SURVEILLANCE AND PRIVACY LAW
IOWA ASSOCIATION OF PRIVATE INVESTIGATORS

September 13, 2018

JAMES "WES" BEARDEN, ATTORNEY

BEARDEN INVESTIGATIVE AGENCY, INC.
1341 W. Mockingbird Lane, Suite 820W
Dallas, Texas 75247
(214) 220-0111 (Tel.)
(214) 855-1250 (Fax)

1980 Post Oak Blvd., Suite 1500
Houston, Texas 77056
(281) 297-8110 (Tel.)
(281) 297-8114 (Fax)

230 Polk Street, Suite A
New Orleans, Louisiana 70124
(504) 702-6786 (Tel.)
(504) 702-6797 (Fax)
beardeninvestigations.com

Disclaimer: This outline is for the purposes of CLE or other organized training. Although several statutes and case cites are referenced below, the law may have changed, it may be out dated or it may not apply to the state or local you are located in. Please consult an attorney and do not rely on this outline as a substitute for legal advice. It is recommended that you seek advice of an attorney. These materials are for reference only and are not meant to establish any attorney-client or investigator-client relationship.

I. INTRODUCTION.

A. Where is the Law?

This presentation draws from a number of areas of law that cannot be all thoroughly explored form here. This law comes from a number of areas of common law and state and federal statutes. There is no way in which we can exhaustively explore all of these areas of law. However, a good list of many of them are listed below:

1. U.S. Constitution – The highest law of the land. Particularly, 4th Amendment (protection against search and seizure) of the bill of rights that guarantees individual protection against government intrusion. But, also general privacy protections including the 1st Amendment (privacy of beliefs); 3rd Amendment (privacy of the home against use by soldiers); 4th Amendment (privacy of the person and possessions); and the 5th Amendment Self-Incrimination Privilege (which provides protection for the privacy of personal information).

2. Iowa or State Penal Code – State criminal code that contains offences which are recognized in in Texas and the penalties which might be imposed for these offences and some general provisions. Generally, Title XVI of the Iowa Code.

3. Electronic Communication Privacy Act ("ECPA") – Federal law primarily designed to prevent unauthorized access to private electronic communications.

4. Privacy Act of 1974 – Federal law that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.

5. Common Law Invasion of Privacy – Common tort law, across the United States, that allows a cause of action under four categories. Those are intrusion on seclusion, public disclosure of private facts, false light and misappropriation of a person's likeness.

6. Federal Rules of Evidence. ("FRE") - First adopted in 1975, the Federal Rules of Evidence codify the evidence law (what gets in and out of evidence) that applies in United States Federal courts.

7. Federal Rules of Civil Procedure. (“FRCP”) – The Federal Rules of Civil Procedure govern civil procedure for civil lawsuits in United States Federal District courts.

8. All Writs Act of 1789 – A federal statute which authorizes federal courts to issue all court orders necessary or appropriate “in aid of their respective jurisdictions and agreeable to the usages and principles of law.”

9. Stored Communications Act (“SCA”) – Addresses the voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers.

10. Iowa or State Disciplinary Rules of Professional Conduct (“IRPC”) –Rules that prescribe baseline standards of legal ethics and professional responsibility for lawyers in the United States. Chapter 32 of the Iowa State Court Rules.

11. Iowa or State Rules of Evidence (“IRE”) – The codified evidence law (what gets in and out of evidence) that applies in Iowa courts. Very similar to the Federal Rules of Evidence. You as an investigator should learn these.

12. Iowa or State Rules of Civil Procedure (“IRCP”) – The Iowa Rules of Civil Procedure govern civil procedure for civil lawsuits in Iowa courts.

13. Communications Assistance for Law Enforcement Act. (“CALEA”) – Enhances the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities, allowing federal agencies to wiretap any telephone, broadband Internet and VoIP traffic.

14. Iowa Code – Particularly criminal provisions and the state wiretap act.

15. State and Federal Court Decisions – Particularly those decision that are within United States Court of Appeals for The Eighth Circuit and the Iowa state courts.

II. CREATING A DECISION FRAMEWORK.

Basically, how do we make decisions regarding technology that is ever changing in a world of law that doesn’t evolve at nearly the same pace.

A. Decision Tests

This following sections deal with evidence ultimately used in a hearing or at trial and the subsequent rules for use, admittance, authentication and whether your investigative technique or method violates the law or not. Because of the gargantuan amount of conflicting law, you must create some framework by way to make a decision about whether to do what you or your client wishes.

1. Line Test – Is what your about to do going to cross the line? In reality, there are really two lines. The first is a line under which all conduct is legal, accepted, recognized and very often not even criticized. The area beyond that line is more grey. It is highly dependent on factual situations, location, and current political and legal movements. The final line is a line where activity beyond that is illegal, clearly unethical, prohibited or highly criticized. That is a "no go" zone.

2. Press Test – The below is organized according to an adopted and modified legal ethics test. Similar to the Stansfield Turner National Interest Test but, with following considerations for *all* involved:

    a. Criminal Responsibility;

    b. Civil Responsibility;

    c. Codified Ethical Responsibility;

    d. Potential to Defend to the Opposing Party and/or Tribunal; AND

    e. Potential to Defend to the Public.

    The potential, is the ability of the authorizer to justify the activity to the designated party. Ultimately, you have to factor all of these and PRESS the potential liability. Then, you must weigh what benefit you get from authorization and what overall liability exists on the other side. Again, consider a) through e), press the liability together, then weigh what you get by authorization.

III. ACTIVITY BARRED BY CRIMINAL LAW.

A. Wiretapping – Both Federal and State statutes, including Iowa prohibit interception of a voice communication unless at least one party to the communication knows of and consents to the interception at the time of interception. 18 USCA 2510 et seq.; and Iowa Code Title XVI § 727.8. The acts, in essence, mirror each other. But, their interpretation and exceptions differ.

1. Electronic Communications Privacy Act of 1986 ("ECPA") – ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which was primarily designed to prevent unauthorized

government access to private electronic communications. It now protects wire, oral and electronic communications *while in transit* from interception by a third party.

The act, also known as the Federal Wiretap Act, prohibits the interception of oral or wire communication by use of any electronic, mechanical or other device. 18 U.S.C. § 2511.

a. Effect on State Law – Title I and II of the Electronic Communications Privacy Act ("ECPA"), preempts state law that provide less security for conversation. However, states can provide more protection by statute.

b. Two Party States – These "two-party consent" laws have been adopted in;

(1) California.

(2) Connecticut.

(3) Florida.

(4) Illinois.

(5) Maryland.

(6) Massachusetts.

(7) Montana.

(8) New Hampshire.

(9) Pennsylvania.

(10) Washington.

c. Complicated Two-Party States – Some states have complicated and ambiguous statutes that you should be aware of when investigating in those areas.

(1) Illinois – Illinois's two-party consent statute was held unconstitutional in 2014. *People v. Melongo*, 2014 IL 114852 (2014). It has now been revised and prohibits recording of a private conversation. 720 Illinois Compiled Statutes 5 / Criminal Code of 2012 Article 14.

(2) Hawai'i – In general a one-party state, but it requires two-party consent if the recording device is installed in a private place. Hawaii Revised Statutes Division 5. Crimes and Criminal Proceedings § 711-1111.

(3) Massachusetts – State bans "secret" recordings rather than requiring explicit consent from all parties. It falls in a two-party consent state. You should pay careful attention to this law as possession of a device with intent to record violates the statute. Mass. Gen. Laws Ch. 272, § 99.

(4) Washington – Statute implies a requirement to satisfy consent by a notice and announcement that is recorded indicating that all parties consent to recording. Wash. Rev. Code § 9.73.030.

(5) Montana – Statute has an announce provision which requires that you give warning. Mont. Code ann. § 45-8-213-1-c-i, ii, iii.

We will leave the Iowa Statute for later. It mimics the Federal statute and consent by one party protects you from ECPA and the Iowa Code:

d. ECPA Cross Border Issues – When recording is in Texas with a party in California, whose law applies? Generally, where the state with the most significant interest is at. If you are here, you are *probably* fine.

See Becker v. Computer Sciences Corp., 541 F.Supp. 694, 704-706 (S.D. Tex. 1982) (where former employee who surreptitiously recorded telephone conversations relied upon laws of Texas when he did so, and former employer was licensed to do business in Texas, conducted business in Texas and had registered agent in Texas, Texas rather than California had most significant interest in case, even though parties whose telephone conversations were recorded lived in California). Public policy interest. Not citied in 8th Circuit but, definitely good law. Should read the case. It is the number and quality of the contacts of each state to the case and to the interest that they are protecting.

e. Federal Exclusionary Rule – Strong exclusionary rule in federal statute for not allowing such evidence to be admitted in Court or any administrative action. 18 U.S.C.A. § 2515.

f. Criminal Penalty – The penalty for a violation of the statute is a fine or imprisonment for up to five years, or both.

g. Federal Civil Remedies – The Federal facts allow for actual and punitive damages for violation of the wiretap act. Although the statute allows minimal liquidated damages of $10,000 for violation of the Federal Act, Courts (majority) have found that that awarding damages is discretionary and the court may refuse to do so for *de minimus* violations. The federal wiretap act also includes a strong exclusionary rule. *Goodspeed v. Harmon*, 39 F.Supp. 2d 787, 791 (N.D. Tex. 1999).

h. Federal Interspousal Exception – The 5th Circuit has actually held a minority position to the Federal Wiretap Act that has said that Congress did not intend the act to regulate martial controversies or override state inter-spousal tort immunity. It has held that the recording of telephone conversations by one spouse against another is not what is meant to be covered by the *Federal* act. *Simpson v. Simpson*, 490 F.2d 803 (5th Cir. 1974). We are the *minority* rule. However, be advised that this exception is limited to eavesdropping by the *spouse* in the *marital home*. *Glazner v. Galzner*, 316 F.3d 1185 (11th Cir. 2002). That does not include anyone assisting them, such as a private investigator. However, beware, the spouse may still be liable under state law. *Heyman v. Heyman*, 548 F.Supp 1042 (N.D. Ill. 1982). Texas's state law clearly outlaws such activity and holds different than *Simpson*. *Collins v. Collins*, 904 S.W.2d 792 (Tex. App – Houston [1st Dist.] 1995, writ denied).

i. Federal Extension Phone Exception - Title I of the Federal Law contains a narrow held exception for eavesdropping over an extension phone that is done for the ordinary use of the subscriber. § 2510(5)(a)(i). Specifically, the statute prohibits nonconsensual interception using an electronic, mechanical or other device. What does that mean?

> "…"electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than--
>
> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the *subscriber or user in the ordinary course of its*

business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;…"

Mostly employer/employee cases. But, it is still very, very narrow and has been interpreted various ways. Not good law to rely on as if you lose, you violated federal law. They are going after the "party line." So, it becomes a great defense and not much of an offense tool.

(1) Cases:

(a) Wife cannot proceed with claim for relief from husband who wiretapped phone in marital home under 18 USCS § 2520, even though wife had filed for legal separation at time of wiretapping, where both parties resided in marital home and could have listened in on phone conversations by use of extension phones, because (1) 18 USCS § 2510(5)(a)(i) "extension phone" exception is expression of congressional intent to leave matters of interspousal domestic conflict to realm of state courts, and (2) there is no evidence that wiretap ever intercepted conversation in which wife participated. *Perfit v Perfit*, 693 F. Supp. 851(C.D. Cal., 1988).

(b) Where city employee was allegedly unaware that system for recording telephone calls to city continued to record statements through employee's headset after calls were terminated, exemption under 18 USCS § 2510(5)(a)(i) for interception using business device in ordinary course of business did not apply to interception of employee's private conversation with co-workers which was unrelated to city business. *Anderson v City of Columbus*, 374 F. Supp. 2d 1240 (M.D.Ga., 2005).

(c) Recording of all incoming and outgoing calls, including employee plaintiffs' conversations, by Dictaphone machine attached to telephone system of company providing central alarm services was in ordinary course of business under 18 USCS § 2510,

and alleged lack of notice was justified; recording is standard practice within central station alarm industry and is intended at least in part to deter criminal activity, was recommended by company's underwriters and relevant trade association, and may be required by authorities in certain instances. *Arias v Mutual Cent. Alarm Serv.*, 202 F3d 553 (2000).

(d) Corporation's use of voice logger, which recorded all telephone conversations on some telephone lines with extensions in security office, did not fall within business-use exception of 18 USCS § 2510(5)(a)(i), since voice logger is not telegraph instrument, equipment or facility, or component thereof, and was not used in ordinary course of its business, even though corporation claimed that it feared bomb threats. *Sanders v Robert Bosch Corp*., 38 F3d 736 (CA4 SC, 1994).

(2) Family Law – Some federal and state courts have interpreted that this exception allows for protection of a parent (even a non-custodial parent) to record his child while interacting with the other parent. *Schieb v. Grant*, 22 F.3d 149 (7th Cir. 1994). The underlying basis here is to not regulate the familial relations and not to subject to liability under a federal act. Now covered by vicarious consent.

j. Federal and State Vicarious Consent Exception – Although the above exception has roots in the statute, courts dealing with both the states and federal wiretap acts themselves have begun to hold that a parent may vicariously consent to record the conversations of their minor children. The federal courts have articulated a "good faith" test. Meaning that if the parent had a "good faith, reasonable basis for believing such consent was necessary for the welfare of the child," then the recording was allowed into evidence. The parent must demonstrate a reasonable belief "…that the minor child is being abused, threatened, or intimidated by the other parent. *Pollock v. Pollock*, 154 F.3d 601 (6th Cir. 1998).

Fairly recently, in *Alameda v. State*, the Texas Court of Criminal Appeals has upheld that where the parent has a good faith, objectively reasonable belief that the recording is necessary for the welfare of the child a vicarious consent exception to the Wiretap Act will make such recordings permissible. *Alameda v.* State, 235 SW 3d 218 (Tex. Ct. of Crim. App. 2007). Again, the age of the child and purpose for surveillance are factors in making this exception.

(1) Press Test – Be Careful here. This is close to a BIC test but not really. If you get it wrong, it could spell disaster for you, your client and their case. If you don't get vicarious consent, you are in violation of the law.

(2) Prior *Alameda* Cases: *Thompson v. Dulaney*, 838 F.Supp. 1535 (D. Utah 1993); *Wagner v. Wagner*, 64 F. Supp. 895, 896 (D. Minn. 1999); *March v. Levine*, 136 F. Supp. 2d 831, 849 (M.D. Tenn. 200 0), aff'd, 248 F.3d 462 (6th Cir. 2001); *Allen v. Mancini*, 170 S.W.3d 167 (Tex. App.–Eastland 2005, pet. denied); (As long as a parent has a good faith, objectively reasonable basis for believing that the taping of telephone conversations is in the best interest of the parent's minor child, the parent may vicariously consent to the recording on behalf of the child).

(3) Alien Mama - Wagner above adopts in the 8th circuit the vicarious consent doctrine. Wagner recorded conversations between his sons and wife who was alienating the children. The good faith basis was the interference with his relationship to his children. But, she did so on a fairly exceptional basis. *Wagner v. Wagner*, 64 F. Supp. 895, 896 (D. Minn. 1999).

(4) Bad Teacher – Iowa teacher calls underage student who is out for summer on phone repeatedly. Dad sees caller ID, overhears odd conversations, is called by mother of daughter's friend who expresses concern and finds out that they are going on a "lake trip" during summer. Dad then taps his home phone to record conversation between daughter and teacher. Teacher is arrested and moves to suppress recordings claiming that the recordings are illegal. No consent. Iowa supreme court upholds the Vicarious Consent Doctrine and applies it to the State of Iowa. *State v. Spencer*, 737 N.W.2d 124 (Iowa 2007).

(5) Discuss Wagner v. Spencer. Understand the difference in fact scenarios and why Wagner is a little riskier than Spencer if you are the investigator involved. Get your release and prove you good faith interest!!!

k. State Interspousal Exception – Some states, like Mississippi, have found that this exception exists. *Stewart v. Stewart*, 745 So. 2d 1319 (Miss. 1994). Texas, however, has made clear that Tex. Penal Code § 16.02(b)(1) does not include that. *Kent v. State*, 809 S.W.2d 664, 668 (Tex. App.-Amarillo 1991, pet. ref'd) (defendant violated code

by placing wiretap on the wife's telephone); *Duffy v. State*, 33 S.W.3d 17, 24 (Tex. App.-El Paso 2000, no pet.).

l. Reasonable Expectation of Privacy – A statutory claim and protection is somewhat predicated on the belief that one has a reasonable expectation of privacy that ought to be guarded. That is almost guaranteed when you are talking on a telephone that has 2 parties on it. Courts have generally held that one must have a objective and subject reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507 (1967). However, what happens when you are in public?

Test – In cases involving the reasonable expectation of privacy afforded to oral communications in the eavesdropping and wiretap contexts. Courts primarily look to considerations such as: (1) the volume of the communication or conversation; (2) the proximity or potential of other individuals to overhear the conversation; (3) the potential for communications to be reported; (4) the affirmative actions taken by the speakers to shield their privacy; (5) the need for technological enhancements to hear the communications; and (6) the place or location of the oral communications as it relates to the subjective expectations of the individuals who are communicating. These considerations help the court develop, but do not define, a set of nonexclusive factors to evaluate the subjective expectation of privacy in oral communications in publicly accessible spaces.

(1) Prayers – Grandmother and father of murdered children who brought suit under 18 USCS § 2511 because their private prayers and conversations were recorded at outdoor grave site memorial service by electronic surveillance microphone placed in funeral urn did not demonstrate that genuine issue of material fact existed as to their reasonable expectation of privacy in their oral communications, and thus court did not err in awarding summary judgment in favor of city, police officers and assistant district attorney; grandmother and father adduced no evidence regarding context of communications that they sought to characterize as private. *Kee v. City of Rowlett*, 247 F3d 206 (5th Cir. 2001).

(2) Earshot – Reporter records political meeting in hotel courtyard and records some voices with a hidden unenhanced audio hearing. Allows evidence to be heard that recording a private conversation in public could be an intrusion. Not a finding, just a reversal of summary judgment. *Stephens v. Dolcefino*, 126 S.W.3d 120 (Tex. App.—Houston [1st Dist.] 2003).

m. Video Surveillance Allowed – The ECPA does not prohibit silent video surveillance. So, if you aren't recording any sound, you are going to be ok. Disable the sound on your devices. At a minimum, use regular non-enhanced microphones. *Thompson v Johnson County Community College*, 930 F. Supp. 501(D.C. Kan. Cir., 1996).

B. State Wiretap Act; Iowa Code § 727.8; § 808B – Same as federal act. One party state that, without consent, if interception occurs it is unlawful. Consent can be both explicit and implicit. Iowa Code § 727.8 and Iowa Code § 808B which is the Interception of Communications Act.

1. Iowa Code § 727.8 – Any person, having no right or authority to do so, who taps into or connects a listening or recording device to any telephone or other communication wire, or who by any electronic or mechanical means listens to, records, or otherwise intercepts a conversation or communication of any kind, commits a serious misdemeanor; provided, that the sender or recipient of a message or one who is openly present and participating in or listening to a communication shall not be prohibited hereby from recording such message or communication; and further provided, that nothing herein shall restrict the use of any radio or television receiver to receive any communication transmitted by radio or wireless signal.

2. Iowa Code § 808B – Interception of Communications – You should print and know this statute. Remember § 808B.2(1)(b) – Prohibits you from referring or teaching your client how to do so. § 808B.2(1)(c) – Prohibits the disclosure or attempted disclosure of content that you know or have reason to know that was obtained illegally. Don't be clever. Strong exclusionary rule in § 808B.7. Civil damages allowed under § 808B.8. Also, pen registers and trap and trace devices must have warrants.

3. No Exceptions – No exceptions for spouses. You record your spouse with another, without authorization, then you are liable. Vicarious Consent is allowed. *Alameda v.* State, 235 SW 3d 218 (Tex. Ct. of Crim. App. 2007).

4. Finding the Tap – If you engage in a Technical Surveillance Countermeasure Sweep of a client's property and locate a wiretap what are your options? You may have to leave it there under this statute if it was placed by law enforcement. Also, remember that you may have a need to report that to law enforcement anyways (unless you are working under the supervision of an attorney).

> "(g) A person commits an offense if, knowing that a government attorney or an investigative or law enforcement officer has been authorized or has applied for authorization

to intercept wire, electronic, or oral communications, the person obstructs, impedes, prevents, gives notice to another of, or attempts to give notice to another of the interception."

Iowa Administrative Rules 661-121.5(6)(g).

"Be of good moral character. Consideration of whether an applicant is of good moral character includes but is not limited to…

Unless rendered confidential by law, the applicant's failing to report: (1) A serious crime, or (2) The location of any stolen property;"

Iowa Code § 719.1 Interference with official acts.

"A person who knowingly resists or obstructs anyone known by the person to be a peace officer… whether paid or volunteer, in the performance of any act which is within the scope of the lawful duty or authority of that officer…commits a simple misdemeanor."

5. Sample Cases

a. Hit Man Blues – In a trial for solicitation to commit murder, defendant was not entitled to suppress an audio taped conversation with an investigator posing as a hit man; the court rejected defendant's wire-tapping arguments, finding that no application was required for an order to record defendant's conversation with the investigator because the investigator consented to the recording. *Casey v. State*, 2006 Tex. App. LEXIS 1266 (Tex. App.-Houston [14th Dist.], Feb. 14, 2006).

b. Consent Given - Where police had permission of a participant in a telephone conversation to record the conversation, record of the conversation was legal, and the recording was admissible at defendant's trial on charges of conspiracy to commit capital murder. *Matthews v. State*, 1998 Tex. App. LEXIS 4556 (Tex. App.-Dallas, July 28, 1998). Iowa Case *See Archer v. State*, No. 3-741 / 12-0995 (Iowa App., 2013). Where police took time to convince a child and mother to provide consent even thought she waivered on whether she wanted to. Why would we want that documented?

c. Jail Birds – Telephone calls that defendant made from jail were not illegally intercepted under Tex. Penal Code Ann. § 16.02(c)(3)(A) because a technical administrator with the contracting company that

operated the inmate phone system testified that a prompt notified inmates at the beginning of each phone call that their calls were monitored or recorded. *Escalona v. State*, 2014 Tex. App. LEXIS 2008 (Tex. App. Dallas Feb. 20 2014, no pet. h.). For Iowa *See State v. Mummau*, 834 N.W.2d 871 (Iowa App., 2013)

d. Vicarious Consent – In a sexual assault on a child case, because a court correctly determined that a mother had a good faith, objectively reasonable belief that recording her child's telephone conversations was in the child's best interest, the court did not err in allowing the audiotapes to be admitted over defendant's objection that the child had not consented. *Alameda v. State*, 181 S.W.3d 772, 2005 Tex. App. LEXIS 9829 (Tex. App. Fort Worth 2005).

e. Minors can Say Yes – In claiming that the recorded conversation between defendant and the victim was illegally obtained and therefore inadmissible under Tex. Code Crim. Proc. Ann. art. 38.23(a), defendant did not point to and the court is not aware of any authority that specifically holds that a minor cannot consent to the recording of his or her own conversations for purposes of Tex. Penal Code Ann. § 16.02(c)(4); the error, if any, in admitting the recording was harmless under Tex. R. App. P. 44.2 because the information on the recording was cumulative of other testimony. *Robertson v. State*, 2010 Tex. App. LEXIS 969 (Tex. App.-Corpus Christi, Feb. 11, 2010).

Iowa Cases:

f. Crabby Clerk – Longtime serving court clerk in Franklin County was in years long running disputes with coworkers. Coworkers complain of her being unfriendly with customers and others. As part of that dispute the clerk records conversations with her coworkers. At least twice she leaves the recorder running when she leaves her desk for other meetings. Clerks report it to a Judge who hears a recording of third party juvenile probation officers. State prosecutes. D claims several appellate issues: (1.) The tape was lost prior to trial and D claimed no proof of recording was entered into trial. Court rejects that argument. Circumstantial evidence exists. (2.) D claims that the phrase "having no right or authority to do so" is vague. Court finds they are not vague as to her situation. *State v. Philpott*, 702 N.W.2d 500 (Iowa, 2005).

h. Executive Override – Iowa DHS consolidated its offices and bought a new phone system. That system included the ability to use an "Executive Override" feature that allowed for listening in on various extensions. Manger utilized the system to listen into the recordings

of various employees for disciplinary purposes. She then made recordings of these various employees to make a report to supervisors. Supervisor finds this out and conducts an immediate investigation and then turns it over to police who file a criminal complaint against her under Iowa Code § 727.8. She pleads guilty to a deferred judgment. This specific appellate case has more to do with her employment discipline than for our purposes. But, a great common fact pattern. *Hall v. Iowa Merit Employment Commission*, 380 N.W.2d 710 (Iowa, 1986).

i. Borrow my Phone – Suspect of theft case uses telephone of the police desk sergeant to call his collaborator and get there stories straight. Unbeknownst to him, the telephone is always recorded. State puts the evidence into trial. However, Defendant's lawyer fails to object. Recording can't be appealed for failure to preserve error. However, likely a violation of the wiretap act. *State v. Lee*, 7-461/06-0573 (Iowa App., 2007).

4. Civil Remedies; Iowa Code § 808B.8 – Allows for liability for improper interception by use of a mechanical, electrical or other device. Allows for recovery of injunction, actual damages, punitive damages and reasonable attorney's fees.

a. Baby Mamma – Papillion and Jones lived together and had two children. Man owned the residence, phone line and telephones. Man began recording conversation every time he left the residence. Uses recordings to threaten custody suit. Jones brings suit against children's father for violation of wiretap act and is awarded damages. Court upholds verdict allows the use of the recording as a basis. Also allows for punitive damages. Same recording rules in Federal statute. Exact same. *Pappilion v. Jones*, 892 N.W.2d 763 (Iowa 2017).

C. Federal Stored Communications Act ("SCA") – Federal law that protects against unauthorized "access" to electronic communication while it is in "electronic storage." These quotes are oddly defined and really deal with transmission interception. Basically, the courts have struggled to define "temporary, intermediate storage" in the context of how data is stored and transmitted over the internet. They are clear on prohibiting interception during transmission. (Think FBI Carnivore Program).

1. Primary Purpose – Protect privacy interest of personal information that is stored on the internet and to limit the government's ability to compel disclosure of information that is held by third parties.

2. Electronic Storage – Oddly defined and depends what court is looking at it. It can depend on whether it is stored on a local drive (like your home computer) or a remote server. The Stored Communications Act is not violated when someone access mails that are stored locally on a computer, but it can be a violation to access webmail that is stored on the internet. There is some disagreement about whether e-mail that is intercepted after it has been received and read is in "temporary, intermediate storage," "backup storage," or "post-transmission storage." The first two categories would be protected under the Stored Communications Act, while the third would not. Most likely, email stored on a local personal computer, post-transmission, does not violate the SCA.

    a. Hard Drive – Some courts have held that computer files that are stored in a hard drive in post transmission storage on your computer are not the same thing as electronic storage. Thus these are free to access: *Fraser v. Nationwide Mut. Ins. Co*., 352 F.3d 107, 114 (3d Cir.2003) F. Supp2d 623 (E.D. Pa. 2001); *White v. White*, 781 A.2d 85 (N.J. Super Ct. CH Div. 2001).

    b. Server Storage – However, sometimes, post transmission storage on a third party server has been found to be protected by the SCA. *See Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp.2d 914 (W. D. Wis. 2002).

3. Social Media – We'll discuss below but it is still an unsettled question to some degree. Recently, a California federal court held that Facebook and MySpace were protected under the Stored Communications Act. *Crispin v. Christian Audigier, Inc., et al*, CV 09-09509-MMM-JEMx C.D. Cal.) (May 26, 2010).

4. ECPA v. SCA – ECPA really deal with communications in transit while the SCA concerns stored communications.

D. State Stored Communications Act – States that have one mirrors almost identically the Federal Statute. Does anyone know if Iowa has one other than: Iowa Code 716.6B Unauthorized Computer Access?

1. Practical Advice – The SCA has a potential to be turned over because it lags behind the times. When dealing with computers, it is always best to get the court order authorizing analysis. It can be sometimes better to have just the image of the hard drive in storage awaiting possible examination. Many times this tactic becomes more of a stick used for settlement than the evidence itself.

E. Voice Mails – USA Patriot Act amended the Stored Communications Act (both federal law) which now treats voicemails similar to email communication under the SCA. Courts had found in the past that retrieving stored voicemails messages violated the Federal Wiretap Act. *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998). Since that courts have now interpreted that it is not a violation to obtain answering machine messages located on a physical recorder, but it is a violation to access voicemail messages stored on a telecommunications system. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874-880 (9th Cir. 2002).

F. Breach of Computer Security – Iowa Code 716.6B Unauthorized Computer Access makes it a crime to access someone's computer without their consent. Aggravated Misdemeanor at most. Also see Iowa Code 715 Computer Spyware and Malware Protection.

1. Criminal Cases – Mainly deal with suppression of the illegally obtain evidence in a criminal case. More specifically, child pornography cases. Why is it that these cases are here? Why is it that there are no hacking cases here? What is the push? Are we weakening the statute? What do we want as investigators?

a. Computer Repairman – Defendant authorized file access to a repair person, who consented to police viewing several of the files at issue, and that the police reasonably believed the repair person had authority; accessing the files did not violate statute because the computer files were accessed in the course of carrying out defendant's repair order and in the ordinary course of the repair company's standard procedures. *Signorelli v. State*, No. 09-06-450-CR, 2008 Tex. App. LEXIS 335 (App.—Beaumont 2008)

b. Computer Tech - Defendant worked in a computer store as a repair technician. He and the other technicians had been instructed never to leave their computers unsecured, and that if they saw a coworker's computer unsecured, they should change a setting to alert the coworker that it had been left unsecured. Defendant brought his personal computer to use at work and left it unsecured. A coworker accessed it to change the background and found child pornography. Court found consent. *Knepp v. State*, No. 05-08-00002-CR, 2009 Tex. App. LEXIS 1765 (App.—Dallas 2009).

c) Sweetheart Email – Because defendant gave his girlfriend access to his email accounts in exchange for her agreement to continue their relationship and because he claimed he had nothing to hide, defendant effectively consented to her access to his accounts, despite his contention that she was only allowed to look at them if he was sitting next to her. Court found consent and no violation of

the statute. *Dipple v. State*, No. 05-12-00114-CR, 2013 Tex. App. LEXIS 273 (App.—Dallas 2013).

2. Civil Liability – You too can be sued for this through its corresponding civil mechanism. See below cases who provide recovery if you violate the first statute.

   a) Website Limited Use – Travel website used a program to obtain fares and other information automatically from American Airlines. American claimed that you can't use that for that purpose. Only for the terms and conditions which they made available. Found violation of the act. *Travel Jungle v. Am. Airlines, Inc.*, 212 S.W.3d 841 (Tex. App.—Fort Worth 2006).

   b) Screen Shots is Accessing – Suit between two former spouses involved in business together. Husband takes screen shots of text messages and phone call logs while wife is sleeping. Court finds that this is a violation of the statute because the phone is a computer under the statute, wife has greater ownership claim on the phone than husband; and that taking a screen shot is accessing under the statute. *Miller v. Talley Dunn Gallery, LLC*, No. 05-15-00444-CV, 2016 Tex. App. LEXIS 2280 (App.—Dallas 2016).

   c) Don't Download at Office – Court held that downloading without consent, even if you are an employee or contractor, from employer's computer systems can be considered a violation of the penal code and actionable under civil practices and remedies code. *Institutional Secs. Corp. v. Hood*, 390 S.W.3d 680 (Tex. App.—Dallas 2012).

G. Online Impersonation – Texas was one of the first states to implement a law prohibiting online impersonation. Makes it impossible to impersonate a witness, subject or other without real problems. Not one in Iowa that I am aware of. But see, Iowa Code 80.6 – Impersonating peace officer or employee.

H. Stalking – Iowa Code § 708.11. This statute is difficult to read. But, I have selected parts so that you can get an idea how the statute works against you:

   1. Statute.

      a. "The person purposefully engages in a *course of conduct* directed at a specific person that would cause a reasonable person to feel terrorized, frightened, intimidated, or threatened or to fear that the person intends to cause bodily injury to, or the death of, that specific person or a member of the specific person's immediate family."

b. Course of Conduct - "repeatedly maintaining a visual or physical proximity to a person without legitimate purpose, repeatedly utilizing a technological device to locate, listen to, or watch a person without legitimate purpose…"

c. Stalking with a weapon = Class D Felony!

2. Defenses – Surveillance is not stalking based on reasonable person's belief. But, you can stalk as an investigator. You can be subject to the statute. Poorly written statute. A good and used argument is that the state provides you a license to include surveillance and if you are granted a license how can you be prosecuted? How is this comparable to a driver's license?

3. True Love – Tyreman and wife file for divorce. During this time, he makes numerous suicide and death threats. Called impersonated a police officer, surveilled her and told others he "knew" what she was up to, threatened family members, broke into her vehicle and put a tracker in her car. Court upheld the conviction and allowed past evidence and prior bad acts into evidence. Prior to the recently passed tracking device. *State v. Tyerman*, No. 9-909/09-0113 (Iowa App., 2010).

I. Unlawful Installation of a Tracking Device – Iowa Code § 708.11A – A person commits unauthorized placement of a global positioning device when the person, without the consent of the other person, places a global positioning device on the other person or an object in order to track the movements of the other person without a legitimate purpose.

1. 2017 Statute – Any word? No Reported Cases. No exceptions for lease cars? Legitimate Purpose? What about tracking your car that wife is driving? What about tracking your car for employment? What about keeping tabs on your vehicle not the individual? Can this be defended?

2. 4th Amendment Search Issues – *US v. Jones*, 132 S. Ct. 945 (2012) (holding that the attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment). This case was decided on grounds of trespass. However, the court did not necessarily throw out the expectation of privacy test. This case may be more of an example of how the Supremes are protecting the vehicle than anything else. So, maybe they have to have the warrant now. Not the case in past criminal law where a bumper beeper was not an unreasonable search and seizure.

J. Restrictions on the Use of Pen Register or Trap and Trace Device; Iowa Code 808B.10 – A person shall install or use a pen register or trap and trace device without first obtaining a search warrant or court order. Some telco exceptions.

K. Illegal Use of Drones; - Several states have passed a law that makes it an offense if the person uses an unmanned aircraft to capture an image of an individual or privately-owned real property in this state with the intent to conduct surveillance on the individual or property captured in the image. See Drone section below. Iowa has two laws that are interesting

Iowa Code 808.15 Unmanned aerial vehicle — information — admissibility.

"Information obtained as a result of the use of an unmanned aerial vehicle is not admissible as evidence in a criminal or civil proceeding, unless the information is obtained pursuant to the authority of a search warrant, or unless the information is otherwise obtained in a manner that is consistent with state and federal law."

Iowa Code 321.492B Use of unmanned aerial vehicle for traffic law enforcement prohibited.

"The state or a political subdivision of the state shall not use an unmanned aerial vehicle for traffic law enforcement."

Also, DPS is supposed to draft guidelines. Not sure this has been done, but if the do, the Feds are deferring to them.

L. Harassment and Revenge Porn; Iowa Code § 708.7 Harassment – Revenge porn bill that makes it a crime to record, promote and distribute intimate visual material. Makes it a crime to:

"Disseminates, publishes, distributes, posts, or causes to be disseminated, published, distributed, or posted a photograph or film showing another person in a state of full or partial nudity or engaged in a sex act, knowing that the other person has not consented to the dissemination, publication, distribution, or posting…

The following do not constitute harassment under subsection 1, paragraph "a", subparagraph (5):
a. A photograph or film involving voluntary exposure by a person in public or commercial settings.
b. Disclosures made in the public interest, including but not limited to the reporting of unlawful conduct, disclosures by law enforcement, news reporting, legal proceeding disclosures, or medical treatment disclosures.
c. Disclosures by an interactive computer service of information provided by another information content provider, as those terms are defined in 47 U.S.C. §230."

M. Invasion of Privacy - Nudity Iowa Code 709.21 – Makes it an offense to photograph or videotape without the other person's consent AND with intent to arouse or gratify the sexual desire of any person. Peeping tom law and law for camera in the bedroom by snooping spouse. What you want to use when you find the camera.

N. Criminal Trespass; Iowa Code § 716.7 – A person commits an offense if the person enters on or remains on the property of another…without effective consent and the person: had intent to commit a public offense; or received notice to depart but failed to do so and others. Usually, have to have a warning.

O. Criminal Mischief; Iowa Code § 716.1– You have to tamper or interfere with use. Generally, you aren't doing that.

X. ACTIVITY BARRED BY CIVIL REMEDIES.

A. Right to Privacy

1. U. S. Constitution – The U. S. Constitution has never truly held that there is a definable right to privacy within the text of the constitution or any of its amendments. A number of discussions, heralding back to the late 1890s, began to lay the foundation of general privacy protections. Harvard Law Review, Volume VI, 12-15-1890, No. 5. However, the Supremes have held through a mishmash of cases and a general interpretation of cases that privacy exists in the 1st Amendment (privacy of beliefs); 3rd Amendment (privacy of the home against use by soldiers); 4th Amendment (privacy of the person and possessions against unreasonable searches); and the 5th Amendment Self-Incrimination Privilege (which provides protection for the privacy of personal information). It thus has become, in both the text of the constitution and through application, a basic fundamental right.

See Meyer v. Nebraska (right to attend parochial schools)*; Griswald v. Connecticut* (right to buy contraceptives); *Stanley v. Georgia* (right to view porno in home); *Roe v. Wade* (woman's right to abortion); *Lawrence v. Texas* (sodomy not illegal). All of which is applied to the states by the 14th amendment. Very broad and abstract policy.

a. Protection Against Government – Most of the above cases are restrictions upon state actors. Remember, the Bill of Rights protects you from unwanted government intrusion. You are a private citizen and are not subject, necessarily, to the same restrictions that police have under those bill of rights. However, you will be *measured* by them. Especially by fourth amendment search and seizure law meant to reign in police. Therefore, be aware of the cases that follow. Some are civil and some are criminal defendants. Many times these are simply deciphered by *State v. Smith* as opposed to *Adams v. Smith*. Remember they are only binding on the government's actions.

b. Fletch's Warehouse – In an injury case, plaintiff and a private investigator, entered a warehouse which was occupied jointly by defendants for the purpose of obtaining evidence relating to this case. While there is some question as to just how they gained admittance to the warehouse, no permission had been obtained from defendants to make an inspection of the scaffolding and the scaffold board. Court held that Fourth Amendment protection against illegal searches and seizures applies to state action by way of the Fourteenth Amendment, and there is no constitutional prohibition against private actions which, if instituted under color of state law, would be prohibited. The question falls within the category of legislative rather than judicial action, and even if defendant had the proper standing to assert such extension of the exclusionary rule we would decline to entertain the question. *Moose v. Rich*, 253 N.W.2d 565 (Iowa, 1977).

2. State Constitution - In addition, most, if not all, state supreme courts have held that privacy, although not explicitly spelled out in the state constitution, mimics the US Constitution and creates various zones of privacy that are protected. These include protection against arbitrary deprivation of life and liberty; the freedom to speak, write or publish; protection of not being compelled to give evidence against oneself; protection of the sanctity of one's home from unreasonable intrusion and right of conscience in religious matters. *Texas State Employees Union, et al v. Texas Department of Mental Health and Mental Retardation, et al*, 746 S.W.2d 203 (Tex. 1987).

3. Common Law Right to Privacy – In addition to constitutional protections, American courts have generally recognized a cause of action broadly titled invasion of privacy when one interferes with another's seclusion of solitude. These civil matters result in money damages. They may not necessarily result in excluding evidence in another trial.

B. Invasion of Privacy – As we discussed above, this fundamental right to privacy is protected through a common law cause of action of Invasion of Privacy. Such a clam should not be lightly taken. Its violation can cause all sorts of fury to rain down on you by a judge or jury should you run afoul of it. Traditionally, there are four distinct torts that one can sue under. They are;

1. unreasonable intrusion upon the seclusion or private affairs of another (AKA, Intrusion Upon Seclusion);

2. unreasonable publicity given to an aspect of one's private life in which the public has no legitimate concern (AKA, Public Disclosure of Private Facts);

3. publicity that unreasonably places another in a false light before the public (AKA, False Light);

4. unwarranted appropriation of one's name or likeness (AKA, misappropriation of name and likeness).

Courts have expressly allowed for intrusion upon seclusion and for public disclosure of private facts. Those causes of invasion of privacy are critical to understand. Several states have explicitly rejected False Light because it essentially is covered by defamation which has a number of substantive and procedural limitations. Texas has likely provided some support for misappropriation of name or likeness. *See Cain v. Hearst Corp*., 878 S.W.2d 577 (Tex. 1994). For our discussions, we will concentrate only on the first two; intrusion on seclusion and public disclosure of private facts.

C. Intrusion on Seclusion – This is what you will be sued upon. Simply put this is the suit that will result for overreaching and over-snooping. The elements for this private cause of actions are:

1. the defendant (investigator) intruded on the plaintiff's solitude, seclusion, or private affairs;

2. the intrusion would be highly offensive to a reasonable person; AND

3. the plaintiff suffered some injury as a result.

See Valenzuela v. Aquino, 853 S.W.2d 512, 513 (Tex. 1993); *Billings v. Atkinson*,489 S.W.2d 858, 859 (Tex. 1973); Restatement (Second) of Torts § 652B. A good discussion of these elements can be found in Restatement (Second) of Torts § 652B and Dorseano's Texas Litigation Guide § 335.03.

a. Intrusion – A showing of conduct in the nature of an intrusion is necessary to establish a cause. The invasion may take the form of actual physical intrusion into a place or it may be by senses (sight, hearing) with or without the aid of mechanical devices. Thus, entering a person's home, hotel room, or hospital room without consent, tapping another person's telephone, or placing another person under surveillance or photographing his or her movements would equal an intrusion. Intrusion may take the form of an investigation or examination into a person's private life, such as by opening personal mail, searching a private room, or examining his or her personal bank records. Restatement (Second) of Torts § 652B, Comment b; Prosser and Keeton on Torts, § 117 (5th ed. 1984).

The intrusion must usually be private. Although an individual is not protected from being observed or photographed in a public place, a person is protected when at home or in the hospital. Similarly, a plaintiff has no cause of action for the inspection of records that are generally considered public record. However, a plaintiff is protected against illegal search and seizure. Thus, the importance of 4th amendment cases. *Id.*

b. Highly Offensive – Must be highly objectionable to a reasonable person. This is the fuzzy element. Usually meant to create a sense of shock. You can have an intrusion which may not necessarily be offensive. This is why these cases are very hard to quantify. There is always a lot of argument here.

c. Damages – You must sustain some damages. These damages can include mental anguish, compensatory, exemplary, loss of earning capacity, injunction, pre and post judgment interest, court costs and attorney's fees.

D. Case Law - These cases include such thing as setting up a video camera in the plaintiff's bedroom without permission; entering the plaintiffs home without permission; entering plaintiff's private office without permission; following, spying on and harassing the plaintiff; making harassing phone calls at unreasonable hours; searching an employee's locker and purse; and, wiretapping.

Specifically, look at these cases, almost all have a subject and objective test for an expectation of privacy;

1. Defendant in Public – Defendant wants to challenge video evidence of him in public. Claims they need a warrant and then claims that they are liable for invasion of privacy. Surveillance video taken of a criminal defendant in public is not an intrusion as he has no seclusion or expectation of privacy. No need for warrant as it is not a search and seizure. *McCray v. State of Maryland*, 581 A.2d 45 (Md. Ct. Spec. App 1990) (video captured images of someone in a private place with reasonable expectation of privacy has invasion of privacy claims).

2. Binoculars and Open Window – During neighbor dispute, neighbor parked in opposing driveway and used binoculars to look into kitchen at plaintiff resident. Court held that one cannot expect to be entitled to seclusion when standing directly in front of a large window with the blinds open or while outside. *Vaughn v. Drennon*, 202 S.W.3d 308 (Tex. App.–Tyler 2006, no pet.).

3. Bedroom Cameras – Wife hired a private investigator to investigate her husband's infidelities. As part of the investigation, private investigator installs a hidden camera in the shared bedroom of the couple. While wife goes out of state, investigator monitors and records husband's sexual encounter with his girlfriend in the marital bedroom. Court upholds invasion of privacy suit against investigator. Even though the investigator may have only furnished technical services in connection with acts constituting invasion of privacy, the private investigator may still be liable as if an actual invasion of privacy has been committed. A spouse by virtue of marriage relinquishes some of his privacy but, not all and not when recording happens without consent and no expectation is had. *Clayton v. Richards*, 47 S.W.3d 149 (Tex. App.–Texarkana 2001, pet. denied).

4. Iowa Bedroom Camera – Husband placed recording cameras in the bedroom of his wife when the two of them shared the marital residence with their children. Husband placed hidden cameras in alarm clock, ceiling and a motion activated camera through a drilled out hold in the bed frame. Iowa court held that court judgement was upheld because a spouse shares equal rights in the privacy of the bedroom. Even thought it was his residence, her privacy. Quotes *White* and *Clayton* above. *In re Marriage of Tigges*, No. 7-922/07-1103 (Iowa App. 5/14/2008) (Iowa App., 2008).

4. Phone Company – Husband and wife separated with wife living in a separate apartment. She installs a land line on her own. Husband then has phone company install an extension to his location to listen in. Court holds both husband and phone company liable for an intrusion. *Lecrone v. Tel. Co.*, 201 N.E.2d 533 (Ohio Ct. App. 1963).

5. Fatal Attraction – Husband, while married, breaks up with his girlfriend after brief extra-marital affair. Girlfriend then followed husband several days a week for several years at his office, home, family vacations, children's schools, dinners with his wife and other outings. She sent him unwanted cards, gifts, and letters. She was overheard making vulgar sexual remarks by his wife, kids and neighbors. Court upholds verdict for invasion of privacy awarding a $40,000 award for Husband. *Kramer v. Downey*, 680 S.W.2d 524 (Tex. App.—Dallas 1984)

6. Peeking over the Fence – Phone company built a cell tower twenty feet from the property line of the plaintiff. During construction, maintenance and work men looked over their 6-foot fence. Court held that evidence didn't justify finding of invasion of privacy. The fact that maintenance workers come to an adjoining property as part of their work and look over into the adjoining yard is legally insufficient evidence of highly offensive conduct. There was no evidence of how often these workers looked, how long, what or who they spied, or even what the plaintiffs were doing when the peering

happening. *GTE Mobilnet of S. Tex. Ltd. P'ship v. Pascouet*, 61 S.W.3d 599 (Tex. App.—Houston [14th Dist.] 2001).

7. Official Photos – Plaintiff went to police to report an assault. Officers told her that they needed her to undress to photo bruises. Over her objections, they ordered her to do so. After taking photos, two other officers reproduced and disseminated the photos through the department. Court found officers conduct was highly objectionable intrusion. *York v. Story*, 324 F.2d 450 (9th Cir. 1963).

8. Aggressive Phone Calls – Plaintiff sued phone debt collector and collections agency for multiple harassing phone calls at home and work. Calls were multiple times of day, early morning and late evening. Harassing telephone calls were found to be overt, unlawful acts which intrude upon a person's seclusion or solitude and, therefore, invade privacy. Court upheld judgement against defendant collection company. *Household Credit Servs., Inc. v. Driscol,* 989 S.W.2d 72 (Tex. App.—El Paso 1998).

9. Videotaping Neighbors, Part II – Landowners sue neighbors for invasion of privacy for videotaping into their kitchen windows. The kitchen window faced the backyard, not a public street, and there was a six-foot-tall privacy fence separating the parties' properties. Taping occurred early one Saturday morning for only 10 second intervals while plaintiff was in kitchen eight months pregnant and wearing only her pajamas. Property was only 10-15 feet from each other. Defendant was trying to document out of control dog as instructed by animal control. Court held that videotaping the landowners' house from their property, over the fence, constituted an actionable invasion of privacy. Court held that when the window of a home is not observable by the alleged intruder in the normal course of non-intrusive activities. You cannot say as a matter of law that a plaintiff has no reasonable expectation of privacy merely because her window blinds are open. *Baugh v. Fleming*, No. 03-08-00321-CV, 2009 Tex. App. LEXIS 9847 (Tex. App.—Austin 2009).

10. Unauthorized Entry into Home – Court held that there was an intrusion when service man walked in and removed telephones from residence without authorization and without anyone being home. *Gonzales v. Southwestern Bell Tel. Co*., 555 S.W2d 219 (Tex. App.–Corpus Christi 1977, no writ).

11. AOL Emails OK – Wife hired PI to go through a family computer located in the family sun room. Wife had recently found a written letter in the room to husband's girlfriend. PI copied hard drive and located incriminating emails of affair which were saved on the local machine and were not password protected. Court held that accessing stored email does not constitute a violation of the common law privacy intrusion tort and that

email in a home computer that both spouses had access to had no reasonable expectation of privacy. No different than flipping through a file cabinet. *White v. White,* 344 N.J. Super. 211, 781 A.2d 85 (N.J. Super Ct. App Div. 2001).

12. Employee Locker – Plaintiff worked at K-Mart who gave employee a locker and sold her a lock to lock it. Employee puts her purse in locker and locks it. Comes back to find locker open and purse rifled through. Employer had received tip regarding stolen property. Court said it was reasonable that constituted an intrusion. However, a unlocked locker might not be found to be an intrusion. *K-Mart Corp. v. Trotti*, 677 S.W. 2d 632, 637 (Tex. App. –Houston [1st Dist.] 1984), writ ref'd n.r.e..; 686 S.W2d 593 (Tex.1985).

13. Shared File Cabinets – Divorce action in which husband sought to suppress evidence of his extramarital affair that his wife found "in one of the office file cabinets in a room to which plaintiff [wife] had complete access." The papers, consisting of love letters sent to the defendant by his paramour and a jewelry receipt for jewelry not given to his wife, had been left "in files t o which she had a full freedom of entry." Court held that no intrusion held. *Del Presto v. Del Presto*, 97 N.J.Super. 446, 235 A.2d 240 (App. Div. 1967).

14. Employee Injury – Supervisor insisted on going with employee to emergency room have incident to make sure his arm was not broken. Employee sued claiming invasion of privacy. However, court held nothing private was discussed. Just an x-ray of the arm. *Morrison v. Weyerhaeuser Co.*, 119 F. App'x 581 (5th Cir. 2004).

15. No Wiretapping – Husband wiretapped telephones of wife's attorney with help of another and then attempted to hide conduct. Court found intrusion and upheld a $1,000,000 award in punitive damages. *Parker v. Parker*, 897 S.W.2d 918, 930 (Tex. App.- Fort Worth 1995, writ denied).

16. Discarded Garbage – Citing *California v. Greenwood*, these courts held that the Fourth Amendment right to be free in reasonable searches and seizures does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of the home. "Curtilage" is the area to which extends the intimate activity associated with the sanctity of a man's home in the privacies of life. Courts concluded that garbage discarded outside the curtilage of the residence had no reasonable expectation of privacy. Thus there can be in intrusion. *California v. Greenwood*, 486 U.S. 35 (1988); *Smith v. Maryland*, 442 U.S. 785 (1979); *United States v. Kramer*, 711 F.2d 789 (7th Cir. 1983); *Nilson v. State of Texas*, 106 S.W.3d 869 (Tex. pp.– Dallas 2003).

17. Office Trash – Commercial dispute where letter was retrieved after it was thrown away by plaintiff into office waste basket, then collected by the maintenance and stored in a community waste area that was locked. No intrusion in an area (community waste area) where she had no expectation of privacy. Area was not in curtilage of her seclusion of office. Can't expect that giving your documents to third party (maintenance man) will protect your privacy. *Danai v. Canal Square Associates,* 862 A.2d 395 (D.C. 2004).

18. Reporter's Recording – Reporter records political meeting in hotel courtyard and records some voices with a hidden unenhanced audio hearing. Allows evidence to be heard that recording a private conversation in public could be an intrusion. Not a finding, just a reversal of summary judgment. *Stephens v. Dolcefino*, 126 S.W.3d 120 (Tex. App.—Houston [1st Dist.] 2003).

19. Martial Problems – Husband wiretaps wife while together. Records conversations with attorney and others. Court allows claim to proceed under both Iowa Code § 808B and under Invasion of Privacy. *Luken v. Edwards*, No. C10-4097-MWB (N.D. Iowa, 2011).

20. Employee Bathroom – 2 female employees were the only employees of an insurance agent. A small (4' × 7') bathroom with a sink and toilet is located in the office. 1 of the females discovered a digital surveillance camera hidden inside the office bathroom. The camera was positioned to view the toilet and surrounding area. When confronted by police, defendant admitted he had placed it in the bathroom and stated he did so because he suspected one of his employees was abusing drugs while at work and was concerned she would embezzle money. However, no recordings were found and the system did not work. Defendant claims that it was for non-invasive purpose and it didn't work at any rate. Court throws out both. *Koeppel v. Speirs*, No. 9-902/08-1927 (Iowa App., 2010).

21. Peeping Tom Lawyer – Lawyer becomes infatuated with 24-year-old girl and begins to look through her windows at various times from outside of the residence. Girl and roommate eventually catch lawyer using a game camera. Attorney is charged with a misdemeanor peeping tom. Girls file a disciplinary action against him under committing a criminal act against trustworthiness. License suspended. *Iowa Supreme Court Attorney Disciplinary Bd. v. Templeton*, 784 N.W.2d 761 (Iowa, 2010).

22. Dinner Time? – News reporter takes video of women at dinner for news story. Woman ask to stop the video while in the dining room of the restaurant. Reporter refuses and uses the footage. She sues. Court does not dismiss her claim outright. Court claims that can't do so without some facts. Could be that the diner was in a private dining room. *See also* Jackson v. Playboy Enters., Inc., 574 F.Supp. 10, 13-14 (S.D.Ohio 1983) (publication

of photograph of plaintiffs on a city sidewalk); Neff v. Time, Inc., 406 F.Supp. 858, 861 (W.D.Pa.1976) (publication of photograph of plaintiff at football stadium); Jaubert v. Crowley Post-Signal, Inc., 375 So.2d 1386, 1387 (La.1979) (publication of photograph of resident taken from middle of street); Cefalu v. Globe Newspaper Co., 8 Mass.App.Ct. 71, 77, 391 N.E.2d 935, 939 (1979) (publication of photograph of plaintiff while he was in unemployment line), cert. denied, 444 U.S. 1060, 100 S.Ct. 994, 62 L.Ed.2d 738 (1980).

E. Public Disclosure of Private Facts – The elements for this private cause of action includes;

1. the defendant publicized information about the plaintiff's private life;

2. the publicity would be offensive to a reasonable person;

3. the matter publicized is not of legitimate public concern; and,

4. the plaintiff suffered an injury as a result of the defendant's disclosure.

Cases - The following cases give you an idea of how this action works. It does require a publication of the information. Meaning the communication must be one that is made to the public at large, or disseminated to so many persons that the matter becomes public knowledge. *Industrial Foundation of the South v. Texas Indus. Acc. Bd.*, 540 S.W.2d 668, 683, 684 (Tex. 1976), cert. denied, 430 U.S. 931 (1977). Most of the cases protect you as an investigator.

1. Bad Press – Decedent killed himself shortly after an article was run by newspaper owner and column author, which indicated that decedent was arrested for indecent exposure in a public park during a police crackdown on homosexual activities in public places. Court held that there was no liability for disclosing fact that are a matter of public record. *Hogan v. Hearst Corp.*, 945 S.W.2d 246, 250–251 (Tex. App.—San Antonio 1997, no writ).

2. Court Information – Sexual orientation and HIV-positive status of a police officer that was disclosed in a court hearing in which the officer's ex-wife claimed that their child would not be safe in the officer's custody was held to be of legitimate public concern. *Crumrine v. Harte-Hanks Television, Inc.*, 37 S.W.3d 124, 127 (Tex. App.—San Antonio 2001, pet. denied).

So if you have to disclose to anyone outside of your client and publish to a number of individuals, then do so by disclosure in court first. Think press test on this also. Always think about your disclosure of findings. Only to your client and more

importantly to your client's legal representative. Any time you release a report or information it has repercussions. Control the disclosure.

G. Defamation – A common law tort which is has a number of procedural and substantive limitation which are not really discussed here. However, it is worthwhile to know the very, very basic elements. A person has a valid cause of action for defamation when; (1) the defendant makes a false and "defamatory" statement concerning the person; (2) the defendant "publishes" or permits the "publication" of the defamatory statement to a third party without a legally-recognized privilege to do so; (3) the publication results from intentional or negligent conduct by the defendant, and; (4) special harm results from the publication of the defamatory statement or the statement constitutes defamation "per se."

Defamation is a long and storied cause of action that is never as simple as one thinks when you file it. For investigators, the best defense is that defamatory statement is true. Truth is the best defense to defamation. So, think about that in your interview, reports, letters and other interactions.

H. Iowa Civil Wiretap Act – Under Iowa statutory law, Chapter 808B of the Interception of Communication Act, a party to a communication has a civil cause of action against a person who intercepts, attempts to intercept, or employs or obtains another to intercept a communication, or against a person who uses or divulges information that he or she knows, or reasonably should know, was obtained by interception of a communication. Iowa Code § 808B.8.

1. Civil Statutes with Invasion of Privacy – Many spy torts are in fact based on a violation of criminal law. However, that is not necessarily a needed statute. Invasion of privacy is going to always be plead. The civil corresponding acts are for purely damages.

2. Interesting State Cases:

a. Animal House – Member who had been dejected by fraternity placed recording device in the ritual room of the fraternity. Records both alcohol violations and perceived hazing violations. Turns them over to the dean who institutes proceedings against the fraternity. Violation of the wiretap act and award over $100k was upheld. However, the court indicated that the fraternity had standing to sue because the fraternity had ownership interest in the recordings. Might be a good thought on our company policy. *Phi Delta Theta v. University of Iowa*, 763 N.W.2d 250 (Iowa, 2009).

I. Inter-spousal Torts Liability – All liability that may be had above, likely involved the coordination or at least notice by your client and the client's legal representative. These cases can be filed by one spouse against another and then

joined to the divorce. They can help offset bad behavior one way or another. Such is the case in these cases;

1. *Collins v. Collins*, 904 S.W.2d 792, 797 (Tex. App.—Houston [1st Dist.] 1995) (holding that the wife was entitled to statutory damages for the husband's covert taping of telephone conversations between the wife and her paramour, their child, and possibly the wife's lawyer).

2. *Meany v. Meany*, 639 So. 2d 229 (La. 1994) (holding judgment for negligent infliction of sexually transmitted disease).

3. *Cater v. Cater*, 311 Ark. 627, 846 S.W.2d 173 (1993) (holding claim for assault and battery-maintained divorce).

4. *Pappilion v. Jones*, 892 N.W.2d 763 (Iowa 2017) (holding claim for wiretapping in divorce).

III. CODIFIED ETHICS RULES AND LIABILITY – Although we have no codified ethics for investigators that are regulated, we do have some regulation that you ought to be aware of. You are also, as we will see below, going to be judged and held to the standard of Attorney's rules. Maybe not necessarily for you benefit but more for the determent your client, client's legal representative may suffer.

A. Iowa Department of Public Safety Chapter 221 – You should know the regulatory authority's rules. No undercover rule?

1. Administrative Rules – Not many… But, watch those reports and get a contract.

a. 661—121.15(80A) Reports. Any private investigative agency licensee who provides services to any client in this state shall make and offer to the client a typed or legibly written ink report containing the findings and complete details of the investigation, a copy of which shall be retained by the licensee for three years and made available to the commissioner for examination at any reasonable time upon a complaint from the client for whom the report was prepared. In the event a client does not desire a written report, the licensee will note the time and date on the file copy of the report that the client stated no desire for a written report or refused the offer.

Unlike attorney's, whose file is owned by the client themselves, you technically own your file. Can you use information in your file for another matter? Probably. You have no affirmative duty to forget. But be careful of conflicts. Why do you need to keep your file beyond three years?

b. Iowa Administrative Rules 661-121.5(6)(g).

> "Be of good moral character. Consideration of whether an applicant is of good moral character includes but is not limited to…
>
> Unless rendered confidential by law, the applicant's failing to report: (1) A serious crime, or (2) The location of any stolen property;"

c. Conflict of Interest – There is no provision for a conflict of interest. You might begin to develop some basic conflict of interest rules. You should know the Iowa Disciplinary Rules of Professional Conduct Rule 32:1.2. Again, not for your benefit but for the client and the client's legal representative.

B. Iowa Association or Private Investigators ("IAPI") – IAPI's code of ethics is similar to that of all other state associations. Basically, do the best you can. Is that specific enough?

1. Code of Ethics – IAPI's code is good but what about these?

   a. Shall provide professional services in accordance with local, state, and federal laws.
   b. Shall honor each client contract, adhering to all responsibilities by providing ethical services within the limits of the law.
   c. Shall safeguard confidential information and exercise the utmost care to prevent any unauthorized disclosure of such information.
   d. Shall refrain from improper and unethical solicitation of business; including false or misleading claims or advertising.
   e. Shall use due diligence to ensure that all employees and co-workers adhere to this same code of ethical conduct; respecting all persons, performing the job diligently and working within the limits of the law.
   f. Shall never knowingly cause harm or defame the professional reputation or practice of colleagues, clients, owners, the company, or any employee of the company.
   g. Shall NOT knowingly make a false statement of material facts.
   h. Shall cooperate with all recognized and responsible law enforcement and government agencies in matters within their Jurisdiction.

2. Position on Locates – In 2008, the National Council of Investigative and Security Services, Inc. adopted a position on providing location information to members of the public. Specifically, it stated, "A member shall, prior to providing a client any personally identifying or location information of an

individual, conduct appropriate due diligence to ensure that the client has a legitimate business or legal interest in obtaining that information. When such due diligence is not possible or appropriate, or if the client appears to not have a legal or business interest, the client shall be informed that their contact information will be provided to the person they are seeking and the personal identifying information of the person they are seeking will only be provided to the client if that party consents."

B. Iowa Rules of Professional Conduct Chapter 32 of the Iowa Court Rules – These are the ethics rules of the State Bar. However, as we will see, lawyers are responsible for their investigators. And, your actions are imputed upon the attorney. Additionally, if you get into a squabble about what you did, these are probably the rules, whether right or wrong, that you will be judged by.

1. Responsibilities Regarding Non-Lawyer Assistants; Iowa Rules of Disciplinary Conduct Rule 32:5.3 –Basically, you are your attorney's agent.

    a) No Discipline to Investigator – Although your lawyer is bound by these rules, you are not necessarily so. Your actions will be taken for the lawyer's actions. You are his agent and as such act under him. It is a wise move not to alienate your client lawyers.

2. Contact with Subject – Generally, considered an ethical violation of Iowa Disciplinary Rules of Conduct Rule 32:4.2: Communication with One Represented by Counsel. "A lawyer shall not communicate or cause or encourage another to communicate about the subject of the representation with a person, organization or entity of government the lawyer knows to be represented by another lawyer regarding that subject."

    a) Dating the Subject – You should avoid the James Bond moment and sleep with opposing party. "…if one spouse employs an investigator to procure evidence, and this agent entices the opposing spouse and her paramour to commit adultery, the spouse cannot successfully obtain a decree, although he may not have directed or authorized his agent to bring such adultery about." Basically, you can't sleep with the subject. *Smith v. Smith*, 218 S.W. 602 (Tex. Civ. App. 1919).

3. Contact with Third Parties or Unrepresented Persons –

    a) Rule 32:4.1 Truthfulness in Statements to Others – In the course of representing a client a lawyer shall not knowingly: (a) make a false statement of material fact or law to a third person; or (b) fail to disclose a material fact to a third person when disclosure is necessary to avoid making the lawyer a party to a criminal act or knowingly assisting a fraudulent act perpetrated by a client.

So, you should not make false statements of material facts. This is more about a client using the lawyer's services to commit a fraud.

IV. DISCOVERY & EVIDENCE RULES

A. Discovery – I intend to give this section *very, very* short shrift. I will concentrate on surveillance issues. You should be aware that surveillance activities by its necessity creates a fact witness which allows for discovery by the other side. You need to be aware that fact witnesses are generally discoverable under both the Iowa and Federal Rules of Civil Procedure. You're report, video, audio, notes and case file have the potential to be discoverable and generally are. Work product is important but, it is dying for surveillance.

B. Evidence – Again *very, very, very* short shrift. For surveillance purposes, let's look at admission of witnesses, business records, audio and video.

1. Witnesses –

   a) Insane Persons – Generally, competent unless insane at the time offered or at the event testified about.

   b) Children – Must appear to possess sufficient intellect to relate the transactions with respect to which they are interrogated. BUT, be aware of Juvenile Codes and political implication.

2. Business Records – All police records, hospital records and even your own records are admitted under this common rule. The key is that as long as it is a record of a regularly conducted activity. If at least 14 days to trial, instead of a records custodian (who is this) you can authenticate these documents by affidavit and ask them to be admitted. You, as an investigative agency, (with a good P&P) can authenticate your regularly prepared reports. Some objections are still here; BUT the practicality of it is that many times they are never made. Great benefit, because they can take your report back with the jury and judge. Score points with your reports with or without you being present to testify.

3. Video Evidence – All should review at some point. Only two things are required to be shown; (1) that the witness knows relevant facts about the scene or objects represented in the photo; and (2) that he or she can say that it correctly and accurately portrays those facts (or, as many of us say, "It is a true and accurate depiction …").

   It is not necessary for the witness to establish the date when the photograph was taken because it does not matter what date it was taken if the condition is unchanged. It is not required that the witness describe how the camera mechanism was properly calibrated, or to establish a chain of custody or

any other such thing, although I did have a chancellor years ago sustain objection after objection until I guessed that he was requiring me to ask the witness to identify who took the photos. But that judge was in error; who took the photos is not relevant to admissibility. All that is necessary is for the witness to establish knowledge of the matters depicted and to affirm that the photo does truly and accurately depict the conditions he observed.

Photographs or videotapes are generally admissible when verbal testimony as to matters depicted is also admissible and, thus, are inadmissible only if probative value is substantially outweighed by danger of unfair prejudice, confusion of issues, or misleading jury, or by considerations of undue delay or needless presentation of cumulative evidence.

4. Audio – Audio can come in to evidence through a couple of different ways. However, most times that you are recording a witness you are doing for impeachment purposes. Usually used under Prior Inconsistent Statement. Almost always the case by which audio is used in the courtroom in the types of investigations you do.

To get it in you authenticate it by a witness with knowledge, opinion based upon hearing a voice under circumstances that connect it with the alleged speaker, or self-identification coupled with the context, content, and timing of the call.

V. SOCIAL MEDIA

A. Requirement to Investigate – Social media is becoming one of the top communication methods for most people. Your duty to investigate them has even been upheld by some courts. *Cannedy v. Adams*, No. ED CV 08-1230-CJC(E), 2009 WL 3711958 (C.D. Cal. Nov. 4, 2009) (stating that a lawyer's failure to locate a sexual abuse victim's recantation on her social media profile could constitute ineffective assistance of counsel); *Johnson v. McCullough*, 306 S.W.3d 551, 558 (Mo. 2010) (affirming that litigants and their attorneys have an affirmative duty to make online investigation part of their jury selection process "in light of advances in technology allowing greater access to information").

B. Civil Discovery Issues - Generally, the preferred, if not required method is to serve discovery requests to the user NOT the providers.

1. ECPA / SCA Limitations – Under the ECPA, electronic service providers (Facebook, Myspace, LinkedIn, Instagram, Twitter, etc.) "shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service. 18 U.S.C. § 2510(a)(1). This narrow language has allowed social media providers to successfully resist discovery by invoking this statute to quash a subpoenas for their customer information. *See In re Facebook, Inc.*, 923 F. Supp. 2d 1204 (N.D. Cal.

2012) (holding that subpoena was invalid because it sought customer communication from a provider); *Theofel v. Farey-Jones*, 359 F. 3d 1066 (9th Cir. 2004) (quashing subpoena under same reasoning); *Viacom Int'l, Inc. v. YouTube, Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (holding that the ECPA prohibits disclosure of electronic communications pursuant to a civil subpoena because the ECPA "contains no exception for disclosure of such communication pursuant to civil discovery requests").

a) You Don't Get Mail – State Farm insurance in suit attempts to subpoena email and other communication from AOL server. Court holds that the clear language of the above statute prohibits AOL, a service provider, from divulging the contents of party's electronic communications pursuant to a civil subpoena. *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp 2d 606, 610-611 (E. D. Va. 2008).

2. Some Exceptions Apply – Under 18 USC § 2702(b)-(c), an electronic service provider can disclose communications only if requested by (1) the originator of the communication; (2) the communication's intended recipient or an agent of the recipient; (3) the National Center for Missing and Exploited Children; (4) a law enforcement agency; or (5) a governmental entity in the case of an emergency involving the danger of death or serious physical injury to another person. 18 U.S.C. 2702 (b)-(c).

C. "Friending" the Subject or Witness – When you "fake friend" an individual for other motives, particularly to advance your lawsuit claim or do your investigation, you can create liability for yourself and the attorney that you work with.

1. Texas Disciplinary Rules of Professional Conduct 4.02 – Remember you cannot make contact with a represented person under this ethics rule. Same rule for the Model Rules of Professional Conduct and in all states. Prohibits attorneys or those that the supervise or direct from this tactic against any individual that might be a potentially interested party. Many bar associations have now held that their rules of professional conduct prohibit lawyers from engaging in deceptive behavior or misrepresentations to third parties in cyberspace. Philadelphia (2009); New York City (2010); New York State (2010); Oregon (2010); and New Jersey (2011).

2. Third Party Can Provide - Information can come from a third party of the use. Allows you asking a person with access to share that information with you. Don't be deceptive. Just ask to see from another friend. *Palmieri v. USA*, F. Supp. 3d, No. CV 12-1403 (JDB) (D.D.C. Nov. 3, 2014). (upholding revocation of security clearance where friend gave over Facebook information. Court held no violation of 4th amendment for law enforcement). Key here is third party. If you give information to third party

then, generally, you lose an expectation of privacy claim on that information. *See Guest v. Leis*, 255 F.3d 325, 333 (6thCir. 2001) (finding that writers of email, just like a letter, lose their expectation of privacy in the emails contents upon delivery to a third party) Again, generally, if no 4thamendment violation, then no invasion of privacy claim.

D. Admission and Authentication – Getting these into evidence can be tricky as there is no clear cut rule. Generally, use the best use of the evidence is to get it authenticated from the witness itself or use it as a party opponent admission. Or, try and ask for the password or to view in open court. If not, Texas courts have held that you should try and present evidence of corroboration to that the social media is what it is supposed to be. *Tienda v.* Texas, 358 S.W.3d 633 (Tex. Crim. App. 2012). What does that evidence look like?

1. Meta Data – Try to obtain and preserve the meta data from the post including the author, location, date, and time by printing out and storing such information.

2. Screen Shot – Screen shots help capture data and show that the data and post was not modified from the date of capture.

3. Witness / Investigator – Use a witness, witnesses, or investigator to act as a trial witness to buttress the authenticity of the message. Although objectionable, put some thought into the idea of creating a standardized social media report. Then try and admit it through the business records affidavit.

VI. DRONES

A. FAA Modernization and Reform Act – Passed in 2012, the purpose was to integrate over a five-year plan unmanned aircraft systems ("UAS") into the national airspace system. As part of the FMRA, Congress provided basic criteria for the establishment of drone regulations by the FAA and also provided a safe harbor for those drones which are under 55 pounds and are model aircraft. Drones which exists in this size have exploded in recent years. Many of them now are equipped with high power and high definition recording devices.

1. Commercial v. Non-Commercial – Last couple of years, the FAA under its rulemaking authority granted to it by Congress, began issuing rules for those drones under the 55-pound threshold. It has delineated these rules for those drones used in commercial applications and those exempted by the FMRA as model aircraft. So, if used recreationally, those drones are now exempt from regulation.

a) Basic Rules – The FAA has further required that operators maintain unaided visual contact with the drone at all times. The FAA has also restricted operation to daylight hours, a maximum speed of 100

miles per hour, and a maximum altitude of 500 feet above ground level. Really an unenforceable rule.

b) Commercial Operators – To do what you want and use it, you would almost have to be a commercial operator. Those proposed rules have been that:

(1) operators pass an aeronautical knowledge test;

(2) operators receive a security clearance from the Transportation Security Administration;

(3) operators would have to obtain an unmanned aircraft operator certificate with a small UAS rating (one that, similar to existing pilot airman certificates, would never expire);

(4) operators must pass a recurrent aeronautical knowledge test every 24 months;

(5) operators must be least 17 years old, AND;

(6) there drone must be registered just like any other aircraft and it must display its aircraft registration markings.

Until these regulations go into effect, you can ask the FAA for an exemption. As of last year, over twelve hundred exemptions had been granted too various public and private entities to lawfully engage in commercial operations using small drones.

On July 21, 2016, the above rules, with some additional limitations, were adopted and will be effective beginning at the end of August, 2016. However, you can still ask for an exemption. FAA Small Unmanned Aircraft Rule (PART 107).

c) Privacy Issues – FAA has punted the ball on privacy issues and appears to signal that local communities will be the one to regulate those matters.

B. Aerial Surveillance – Although unmanned drones are still an issue, use of aerial surveillance has constantly been upheld by a variety of courts. Basically, they have held that a flight in the normal airspace following FAA regulations which oversees with the naked eye evidence is not a search or seizure under the fourth amendment. They have consistently said that there is no reasonable expectation of privacy by a fly over. However, problems do surface when the fly over becomes disruptive or repetitive. Thinking hovering helicopter. *California v. Ciraolo*, 476 U.S. 207 (1986); *Dow Chemical Co. v. United States*, 476 U.S. 27 (1986); *Florida v. Riley*,

488 U.S. 445 (1989); *Moss v. State*, 878 S.W.2d 632 (Tex. App.—San Antonio 1994).

THE END!

HAVE A GOOD CONFERENCE!!