Pretexts: Legal and Ethical Considerations in Internal Investigations

By Christopher T. Marquet, CEO, Marquet International Ltd.

This week's revelation that Hewlett Packard hired an investigative firm to determine the identity of a leaker on its Board, which reportedly utilized pretexts to obtain private phone records, raises serious questions of a legal, regulatory and ethical nature. While the investigation successfully identified the culprit on HP's board, the ends do not necessarily justify the means. Clearly the specific circumstances in this case will need to play themselves out as civil, criminal and regulatory probes proceed, before we will know whether any actual criminal wrongdoing was involved. Nevertheless, where the company was clearly justified in conducting an investigation in this case, tactics used may end up causing considerably more damage then any leaks that may have occurred.

A pretext is the use of a subterfuge on the part of one party, usually posing as someone they are not, or using an individual's personal identifiers, to obtain information from another party who would not otherwise disclose such information. Some private investigators have used this technique in interviews with individuals and in making inquiries with private and government institutions. While there are some circumstances where pretexts can justifiably be made, there are many where pretexts are inappropriate and even illegal.

Obtaining financial information from institutions utilizing pretexts is strictly illegal under Federal law (see Gramm-Leach-Bliley). Similarly, the Federal Trade Commission, under the Fair Credit Reporting Act, requires consent for parties to obtain credit information on individuals. In other words, it is illegal to obtain banking records, credit reports, securities accounts, etc. by posing as an individual using their personal identifiers or as an authority of some kind to do so.

In the course of an internal investigation, there are many legitimate avenues of inquiry, such as the inspection of books and records, including electronic records, under the control of the company. However, when records fall outside of that control, i.e. records from personal accounts, such as residential phone, cell phone, credit card, banking and e-mail records not owned by the company, we would consider these out-of-bounds. According to the FTC, utilizing pretexts to obtain personal phone records is also illegal.

Certain states, such as California and Illinois, have made all forms of pretexts illegal. In at least one third of the states, utilizing pretexts to obtain information in the context of an insurance claim, has also been outlawed. Many states, as well as Federal regulations designed to protect consumers from identity theft, constrain both record holders and would-be pretexters over personal information. So when are pretexts appropriate?

Generally speaking, it is inappropriate to impersonate an existing individual in order to obtain confidential information. To obtain personal identifying information, such as date of birth, social security numbers and mother's maiden names and then use it to obtain confidential information from third party institutions posing as that individual, is also wrong, if not outright illegal. Posing as a law enforcement officer, regulator or other authority to elicit information is likewise inappropriate, if not outright illegal.

A legitimate pretext might be where an investigator pretends to be conducting an industry survey and interviews a group of executives using a fake name to obtain information not generally available to the public. Nevertheless, the use of pretexts is one of those black or grey areas that warrant strict scrutiny when contemplated. Another form of pretext, generally deemed appropriate, involves sting operations. Posing as an individual with a business proposal can sometimes be a very effective tool in conducting intellectual property theft investigations. Such an operation would require thorough planning and oversight before implementation.

Other investigative techniques, such as surveillance and "garbology" – dumpster diving in lay parlance – also face strict privacy restrictions. Third party eavesdropping on conversations without a warrant, is also illegal. However, in states where one-party consent is allowed, such as in New York, an investigator can tape conversations without disclosing the fact. Otherwise, surreptitious taping of phone conversations is illegal.

There are many appropriate investigative techniques available to outside and inside investigators. For example, there is a plethora of public information available on individuals and companies in the US (not so true overseas) to be culled. Investigations should always begin there. Privacy laws restrict the actions of investigators who, many times are operating at the direction of counsel. Unfortunately, instances like the one involving investigators for HP using apparently improper pretexts and the apparent illicit eavesdropping conducted by Hollywood private investigator Anthony Pellicano several years ago, highlight the necessity for counsel and advisors to be certain of their investigators and what they charge them to do.

Some sensible things to consider when hiring and managing private investigators include:

- Obtain referrals from other attorney(s)
- Make sure they are professionally licensed & have appropriate insurance
- Check references
- Be sure they have a reputation for legal & ethical behavior
- Make sure they pass the "face-to-face" test
- Be sure they have no conflicts of interest
- Have a written engagement letter or agreement for each assignment (establish confidentiality & work-product privilege)
- Set forth investigative activities clearly
- Discuss case thoroughly in advance
- Agree to a budget and timeline in advance
- Agree to the deliverables (reports, verbal & written)
- Maintain regular and clear communications
- Be wary of the "wink and nod"

There are many excellent uses for private investigative and intelligence firms, including conducting due diligence, fact finding, forensic accounting, electronic evidence gathering, competitive intelligence, asset searching and conducting interviews. Nevertheless, our industry must live within legal, regulatory and ethical boundaries as does every other profession.

Christopher T. Marquet is CEO and Founder of Marquet International, Ltd., corporate investigative, due diligence, litigation support and security consulting firm. He can be reached at chris@marquetinternational.com or (617) 733-3304 in Boston or (917) 733-1038 in New York. Visit our web site at www.marquetinternational.com.