serve as a deterrent. They concluded that in this case any punitive damage award in excess of $5 million would be unreasonable and disproportionate to the behavior of Republic.

## ***Extreme Shadowing of a Target Led To Invasion of Privacy***

In the early 1960's, Ruth Stevens was injured in a collision with an automobile driven by one Bell who was insured under a motor vehicle liability insurance policy by the defendant United Services Automobile Association, in which collision she suffered physical injury and severe shock to her "nervous and emotional system." She thereafter filed an action for damages against Bell alleging these facts.

The insurance company, through its attorney, employed the defendant Pinkerton National Detective Agency, Inc. to follow the plaintiff and furnish reports of her activities in an effort to determine the extent of injury. Employees of this defendant commenced shadowing plaintiff, stealthily at first and then with progressively increasingly objectionable behavior.

Stevens claims she was constantly under surveillance. The detectives would ***peep through the hedge*** adjoining plaintiff's home, ***slink around her house, snoop and eavesdrop upon her activities therein***, ***park near the house*** where they could watch her through a hole in the hedge, and later ***park across the street from early morning until late at night***, ***follow her, especially at night, in automobiles staying only a few car lengths behind***. In particular, they drove past the house several times a day; parked different colored automobiles beyond the hedge and peeped through the hedge several times on several days; came on her premises at night near her windows and ran on being; ***eavesdropped and listened in on conversations inside the house***; went into the woods behind her house; cut a hole in the hedge alongside the street in order to peep into the windows; ***came to the door pretending to be television salesmen***; ***followed her closely in an automobile on given dates, into stores and public places; followed her into a named restaurant and were waiting outside a restroom door when she came out***, and so on.

On one occasion the plaintiff returned home at night and was so closely followed that she ran into the house in panic, hit a piece of furniture, and

knocked herself unconscious. On another occasion at a given date her automobile was followed so close that police intercepted it and the identity of the persons shadowing her was discovered.

During the early part of the surveillance plaintiff, who was already emotionally upset as a result of the collision, had a continuous feeling of being followed and spied upon, which her doctor and members of her family thought to be hallucinatory, and she suffered extreme mental torment in the belief that she was losing her mind. Later the disturbance manifested itself in nervous spasms, sleeplessness, nightmares, and the appearance of rash and lesions at dermal nerve endings over her entire body, accompanied by unbearable itching. She was forced to employ both medical and psychiatric aid.

After finally discovering the identity of the defendants, her attorney contacted the attorneys for defendants and informed them of her condition and that their conduct had almost made her lose her mind, and defendant's attorney stated he would request his client to discontinue these activities; nevertheless, the surveillance was continued in as aggravated a form as before, and plaintiff was forced to undergo further psychological treatments.

The conduct of the defendants in shadowing, snooping, spying and eavesdropping upon plaintiff was done in a vicious and malicious manner not reasonably limited and designed to obtain information needed for the defense of plaintiff's lawsuit against Bell but deliberately in a way calculated to frighten and torment her. Plaintiff's neighbors also noticed the espionage and thereby gained the impression that she was engaged in some wrongful activity and began to discontinue any association with her. The shock and injury to her nervous system is permanent.

The plaintiff alleged that the mental impairment and emotional injury for which she sues were caused by the acts of these defendants and not by the injuries and shock to her nervous and emotional system which she suffered and for which she recovered a verdict in the damage suit arising out of the

The court decided that ***overt and extended surveillance by an investigator agency on behalf of insurer, which frightened and harassed a target, is considered a violation of right of privacy***. Reasonable surveillance of residence from public road by insurance company is common method to obtain evidence to defend a lawsuit. "It is only when such is conducted in a vicious or malicious manner not reasonably limited and designated to obtain information needed for the defense of a lawsuit or deliberately calculated to frighten that it becomes illegal.

# ADMISSABLE EVIDENCE

An important focus of many investigators is to collect evidence that will be admissible in court. In order for evidence to be admissible, it must be ***relevant and reliable***. Just because you have collected something that you feel could be helpful to your case doesn't mean that it can be used in court.

If it has been gathered in a way that doesn't break the law, most evidence gathered by a private investigator is legal and usually admissible in court. That includes: conversations that the PI overhears which take place in public places, in a normal tone of voice, or any pictures that the PI takes of individuals in a public place.

## *Reasonable Expectation of Privacy*

The question that guides admissibility is simple . . . when the evidence was collected, did the people involved have a ***reasonable expectation of privacy***? Example: If two people are talking about incriminating activities while in the middle of a crowded store, then they do not of any expectation of privacy. Likewise, if they are observed doing something in a public area, they cannot expect to have privacy. In instances like this the PI is basically acting like any regular eye witness from a legal standpoint, and anything these people say or observed doing is admissible in court.

Evidence gathered by a private investigator where reasonable privacy can be expected may be illegal and not admissible in court. For instance, if the PI breaks into a private residence, taps a phone, or uses a planted microphone or listening device in a private place, then in these cases such ***evidence is not generally admissible***. That is because any conversations or activities done in private places, behind closed doors have a reasonable expectation of privacy.

Evidence gathered as a result of ***other illegal activities*** undertaken by the PI that are deemed inadmissible can damage the credibility of the PI and/or spell legal trouble as well. Since no PI is not above the law, he or she must still behave in a manner that is legal and they should act with integrity.

In collecting information***, investigators may have distinct advantages*** over higher profile people, like the police, or untrained citizens. These include:

- **Anonymity –** one of the main factors that make PIs valuable for gathering evidence is that they do not come across as suspicious, or as people who should be avoided. For instance if you are the party being wronged, then naturally the perpetrators won't discuss their plans or continue their actions in front of you. However, if the PI just seems like a regular, uninterested third party, then they may be much more likely to let their guard down.

- **Experience –** Private investigators are good at what they do. They know how to watch and listen without being obtrusive and they have the experience and resources to get full, detailed information. A non-professional might make a lot of mistakes that would either give them away or fail to garner enough information to be useful.

- **Time –** Private investigators have the luxury of taking their time and waiting for opportune moments to occur. If a regular person were attempting the same thing then it is very likely that their regular life would get in the way. They would need to go to work, attend to their families, take care of personal business. With a PI their job is what they are doing so they can give it their full attention.

- **Freedom –** People involved in the legal system are bound by much more strenuous rules and requirements, ***like the fourth amendment***, than everyday people such as private investigators. For example police officers will need to have warrants. Attorneys and judges must also carefully follow codes of conduct and extra laws. However, a private investigator will generally have all of the regular freedoms of any other citizen, which can allow them to do things and obtain information that would not be possible for someone in the legal sector.

  However, PIs are not obligated by law (as law enforcement *is* obligated by law) to reveal their observations or seizures to the other side. For example, in a custody case, PIs photographed drug manufacturing at an estranged spouse's house to obtain sole custody for the husband. If the estranged wife's attorney had caught wind of this evidence and subpoenaed to have it turned over, the husband's attorney would have used the **work-product doctrine** (which has nothing to do with Fourth Amendment protection and has everything to do with attorney-client privileges) to bar the revelation of the documents and testimony.

## ***Types of Evidence***

The main types of evidence collected includes:

- Testimony. An oral statement that a witness has made in open court.
- Real Evidence. Typically a material object of some form that can be inspected.
- Hearsay Evidence. When a witness or individual makes a statement in the course of their testimony. It can also be referred to as an "out of court statement."
- Original Evidence. This is another type of "out of court statement" that is presented for a relevant purpose, such as to prove someone's mental state.
- Documentary Evidence. Documents that have been produced to be inspected in the courtroom. The documents can be real, original or hearsay.

## ***Work Privilege / Loss of Evidence***

PI's are normally afforded protection of attorney work privilege as the agent of the attorney. However, when work privilege protection fails, evidence can be considered inadmissible.

In **Roberts v. Americable International, Inc**. (1995), the plaintiff asserted work product and attorney client privilege with respect ***to secret tape recordings of conversations between plaintiff and the individual defendant manager*** for use in an employment discrimination case. Plaintiff asserted attorney-client privilege and work product protection. The court denied the privilege assertion because none of the recorded communications was for the purpose of seeking legal advice, i.e., they were ***not admissible in court***. The court further ruled the materials were not attorney work product because the recordings did not reveal the mental processes of the attorney or investigator— neither of whom were parties to the taped conversation.

***Secret recordings*** pose a number of problems related to admissible evidence. First, it is considered to be an ethical violation to secretly record another party. Such recordings may violate other applicable regulations such as ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 01-422 (2001). Where secret recording violates state law or under professional rules relating to fraud and deceit, work product protection does not apply. Even when the recordings are lawful, attorneys and investigators alike,

should keep in mind the evidentiary issues they raise, including the quality of the recording and authentication.

In **Laxalt v. McClatchy**, evidence was inadmissible because investigators refused to identify key witnesses in connection with a libel action. The court drew a line, however, at requiring investigators to point out which witnesses they had interviewed, and to state which documents they had been shown by defendants, since this type of information was likely to reveal the type of mental impression and trial strategy that the work product doctrine protects.

Even when a privilege applies to an investigator's work, it may be waived under the same rules and exceptions applicable to attorneys. ***By listing a private investigator as a witness, a party is deemed to waive the work product privilege with respect to matters covered in the investigator's testimony***.

Voluntary disclosure to others and failure to timely assert work product protection or attorney-client privilege are other common sources of a potential waiver.

## ***Illegal Acts***

***Dumpster diving*** by a PI led to court sanctions and ***loss of admissible evidence*** in **Slesinger v Walt Disney** (2007). To satisfy their ethical obligations, the lawyers in the above example could not simply instruct the investigator to avoid unlawful conduct. Despite the private investigator being admonished to "obey the law." Plaintiffs claimed royalty payments allegedly due for Winnie the Pooh Merchandise under a licensing agreement with Disney. The Court issued terminating sanctions after plaintiffs' investigator was found to have ***stolen more than 6,000 pages of documents from garbage dumpsters located at multiple Disney document production facilities***. In affirming the sanction, the appellate court ruled that plaintiffs failed to adequately supervise the investigator's activities, that circumstantial evidence showed their knowledge or deliberate indifference to his trespasses, and that they were vicariously liable for his work.

## ***Ex Parte Communications***

Ethical rules prohibit an attorney from communicating about the subject of the representation with a witness the attorney knows to be represented by another lawyer, without the consent of the witness's counsel. The same rules apply to private investigators.

That is not to say that all inadvertent or unwitting contacts with a represented party will result in sanction and loss of evidence. Many courts would find no violation if the investigating attorney does not actually know that the witness is represented in the matter at the time of the communication. In **Jorgensen v. Taco Bell Corp**. (1996), the trial court declined to find unethical conduct in connection a pre-litigation investigation in which plaintiff's investigator interviewed Taco Bell employees before the plaintiff had filed a complaint. The Court held that it was not possible for the attorney to know that Taco Bell was represented in the as-yet-unfiled matter. The court did not require the attorney to contact Taco Bell's in-house counsel to determine whether Taco Bell was actually represented in the matter before making contact. This rule will not be the same for every jurisdiction.

Before interviewing or communicating with a third party or potential witness, consider whether the contact falls within the ethical rules. Has a complaint been filed? Do you know whether the third party is represented? How does your jurisdiction define knowledge of representation, and whether a particular witness is represented by corporate counsel? Is the witness a low-level employee of an adverse party? If so, did they engage in any acts or omissions which might be imputed to their employer for liability purposes? These rules apply regardless whether the "ex parte" contact is initiated by an attorney, investigator or other person supervised by the attorney or investigator.

## ***Electronic Evidence***

Due to the enormous growth in electronic correspondence, electronic writings (also known as e-evidence) have evolved into a fundamental pillar of communication in today's society. Not surprisingly, various forms of electronic evidence (*i.e.*, e-evidence) are increasingly being used in both civil and criminal litigation.

***Admissibility of electronic evidence*** is governed by a four criteria:

1. ***Authenticate or Identify.*** Authentication means the party offering the electronic evidence must present sufficient evidence to support a finding that the exhibit in question is what the proponent claims it to be, usually by testimony by a witness with knowledge that the exhibit is what it claims to be.

2. ***Hearsay or Not?*** Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in

evidence to "prove the truth of the matter asserted." One proven method to determine whether a statement constitutes hearsay is to apply what has been referred to as the "Fool-Proof Hearsay Test": 1) Ask whether the relevant purpose for offering the out-of-court statement is its truth; if the answer to that question is "yes," the out-of-court statement is hearsay. 2) If the answer to the question is not clearly "yes," ask "Must the content of the out-of-court statement be believed in order to be relevant?" If yes, the statement is hearsay. If no, the statement is not hearsay.

3. ***Relevant" and Not Unfairly Prejudicial?*** Relevant evidence "means evidence having any tendency to make the existence of a fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."

4. ***Not "Privileged" Communication?*** This identifies various communications (*e.g.*, husband-wife; attorney-client; doctor-patient; clergy, etc.) that are considered "privileged" and thus, not admissible unless the privilege is deemed waived.

***Websites.*** Information appearing on private, corporate and government websites is often proffered as evidence in litigation. Printouts of web pages must be authenticated as accurately reflecting the content and image of a specific web page on the computer.

Information retrieved from government websites is self-authenticating, subject only to proof that the webpage does exist at the governmental web location. On the other hand, private websites are not self-authenticating and therefore require additional proof of the source of the posting or the process by which it was generated. For example, in assessing the authenticity of website data, important evidence is normally available from the person(s) managing the website ("webmaster"). A webmaster can establish that a particular file, of identifiable content, was placed on the website at a specific time. This may be done through direct testimony or through documentation, which may be generated automatically by the software of the web server.

The most common method of authenticating website data is having a competent witness testify that he typed in the URL of the website; that he logged onto the site and viewed what was there; and that the exhibit (printout) fairly and accurately reflects what the witness saw.

***Social Networks.*** Social networking websites permit their members to share information with others. Despite the novelty of social network-

generated documents, courts have applied traditional concepts of authentication under existing rules of evidence. The key issue is typically one of authorship: Who authored/posted the proffered document in question? Because of the increased dangers of falsehood and fraud with this new type of medium, courts have imposed a heavier burden of authentication on social network messages and postings.

Generally, there must be confirming circumstances sufficient to permit the inference that the purported sender was in fact the author. As with email, the electronic signature on a document must be corroborated with additional proof of the identity of the sender, such as application of the reply letter doctrine, content known only to the participants, or retrieval of messages from a specific computer.

Generally, electronic conversations on social networking sites (instant messaging) can be authenticated by testimony from a participant in the conversation that (a) he or she knows the user name on the social networking site of the person in question, (b) that printouts of the conversation appear to be accurate records of his or her electronic conversation with the person, and (c) a portion of the contents of the communications are known only to the person or a group of people of whom the person in question is one. In the absence of significant corroboration courts have excluded social network messages, stating their concerns with the website's security and the potential for access by hackers.

***Emails.*** Like internet evidence, email evidence also raises novel authentication issues. The general principles of admissibility are essentially the same since email is simply a distinctive type of internet evidence; namely, the use of the internet to send personalized communications.

Authenticity is often established by testimony of a witness who sent or received the emails, in essence, that the emails are the personal correspondence of the witness. Testimony from a witness with knowledge that the emails were exchanged with another person constitutes prima facie evidence of authenticity.

***Text Messages.*** Like email, text message evidence also raises novel authentication issues. The general principles of admissibility are essentially the same since text messages are a distinctive type of electronic evidence, namely, the use of a cell phone to send personalized electronic communications. Text messages sent between cell phone users are treated the same as email for purposes of authentication.

Typically such messages are admitted on the basis of identifying the author who texted the proffered message. Like email and social media, text messages have certain seemingly self-authenticating features. For example, email messages are marked with the sender's email address, text messages are marked with the sender's cell phone number, and Facebook messages are marked with a user name and profile picture. Nonetheless, given that such messages could be generated by a third party under the guise of the named sender, the majority of jurisdictions have not equated evidence of these account user names or numbers with self-authentication.

***Computer Documents.*** When a computer is simply used as a typewriter, computer-stored documents may be authenticated by a percipient witness or by distinctive characteristics that establish a connection to a particular person. The mere presence of a document in a computer file will constitute some indication of a connection with the person or persons having ordinary access to that file. However, much will depend on the surrounding facts and circumstances, and it is reasonable to require that these include some additional evidence of authenticity.

# HACKING

## *Nerds Hired To Hack*

A couple of San Jose investigators and two hired computer hackers were indicted in a series of 2015 crimes related to a conspiracy to access the e-mail accounts, Skype accounts, and computers of people opposing the PI's clients' in civil lawsuits.

Specifically, a federal grand jury indicted the defendants, charging them with one count of Conspiracy, in violation of 18 U.S.C. § 1030(b), six counts of Accessing a Protected Computer and Obtaining Information, in violation of 18 U.S.C. § 1030(a)(2)(C), and two counts of Interception of Electronic Communications, in violation of 18 U.S.C. § 2511(1)(a).

The Indictment alleges that the object of the defendants' conspiracy was to obtain information that would assist clients of the investigators. The nerds were hired to hack into the victims' e-mail accounts, Skype accounts, and protected computers. In addition, the defendants allegedly installed and used a ***keylogger***—a tool that ***intercepts and logs*** the particular keys struck on a keyboard in a covert manner so that the person using the keyboard is unaware that his or her actions are being monitored—to obtain information that would assist the PI clients..

## ***Islamic Militants?***

A Florida private investigator faced criminal charges over his alleged effort to ***infiltrate a charity's computer network while researching whether nonprofits are financing Islamic militants***. According to the complaint, an unidentified global charity headquartered in New York experienced about 390,000 attempts to gain unauthorized access to its computer network over a three month time frame.

The attempted intrusions, which disrupted employees' ability to access email and conduct business, were made by computers associated with two internet protocol addresses subscribed to by the PI at his home in Florida, the complaint said.

Prosecutors said U.S. Secret Service agents on Friday executed a search warrant at the investigator's home, seizing among other things, 30 computers and notes related to the charity, one of its executives and a third person publicly linked to it.

The computers contained a list of the charity's employees' email account user names and a so-called ***brute force password-cracking tool*** designed to launch a barrage of potential passwords at an email account to guess at the correct one.

According to the complaint, the investigator told the agents he was researching charities to determine if any were unintentionally financing jihadist groups by sending funds to Middle East charities that were then seized by Islamic militants. The investigator said he had conducted the research in his role at a private investigator with hopes to sell it, the complaint said.

## ***Hackers For Hire***

***Hacktivists*** or criminal gangs, is a growing cottage industry of ordinary people hiring hackers for much smaller acts of espionage. In the typical scenario, lawyers seek to ***hire a private investigator who is willing to skirt the law but do so in a way that gives them plausible deniability*** of any potentially illegal activity.

According to Daniel B. Garrie, executive managing partner with Law and Forensics, a computer security consulting firm. "A law firm is well advised to create a written record with the private investigator so there is no misunderstanding later on," said Mr. Garrie, who is a lawyer. "A lawyer

should never hire an individual to hack except in a very narrow and limited circumstance where the side being hacked has consented to the action or there is a court order permitting the hacking."

In London, a private investigator played a chief role in the criminal prosecution of Andy Coulson, the former editor of the tabloid News of the World, which had a practice of hacking into voice mail messages left on mobile phones. The investigation found that some editors of the tabloid, which is now defunct, had paid an investigator to hack into voice mail messages as a source of leads for articles.

In the United States, the hacking that some private investigators are involved with is far different from the recent prominent online attacks on companies like Anthem, Target, Sony and JPMorgan Chase. In those cases, cybercriminals or hackers, often working with the blessing of foreign governments, initiated large-scale assaults to obtain the internal emails of executives or sensitive personal information about customers or employees.

Much of the hacking by private investigators is narrower in scope, usually limited to obtaining email login credentials or unearthing information from social media accounts, security experts said. It is similar to many of the dubiously legal jobs now being advertised on ***Hacker's List***, an online forum where hackers can bid anonymously for a job posted by person looking to conduct some espionage.

A representative for Hacker's List, which warns customers not to post jobs that involve breaking the law, said 181 of the 1,942 active projects posted on the website had been completed by a hacker.

## ***Police Hacker For Hire***

As described in greater detail in **USA v Buell** (2004), officer Buell, the defendant, accessed a federal law enforcement database using a New York state computer system on at least 15 occasions to obtain criminal history information and other personal information related to witnesses and other individuals associated with at least 11 federal criminal prosecutions in the Southern District of New York on which PI Dwyer, the defendant, had been retained as a defense investigator and paid with public funds. During the same time period, ***Buell deposited into his personal bank account at least 17 checks issued by IRG totaling nearly $9,000. The investigation has further established that Dwyer submitted billing invoices to the Criminal Justice Act ("CJA") administrative office*** in the Southern District of New York seeking payments and reimbursements for purported

investigative work performed to obtain criminal histories of the individuals associated with the federal criminal prosecutions, when in truth and in fact, Dwyer had illegally obtained the criminal history information through bribes paid to Buell. The United States Treasury Department issued checks on these invoices, which were mailed from a location outside of the State of New York to DWYER's office on Long Island, New York.

# PROFESSIONAL MISCONDUCT

## *Records & Communication*

In **Frank v Louisiana Board of PI Examiners** (2016), a host of investigator issues surfaced that eventually lead to a revocation of the PI's license. The case started out as a search for a biological mother. In 2008, the client (an 18 year old son and his dad) hired the PI to seek her out. Services were discussed, a contract signed and a $2500 retainer deposited.

In early 2009, the investigator shared his research with the boy. Without providing a specific name, he provided the son with a list of choices he had narrowed to four individuals. He could go further, but informed the boy he needed more money. Nothing more happened until 2012 when, tragically, the boy ended his own life.

In the months that followed the son's death , the father decided to continue the search that the investigator had begun. However, the investigator told the father that as a business practice, all records after 3 years were destroyed. He would have to start over and he would need a new retainer fee of $5,000. The father thought this was inappropriate and contacted the Louisiana Board for assistance. The complaint led to an administrative hearing and the revocation of the PI's license.

The board decided that the investigator's actions constituted ***professional misconduct*** by:

- Not keeping the client ***reasonable informed*** through the investigative process
- ***Failing to produce records*** -- a written report / file. This allegation was later reversed as the jurisdiction states records need to be kept only three years.
- ***Misconduct*** in that (he ***told client that records were routinely destroyed*** after 3 years but he admitted in the board investigation that he still had the file).

It should be noted that the Board made it's decision in part due to the PI's lack of recall, lack of cooperation and inconsistency in his answers. Further, the investigator generally lacked knowledge about the original contract, how he collected information in this case or how it was backed-up.

# EMBEZZLEMENT

## *Investigator Participated in Alleged Embezzlement.*

In 2016, a former police officer turned investigator was accused of embezzling $7 million from the Kaiser Foundation Health Plan.

The investigator became senior supervisor in charge of investigating fraudulent insurance claims at Kaiser Foundation Health Plan. He worked in Oakland and was responsible for hiring investigators to conduct surveillance on people who were suspected of filing fraudulent claims. The investigator was authorized to approve charges of as much as $50,000.

In the end, he was ***submitting invoices for investigative services that were not performed*** or were not justified over a 16-year span after he joined the company in 1998.

Attorneys for Kaiser said much of the work was never done . . . "the investigator regularly directed Kaiser to pay invoices for investigative services that were not in fact performed, as well as invoices for work that was performed but nonetheless was not in fact justified.

Several Bay Area investigators were said to have been hired — they are named as co-defendants in the civil case. The Kaiser investigator regularly purported to work for and regularly accepted payment from these contracted PIs.

By the time Kaiser learned about the alleged racket, the investigator had processed 718 suspicious invoices, totaling just over $7 million.

# ASSET SEARCHES

A divorce, inheritance or creditor trace assignment might involve an investigator's search for hidden assets. Asset leads are discovered by reviewing passports, phone records, bank account statements, credit card transactions, tax filings or other confidential information.

***Obtaining this confidential information illegally could land you and your client in a lot of hot water***, especially where both parties knew the confidential information was to be obtained in a suspect manner.

## ***Confidential Information Illegally Obtained***

In **USA v Torrella** (2007) several private investigators and their information brokers were accused of illegally obtaining confidential information during asset search investigations they performed for their clients. According to a U.S. Attorney press release, if the clients knew the '***confidential information was obtained illegally***' he might pursue prosecution of them as well.

The subjects of the investigation had not given permission for their personal information to be disseminated. Using names, addresses, social security numbers and other personally identifying information of people they had been hired to investigate, the PIs and their data brokers would ***call various government agencies posing as other people to obtain personal records*** -- obtaining or attempting to obtain confidential information on more than 12,000 people nationwide.

The private investigators had been hired by attorneys, insurance companies and collection agencies to investigate the backgrounds of opposing parties, witnesses and benefit claimants, and to uncover assets or income. A variety of strategies were used to trick the government agencies to provide them information they wanted. With the IRS they would ***impersonate a taxpayer and ask for past tax returns***, claiming that a bookkeeper was being investigated for embezzlement. On other occasions they would ***similarly claim to be the taxpayer, in the hospital awaiting surgery, and needing the tax returns*** to demonstrate to the hospital that they could pay for the services.

In calls to various agencies and financial institutions the "pretexters" ***claimed various hardships such as being a battered spouse, facing bankruptcy, foreclosure or serious illness.*** In one case the pretexter tried to ***claim she needed the information because a child had been abducted***. Or in another instance they would ***call pharmacies and hospitals posing as someone from the subject's doctor's office, for the purpose of obtaining medical information.*** The information was then forwarded to private investigators for fees ranging from $30 to $300 per record.

An indictment charge of the data brokers and the PIs who used them exposed the alleged theft and misuse of confidential information from various state and Federal record systems, including those relating to the Unemployment Insurance program.

Conspiracy is punishable by up to five years in prison. Wire Fraud is punishable by up to 20 years in prison. Fraudulent Elicitation of Social Security Administration Information and Solicitation of Federal Tax Information are punishable by up to five years in prison. Aggravated Identify Theft is punishable by a mandatory two year term on top of any sentence on the underlying offenses.

***"This indictment alleges that private investigators across the country illegally obtained confidential information and sold it to the clients who hired them,' said United States Attorney Jeffrey C. Sullivan. 'This is a very serious matter, the investigation is continuing and it is our intention to go after these 'clients' if we can prove that they knew this information was obtained illegally."***

## ***The Fred Abrams Blog***

Fred Abrams is an attorney who represents the victims of asset concealment schemes. He searches for assets which individuals and corporations may have hidden. He does this through court-ordered discovery or the pursuit of other legal remedies. In an effort to protect consumers, Fred's ***assetsearchblog.com*** reveals many illegal schemes as well as PI blunders you should know. Here are just a few:

***The Wire Fraud (email)Case.*** *"K.C." hired a PI to investigate a suspected stalker.* She made 59 payments to the investigator who represented to "K.C." that some of the payments would be given to "Scott", a Captain with the local police who could help with the investigation.

The PI even supplied "K.C." with e-mails purportedly sent by "Scott" & represented that "Scott" was a potential romantic suitor for "K.C." The ***investigator, however, never paid anyone named "Scott", to investigate on behalf of "K.C."*** It was a complete fabrication. Given all of the foregoing, federal prosecutors in USA v. Walker-Halstead charged the PI with 11 counts of wire fraud based on the alleged false emails.

The PI ultimately pleaded guilty to one count of wire fraud, sentenced to 12 months & 1 day of imprisonment and ordered to pay restitution to "K.C." in the amount of $500,000.00.

***The False Records Case.*** From about 2006-2012 ex-Toronto private investigator E. White &/or her ex police detective husband offered asset searches including a search for bank accounts. Their clients were licensed private investigators, divorcing spouses & others seeking assets hidden from them***. Unfortunately, the Whites supplied their clients with phony financial data/spurious bank account information***. They were later criminally charged with providing clients with "**false and fraudulent data and fabricated bank records…**" In 2014 both were both sentenced to 66 months in prison, 3 years of supervised release and ordered to pay $1,021,738 in restitution.

***The New Jersey Wife Case***. Ralph was a medical doctor with a thriving private practice, yet in his New Jersey divorce he claimed a low net worth. Ralph's divorcing wife Nancy suspected Ralph had hidden money in anticipation of the divorce. Nancy gathered documents she obtained during the pretrial discovery phase of the divorce and before.

These documents included copies of Ralph's: passport, statements for airline frequent flyer miles, phone bills, tax filings and additional financial records. Nancy gave the documents to Mike, the licensed private investigator Nancy retained to perform an asset search regarding Ralph. After conducting an investigation for more than a month, Mike told Nancy that Ralph hid monies at offshore banks and at a bank in Nevada.

Mike stated that Ralph secretly maintained about $2.5 million dollars in the offshore bank accounts which were located in ***high-risk geographical locations*** known for money laundering. Ralph had supposedly hidden another $85,000 dollars in the secret bank account in Nevada. Mike explained to Nancy that he could collect evidence regarding the secret bank accounts by conducting searches at the Nevada and the offshore banks.

Nancy paid Mike over $10,000 dollars for the bank account searches and Mike provided Nancy with an investigative report summarizing his search results. The report named the offshore banks and the Nevada bank Ralph supposedly used to hide his money. It supplied the purported secret bank account numbers; account balances and detailed the bank signatory information.

The report meanwhile, never explained the source of Mike's information/how Mike detected Ralph's supposed secret bank accounts. When Nancy asked Mike how he had obtained the information at the report, Mike said the report was completely reliable. A trusted colleague supplied Ralph's offshore bank account information, Mike said. Mike also explained he obtained Ralph's Nevada bank account information from an

"insider", a teller who worked for the Nevada bank. According to Mike, the insider used the bank's computer system to sneak a peek at Ralph's $85,000 dollar bank account.

***Assuming that Mike's representations to Nancy were true, then the bank teller and Mike could have violated privacy and other U.S. laws.***

# TESTIMONY

The law has traditionally regarded the testimony of private investigators with some ambivalence. On the one hand, the testimony of investigators is essential to the effective discovery and proof of events such as adultery. On the other hand, ***PIs have had such credibility problems over the years*** that the law has become careful about accepting their testimony.

Aside form the credibility issue, the reason for receiving the testimony of a hired employee, or investigator, with great caution is obvious. A man who sets himself up as a discoverer of supposed delinquencies, ***whose pay depends upon the extent or success of his employment***, the extent of his employment depending upon the discoveries he is able to make, becomes a most dangerous witness. The courts have therefore been slow, or rather cautious, in receiving such testimony.

While the above statements certainly cover some of the policy reasons behind the rule, they do not fully explain it. ***Expert witnesses*** on such questions as valuation and earning capacity are likewise employed by each party, not to determine truth, but to support a particular position. Courts certainly do not regard the parties' expert witnesses as disinterested, but neither do they routinely go out of their way to require that their testimony be viewed with "great caution" or "minute scrutiny." Moreover, the parties themselves are even more interested in the case than their investigators, yet no special standard of credibility (apart from the common-law corroboration requirement) applies to their testimony. The mere fact that the investigator has a financial interest in the case therefore does not explain why there is a special credibility standard applying only to detectives.

The ***most powerful evidence is direct testimony of a witness who observed the act in question***. When an investigator presents this type of direct evidence in a facially credible manner, that evidence is usually sufficient to prove the case. However, this being a blunders course, it doesn't always go as planned as you will read among several adultery cases:

***The Back Door Was Not Covered*** A spouse who has been observed staying overnight with a "friend" will sometimes claim that the detective's testimony is not persuasive unless all exits from the residence in question were under observation by detectives. Otherwise, the spouse will claim, there is no proof that either the spouse or the "friend" did not leave and return. In most cases, this argument has failed. However, in **Everett v. Everett** (1977), the investigators saw the husband stay overnight with his "friend" on two separate occasions. The trial court held that the ***investigators testimony was not not proven because the back door of the home was not under observation***. The husband admitted staying overnight with the, however, denying only that sex had occurred.

***Missing Minutes.*** In **Deckman v. Deckman** (1972), the investigator testified that the wife and her "friend" arrived at 2:45 a.m., entered the wife's home, and turned out the lights. The investigator left at 4:00 a.m., but testified that the friend's truck was still at the wife's home when he checked at both 7:51 a.m. and 11:09 a.m. He admitted that he had not kept the back door under observation.

***Positive Identification***. It is essential, of course, that the investigator be able to testify positively that the opposing spouse was one of the persons who stayed together overnight. In **Bynum v. Bynum** (1974), the husband sought to prove that the wife was committing adultery with a certain Dr. Mullen. To prove his claim, he introduced the testimony of a detective hired by Mullen's wife to follow Mullen. The detective testified that he saw Mullen and a woman spend the night in a hotel room, and even testified that the woman had come outside the door briefly in the morning, in bathrobe and curlers, to check the weather. The problem, however, is that the detective was not able to give a very good description of the woman. He did identify the wife in court as the woman he had seen, but he admitted that he did not get a very good look at her, and his description of her features was vague. The court held that adultery had not been proven. The detective in Bynum did a very good job of proving that adultery had been committed, but a very bad job of proving that it was committed by the wife.

***Two Men.*** The Weaver v. Weaver (1983) case testimony of an investigator failed to prove adultery. The wife was seen in residence with two men at 7:45 p.m., and left the next morning at 6:30 a.m.; because two men were present in the residence, there was insufficient proof of adultery.

***Less Than a Full Night***. When the other spouse and his or her "friend" have not spent an entire night together, some courts have held that adultery is not proven. For example, in **Painter v. Painter** (1975), the

investigators saw the husband and his "friend" embracing and kissing in a car. They then observed the husband's truck parked in the friend's driveway at 11:55 p.m., and saw the husband leave at 1:45 a.m. the next morning. The court recognized that the circumstances created "grave suspicion" of adultery, but held that there was not sufficient evidence to prove adultery.

***Just A Kiss***. Likewise, in **Dooley v. Dooley** (1981), the investigators saw the wife's friend's car parked at her home at 10:55 p.m. The friend stepped out onto the porch, kissed the wife, and left at 1:10 a.m. On a second night, the friend did not leave until 2:45 a.m. The court again found the evidence insufficient to prove adultery.

***Everyone Likes Trains.*** In **Armour v. Armour** (1946), the investigator testified that he followed the wife and a gentleman friend in his car, and that when they took a train, he parked his car and took the same train. When they left the train, he said, he followed them again. He saw them embrace after leaving a restaurant, and he saw them kissing in a car. When asked where he stood when he saw these things, however, he responded that he sat in his car. This could not have been so, for, by his own testimony, he had parked his car before taking the train. The court reversed a lower court decision holding that the wife had committed adultery.

***On the Porch.*** Likewise, in **Gray v. Gray** (1943), two investigators claimed that they had seen the wife commit adultery on a cot on the screened-in back porch of her duplex home. The wife and others familiar with the neighborhood testified, however, that the investigators could not have seen into the porch from where they claimed to stand. The porch was screened into two portions by a partition, one portion of which belonged to the residents of the other half of the duplex. The residents of that duplex slept on the porch that night, and testified that they would have heard sounds if adultery had been committed. Finally, there was evidence that a number of dogs were running loose in the back yard, and that they would have barked if the detectives had actually been present observing the porch. A trial court decision refusing to find adultery was affirmed upon appeal.

***Unprofessional Behavior by the Investigator***. An investigator's testimony is also likely to be discarded when he behaved unprofessionally in the course of gathering evidence. The classic example of this point is the bizarre fact pattern presented to an Alabama court in **Pitchford v. Pitchford** (1931). In that case, a team of PIs saw the wife, her female roommate, and a man enter the wife's two-bedroom second- floor

apartment. The detectives entered the first story of the building and listened upward, identifying barefoot footsteps and bedsprings, and concluding that some sort of sexual act was in progress. Three hours later, at 2 a.m. to 3 a.m. in the morning, the detectives decided to collect clear evidence of the activities above by forcing entry into the apartment. The wife and her roommate resisted the forced entry and placed a "riot call" to police headquarters, with the result that police officers escorted the detectives out of the building. Amazingly, the detectives conceded that while they were listening on the first floor, they had left no one observing the front door, so that the man could easily have left without being observed. Not surprisingly, the court found the wife innocent of adultery.

# CONTRACTS

***Pursuit Magazine*** says that "***PI contracts are crucial in the private investigation business. Never accept an assignment without having one*** in place!" They cite the following reasons:

- First, you want ***to get paid*** for your work! A well-written contract for services or retainer agreement spells out terms of work and billing rate, and it specifies how payment will be made.

- If a client balks at your invoice, then you have evidence of the agreement that hopefully will stand up in court should in case of non-payment and breach of contract. There are penalties for not paying and/or trying to reverse the charges on the credit card used to pay for services as well.

- A contract for services or retainer agreement maximizes an investigator's protection in the event of a client dispute. Other client problems such as misunderstandings, refunds, complaints, or clients threatening to sue, can easily be avoided or defended with a properly drafted and executed contract or retainer agreement.

- ***Contracts manage client expectations*** rather than to absolve or indemnify your company of any perceived liability which may arise from our investigation. Very few "retail" clients have a realistic understanding of the investigative process and what they can or cannot expect; this isn't *CSI Miami* or *Magnum PI,* and the end result of any investigation may be less than dramatic and not what the client had expected. A great contract diffuses unrealistic expectations and helps to prevent "buyer's remorse" when an investigation doesn't turn up hoped-for slam-dunk evidence of an affair.

- Sometimes the difference between stalking and surveillance is a contract. If the subject of your investigation calls the police, the responding officers are going to want a good explanation for why you have been "harassing" the complainant. A crime of stalking or harassment requires the intent to create distress in the victim, and ***evidence that you are a disinterested professional diligently working on behalf of a third party*** could go a long way in sorting out the mess before it lands you in jail.

Other pitfalls to watch according to Pursuit Magazine:

- Mapping out ***what the client intends to do with the information*** you obtain during the investigation will reduce an investigator's liability in the event of a client dispute or a client's misuse of the information obtained during the investigation.

- ***Using a*** **database provider** to get the job done? Try to closely match some portion of the description of the purpose of the investigation to a "GLBA Permissible Purpose" which the data broker, e.g., *"The client is employing the services of the agency in order to conduct surveillance upon John Smith (subject) in an effort to determine the extent of the subject's injuries as it relates to a potential legal liability claim against the client."*

- ***Failures in communication*** are the most common source of friction in investigator-client relationships. The investigator should keep the client reasonably informed about the status of a matter, promptly comply with reasonable requests for information from the client and provide client with adequate information to participate judiciously in decisions concerning the objectives of the investigation.

- Provide a ***non-guarantee statement*** in your agreement saying that you will do your very best to collect the facts they are looking for but that there is no guarantee you will obtain the exact results they desire.

- A ***limitation of liability clause*** is often inserted into a contract to exclude or limit your liability for breach of contract or negligence.

- A ***disclaimer*** is generally any statement intended to specify or limit the scope of rights and obligations that may be exercised and enforced by parties in a legally-recognized relationship. e.g., *There is no restraining order or protection order against me (CLIENT) for this*

*individual. _____,* and/or *There has never been a charge of stalking or aggravated stalking against me (CLIENT).*_____

## ***Contract Not In Writing***

A wife and U.S. Citizen followed her husband to Lebanon (his natural country) for better employment. Once there, the relationship deteriorated and husband became increasingly abusive to wife. Fearing the husband was tapping her phone, and her children would not be allowed to leave, she contacted a private investigator and entered into an ***oral agreement*** to help remove the children from Lebanon.

The wife paid the retainer fee of $15,000, hourly and daily rates depending on where the services were provided, plus fees and costs, and the PI defendant attempted to extricate her and her children from Lebanon. The PI was unable to help but still wanted payment for additional expenses. A breach of contract suit entailed.

In testimony, the ***client admitted*** that she agreed to the fee schedule asserted by defendant, but that "she agreed to pay the fees if defendant met its obligation under her agreement with defendant." Defendant also contended that the parties agreed upon the rates for services at $75.00 per hour for all services not requiring travel outside of the United States, and $750.00 per day plus costs and expenses for all services provided outside of the United States.

In her deposition, the client plaintiff also said the PI made no guaranties with respect to when, if at all, she and the children would be removed.

Despite the contract not being in writing, this time, the PI was lucky and the court agreed there was a legal agreement and the wife needed to pay the additional costs. Next time . . . who knows???

## ***Contract Lacked Witness Fees Provisions***

Shortly after plaintiffs' arrival at hotel Dixie Landings, Mrs. Wyatt was injured in an accident involving the tram used by Dixie Landings to transport hotel customers from the registration desk to their rooms. In **Wyatt v WDW** (2002), Plaintiffs sought compensatory and punitive damages, intentional infliction of emotional distress as well as counsel fees. Based upon the alleged conduct of defendants, the defense retained an investigator to investigate the accident.

Keys investigation involved only conducting surveillance of the injured plaintiff in public. Unfortunately, the PI could foresee being hailed into court in North Carolina for the claims filed. The basis for Plaintiffs' emotional distress claims were committed in North Carolina by the private investigator.

The actual facts of the case and outcome are not as important as the fact that ***the jurisdiction of the Wyatt v WDW case was changed from Florida to North Carolina. The PI, who was based in Florida, now had to make numerous trips for depositions and a trial***. Since his contract did not have a witness reimbursement clause, he paid for all the travel and accommodations out of his own pocket.

## *Was PI An Agent or Independent Contractor?*

Mrs. Nobel was the plaintiff in an action against Sears for personal injuries allegedly caused while she was shopping in a Sears store. The attorney defendants were employed by Sears to defend that action. Defendant Pruitt, an investigator, was hired to assist in preparing the defense. The attorneys desired to take the deposition of a man named Bohm, who had accompanied plaintiff on her shopping trip. That effort was frustrated because plaintiff either could not procure or did not have an address for Bohm. In an effort to secure the address from plaintiff, an employee of Pruitt, named Lemon, gained admittance to a hospital room where plaintiff was confined and, by deception, secured the address.

It is that alleged invasion, and Lemon's conduct while in the room, which form the basis for ***plaintiff's claim of injury***. Additional charges against the investigator in this case include: Trespass; battery; fraud; negligently caused physical, mental and emotional injuries; invasion of attorney-client relationship; invasion of privacy; negligent entrustment of agents (two counts); conspiracy; violation of statutory duties; and violation of attorneys' ethics.

Plaintiff argues that an ***unreasonably intrusive investigation***, which plaintiff has alleged in her sixth cause of action, is a tort for which damages are recoverable. The court agreed that the investigator was intrusive and his actions a violation of the plaintiff's right to privacy.

The unknown in this case was whether the PI was to be considered an agent of Sears independent contractor responsible for his own actions. There was nothing in the contract between the Sears attorney and the PI as to the relationship (employee, independent contractor, etc). However, the court reasoned that even though hirers of an independent security or

protective agency have generally been held not liable for negligent torts of agency personnel, ***where the professional hirer did not exercise control over them, hirers have been held liable for the intentional torts of the agency's personnel committed, in the scope of the agency's employment, against the hirer's invitees.***

Plaintiff here alleged a duty on the part of Sears and its attorneys to supervise their agents, and that failure to exercise supervision constitutes negligence. Absent language in the PI contract as to whether the private detective was an independent contractor or agent, and without any discussion as to possible differences in liability where the agency is hired to protect rather than investigate, the court held that there was sufficient evidence to support the jury's finding that Sears was liable.

## ***Right To Control PI***

King, contracted with Smith Protective Services, Inc. to investigate a number of his competitors in the equipment business. A contract between King and Smith Protective Services, Inc., reflects that King contracted with Smith to conduct certain investigative services and agreed that the services would be performed by licensed investigators if required by law.

In particular, King wanted to determine ***who was selling parts to a competitor*** "at a lowest cost than what was the normal rule within his area." Cal Meyers, a manager at Smith Investigations, testified that King explained to him what was required in order to satisfy the John Deere people that someone was infringing upon his region. Meyers stated that King told him that ***the only thing that would satisfy the John Deere people would be an invoice showing a 20% discount*** and that he wanted to secure one of those invoices. "***He didn't particularly care how he went about getting it and said money was no object***."

Thompson, another Smith employee burglarized the offices of the competitor in order to obtain the sales invoices. The competitor, upon learning of the burglary, sued Smith Protective Services, Inc., Cal Meyers, the investigations manager for Smith, and, King, for damages incurred as a result of the alleged break-in. The suit also alleged that an agent or representative of the defendant King, committed a trespass.

In fact, Thompson admitted to the burglary and trespass.  And, in the end, the PI was left holding the bag since there is nothing in the testimony of Mr. King which would support the conclusion that he ***had any right to control Smith as to the method or means by which the work contracted for was to be accomplished***. There is no testimony that King

in fact instructed either Meyers, Thompson, or Dolly concerning the methods to be used in conducting the investigations. Only that we wanted results.

Was Smith an independent contractor or whether the corporation and did its employees had the status of agents or employees of King? ***The written agreement merely provides that Smith Protective Services, Inc. Will be compensated at the rate of $20 per hour plus expenses for its investigative services.*** It does not specify the services to be rendered.

Although there is no single rule that is absolute and definite, the outstanding and ultimately ***decisive consideration in determining the independence of the contract is the employers right to control the details of the work.*** The basic test of a contractor is that he render service in the course of an independent occupation, representing the will of his employer only as to the result of his work, and not as to the means by which it is accomplished. Thus, ***if the employer is interested only in the results, and there is left to the party performing such services complete control of the details as to the method and manner of such performance, then the relationship of independent contractor exist.***

## ***Non Compete Clauses***

The following letter from an investigator underscores the need to watch what is in contracts you sign. This poor fellow was unaware of a non-compete clause with his former employer . . . it virtually shut him down:

*I work as a Private Investigator, signed a non-compete agreement. I was fired for refusing to share a motel room. Binding statements: ''I will not directly or indirectly engage in any business that competes with former employer'' ''I will not directly or indirectly solicit business from...license or provide the same or similar products...as are now provided to any customer of former employer''. There are no stipulations on termination. There are time limits. I was forced to sign this document. They found I did not have a non-compete agreement and threatened to terminate after 3.5 years. I had no choice. This seems to prevent me from working as a Private Investigator in any form. I'm not sure if this is enforceable in Florida because Florida is a ''Right to Work'' state. I have been told that since I was terminated, I am free to employ myself, but I'm just not sure. I want to utilize the contacts I have developed over the years both with my former employer and with others. However, since I was fired and even though the agreement was signed under duress, I believe I have limitations and few options..*