PRETEXTING AND OTHER ELECTRONIC EVILS

By Marshall W. Waller, Family Lawyer

Welcome to the 21st century a wonderful time indeed to experience all that technology has to offer in the form of smartphones and the Internet. Gone are the days when we could communicate in a presumed secure and confidential environment, nor are we exempt from having our specific location pinpointed almost anywhere on the planet. Bad times, indeed to be a teenager ... or a divorcing spouse.

Since we are discussing a concept that is the by-product of 21st Century technology I thought it would be fun to trace its roots, so I looked up the word "pretext" in a copy of Black's Law Dictionary I have in my office that my dad used when he studied law after World War II. It defines pretext as: "Ostensible reason or motive assigned or assumed as a cover for the real reason or motive; false appearance, pretense." Dictionary.com provides the following definition: "something that is put forward to conceal a true purpose or object; an ostensible reason; excuse."

Pretexting is anything but new. It has been around undoubtedly as long as humans have been around and able to think and communicate with each other. It is the sweeping availability of the tools of pretexting, however, brought about by the age of the Internet and the resultant multitude of traps for the unwary, that has moved this term from a noun to a verb.

For those of you who care about this kind of thing, the word pretext traces its origins to the» 14th century Latin, literally meaning "to weave in front, to adorn." And in the UK pretexting typically goes by the name "blagging" (go figure), although to "blag" perhaps made its way across the English Channel from France in the late 19th century from the French blaguer, "to tell lies."

A search of the Internet reveals this definition: "Pretexting is a form of social engineering in which an individual lies to obtain privileged data." Usually this takes the form of someone pretending to be someone else in the form of identity theft when they set up a Facebook or similar account in someone else's name so they can gain access to the other person's friends and such and with it personal information they think can help them in some way.

Pretexting to gain financial information was specifically criminalized in 1999 by the Gramm-Leach-Bailey Act, but those restrictions do not apply to information that finds its way into the public domain, such as real estate transactions, court documents and the like. Further, when someone hi-jacks a Facebook account, that information is for the most part entirely in the public domain anyway, so who gets to exercise control over that? It is indeed a bit of a gray area.

As for how this comes up ... how about when your client gives you their access information to Our Family Wizard so you can farm it for evidence to use against the opposing party? The minute you log on you are "adopting" the identity of your client, and thus engaging in pretexting. Or perhaps your client gives you the access information to their Facebook account, or their bank's web site? Have you ever had your assistant, or perhaps even you yourself, call somewhere and pretend to be someone else in an attempt to gain information, "Hello, I am

calling from 'X' Flower Shop. Will Mr. Jones be in later today to receive a delivery?" If so, you are pretexting.

By the way, "pretexting" isn't simply pretending to be someone else; pretexting extends to obtaining information by any form of deception as well, for example when a criminal calls a victim and pretends to be conducting a survey in an attempt to obtain personal information, which the criminal can then use when speaking with, for example, the victim's bank. Pretexting can arguably be used for good: have you ever seen "To Catch A Predator" on TV? That's the show that lures pedophiles in so they can be filmed, caught and then arrested.

In 2006, the CEO of computer giant Hewlett-Packard became embroiled in a pretexting scheme and eventually resigned. In an effort to discover the source of internal information leaks, the former CEO hired an outside investigator. Several Hewlett-Packard executives discovered that their personal and professional phone records had been collected without their permission. Following an investigation, it was determined that the outside investigators had used pretexting in order to obtain those phone records. The phone company's representatives believed they were communicating with the real Hewlett-Packard employees.

Pretexting is huge, and becoming more so. It is all over the Internet and is becoming a cottage-industry in its own right. It is spoken of as "social engineering" and those who practice it as "social engineers," and you are probably doing it even now without even realizing it.

This issue also extends into the area of email. Who among us hasn't at some time had free access to our spouse's email account? It is certainly not uncommon and in this author's experience happens with great frequency. Problems arise, however, when your client, who possibly has this information because she set up her husband's email account and therefore knows his password to login, is now able to view all of her husband's private emails. How often have you had a client bring an email in to you that he or she took from their spouses email account? Can counsel use this information? What should be done here?

Best practice instructs not to use them or give them to the judge. Most personal emails (not employer-provided emails) are "private." Hacking into private emails can actually be found to be an act of domestic violence (See IRMO Nadkarni (2009) 173 Cal.App.4th 1483, which held that allegations that a former husband accessed, used and publicly disclosed his former wife's confidential email were facially sufficient to satisfy subsection (a) of Family Code section 6320, which lays out the statutorily offensive conduct. Family Code section 6203 defines "abuse" such as will justify the issuance of a restraining order as "to engage in any behavior that has been or could be enjoined pursuant to section 6320.

At the point that the client hands her lawyer this information the lawyer definitely has a problem, because if the client now wants to testify about the information learned from the email she is exposing herself to serious consequences, perhaps even criminal consequences. If this occurs in court, counsel should, at the first opportunity (and should create such an opportunity immediately if the client is about to testify), go outside and discuss with the client the inappropriate nature of what she did, the potential consequences of her actions and the fact that she cannot be asked nor can she testify about this information or any information that stems from it (fruit of the poisonous tree) without being exposed to negative consequences. If the client has information about this from other source, then that is a way to delve into that subject, but the client needs to be able to answer the question on cross-examination "how do you know that?" and she better not say "I got it out of my husband's email."

This problem is further exacerbated if the client brings in emails she obtained from her husband's account that are communications between him and his lawyer. If counsel becomes exposed to material that is reasonably believed to be privileged material from the opposing attorney, counsel must immediately stop reviewing it and return it to the opposing attorney or shred it, delete it, whatever it takes to permanently remove it from counsel's file and office.

Add into this mix GPS (Global Positioning System) devices and the exposure increases even more. It is not at all unusual for clients to want to, or actually surreptitiously place devices on their spouse's car so that their movement and driving behaviors can be monitored and reported. These devices cost about $400, are available on the Internet, are about the size of a pack of cigarettes and can be installed in less than a minute using no tools whatsoever.

This is an interesting issue: what is the legality of installing a GPS tracking devices in a spouse's vehicle? If the vehicle is solely owned or leased by the tracked spouse, then this conduct would be prohibited without the tracked-spouse's authorization. There is no relief if the vehicle is in joint (both) names, however, because the registered owner has to consent to the placement of the tracking device, and if both spouses own the car then isn't the consent of both registered owners needed? In this author's opinion the answer is "yes." Further, if the tracked spouse regularly drives the vehicle, even if the car is registered only in the name of the- tracking spouse, that tracking spouse may be prosecuted for stalking.

Penal Code section 637.7 sheds light on this subject. It provides, in part:

> (a) No person or entity in this state shall use an electronic tracking device to determine the location or movement of a person.
>
> (b) This section shall not apply when the registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle.

Subsection (f) of section 637.7 ups the ante quite a bit for lawyers in this situation in that it essentially provides for revocation of licensure as a punishment for violation of this section:

> (f) A violation of this section by a person, business, firm, company, association, partnership, or corporation licensed under Division 3 (commencing with Section 5000) of the Business and Professions Code shall constitute grounds for revocation of the license issued to that person, business, firm, company, association,• partnership, or corporation, pursuant to the provisions that provide for the revocation of the license as set forth in Division 3 (commencing with Section 5000) of the Business and Professions Code.

To thus answer the question: What should be done with this information? If it is used, isn't counsel using information illegally obtained? In this author's opinion, that answer is "yes" and counsel is ethically prohibited from doing that lest he lose his license to practice law. Indeed, Business and Professions Code section 6106 ("Moral turpitude, Dis- honesty or Corruption Irrespective of Criminal Conviction") provides that "the commission of any act involving moral turpitude, dishonesty or corruption, whether the act is committed in the course of his relations as an attorney or otherwise, and whether the act is a felony or misdemeanor or not, constitutes a cause for disbarment or suspension."

Further, Business and Professions Code section 6103 ("Disobedience of Court Order; Violation of Oath or Attorney's Duties") provides "A willful disobedience or violation of an order of the

court requiring him to do or forbear an act connected with or in the course of his profession, which he ought in good faith to do or forbear, and any violation of the oath taken by him, or of his duties as such attorney, constitute causes for disbarment or suspension."

And what oath do lawyers take?

> (a) To support the Constitution and laws of the United States and of this state.
>
> (b) To maintain the respect due to the courts of justice and judicial officers.
>
> (c) To employ, for the purpose of maintaining the causes confided to him or her, those means only as are consistent with truth, and never to seek to mislead the judge or any judicial officer by an artifice or false statement of fact or law.

It does indeed seem obvious that lawyers cannot knowingly use information that has been illegally obtained without violating their oath as an attorney, and yet far too often we see this type of behavior in court, in depositions and in settlement negotiations.

It is also not uncommon for these intrusions to take the form of surreptitious video recordings. People v. Gibbons (1989) 215 Cal. App. 3d 1204, dealt with a violation of Penal Code section 632 and involved a defendant who set up a video camera in his closet so he could record himself having sex with unsuspecting women. The defense argued that because there was no audio portion it was not a violation, but the court drew out the term "communication" from the statute and found that "communication" can include a person's "conduct" (referred to as "communication by conduct.") The court stated at page 1209: "we find that "communication" as used in the privacy act [of which section 632 is a part] is not limited to conversations or oral communications but rather encompasses any communication, regardless of its form, where any party to the communication desires it to be confined to the parties thereto. If the act covers eavesdropping on or recording of a telephone call, it surely covers the non-consensual recording of the most intimate and private form of communication between two people."

This paragraph is less instructive than it seems, however. On the one hand, it seems that if the behavior obtained by the hidden video falls into the category of something intended to be "confined to the parties thereto," regardless of what it is, the privacy statutes would apply, but the court then goes on to discuss an example of such a communication using the phrase "the most intimate and private form of communication between two people." A credible argument can be made that the court intended its ruling to be limited to conduct (communication) of a highly intimate and private nature, opening the door for more mundane (yet nonetheless potentially damaging) conduct to be allowed to be used. It is recommended that prior to citing this case a good read of the dissenting opinion is undertaken.

Finally, care should be given before hiring the services of a private investigator in these cases. Judicial officers are generally on the lookout for behavior exhibited by a spouse (or their attorney) that gives cause for them to question the motivation for such behavior. Too often, courts will look upon the retention of a private investigator as a sign of stalking or a more deeply (and disturbingly) inability to "let go" and move forward.

The case of Noble v. Sears, Roebuck (1973) 33 Cal.App.3d 654 discusses the potential for liability for invasion of privacy by reason of unreasonably intrusive investigation. Also, the hirer of an investigation agency/provider may be liable for intentional torts of those employees and also for negligent choosing of an investigator. The truth is, when a lawyer hires an investigator

to perform services for the lawyer, liability attaches, and this should be approached with caution because when new people are incorporated into the legal representation care must be given to control and direct their efforts as much as possible, especially since their actions could create conflicts, ethical violations and violations of the law.

The moral of this story then is to exercise caution when managing and processing these cases. Use care in the acceptance of information from the client, and be aware that such information might very well have been obtained illegally, either innocently or intentionally. Some basic rules to share with divorce clients at the beginning of the case include the following:

1. OBEY THE LAW
2. Don't stalk your spouse
3. Don't hack into your spouse's email
4. Don't destroy evidence
5. Don't commit perjury

Seems basic enough, and yet these simple rules are violated on a daily basis. The license to practice law is obtained with difficulty and very easily lost, and whether the approach is one of "winning" or "resolving," care must be given to play by the rules and not get caught up with a client who doesn't.

This article has been used with permission by its author and originally appeared in ACFLS Family Law Specialist, Summer 2013, No.2.

Marshall Waller is a Certified Family Law Specialist with Feinberg & Waller in Beverly Hills and Calabasas, CA. He has gained a reputation as a dynamic and entertaining speaker and has spoken nationally and locally to trade, civic, and private organizations. www.feinbergwaller.com