

THE FCPA AND WIRETAPS

Michael Volkov, Partner, Mayer Brown LLP, Washington, D.C.

Corruption, Crime & Compliance: <http://corruptioncrimecompliance.com>

The idea of wiretaps in corporate board rooms sends shivers down every director's spine. It should. The Justice Department no longer views white collar crime as different than organized crime, gangs or drug trafficking. What that means from a practical standpoint is that federal agents are using the same investigative tactics as they have historically used against organized crime and drug traffickers.

For companies this exponentially increases the risks of enforcement and successful prosecutions against companies and individual directors, officers and employees.

It is only a matter of time until an FCPA case is prosecuted using wiretaps. Federal agents have used every tactic up to the point of wiretaps – undercover officers, telephone recordings (over 5000 in the Shot Show sting case), videotaped meetings, one-party consent recordings, ambush interviews and search warrants.

For in-house counsel and compliance officers, there is one important message that must be communicated inside an organization – it is risky for any director, officer or employee to discuss with any outside party any sensitive topics relating to the FCPA or any other legal compliance issue.

As I frequently explain, imagine that every person you speak to outside the organization is recording what you say. Not only do directors, officers and employees have to be careful when writing emails but they need to be just as careful when speaking to anyone outside the organization. In some cases, this may extend to people inside the organization since whistleblowers or disgruntled employees may be recording conversations or telephone calls (assuming that such recordings are authorized under state law). This risk was amply demonstrated in the Archer Daniels and Mark Whitaker fiasco in the 1990s when Whitaker recorded and videotaped numerous cartel meetings and communications in the vitamin industry.

The government will not seek a wiretap unless it is going to be productive and advance an investigation. Federal agents have an incentive to conduct a wiretap because it is an important task for them to complete in order to advance their careers in their respective organizations. They are very costly and time intensive. Many agents do not like to conduct wiretaps because of the extensive time required. However, some agents like using wiretaps because they can avoid “street work,” especially in those cases where other investigative techniques are unsuccessful or difficult to conduct.

Federal agents are always looking for a possible “dirty phone,” a phone that is being used to advance or facilitate a federal crime such as foreign bribery, insider trading, or mail or wire fraud. Informants and undercover officers are used to help identify the “target dirty phone” and then record calls which show the target using the phone for illegal purposes with the informant or undercover officer. Cell phone records and pen registers usually supplement such

information to demonstrate that the target uses the telephone to communicate with other individuals involved in criminal activity.

The power of wiretap evidence, when corroborated, can be overwhelming in front of a jury. There is nothing more devastating to a defendant than his own words being played in front of a jury.

The Justice Department's success in its inside trading investigation was the direct result of its ability to obtain and then use wiretap evidence. Without this evidence, there is no way the Justice Department would ever have been able to identify the secret, illegal information being communicated among private equity and hedge fund operators and the use of expert consultants to communicate such inside information.

Some have argued that wiretaps for white collar cases like insider trading or FCPA violations are not authorized by the wiretap statute. They are deluding themselves and their clients. That is not the most effective way to challenge a wiretap. It is a losing argument. Even if defense counsel finds a sympathetic judge, the statute is clear and there is a minuscule chance that the wiretap would be suppressed as unauthorized, especially if the government pays close attention to the authorization and approval process by carefully preparing its documents and monitoring the wiretap.

There are a limited number of arguments to raise challenging a wiretap.

First, any person intercepted has standing to challenge the wiretap. One critical requirement that the government must demonstrate in its wiretap application and affidavit is that agents have exhausted all traditional investigative techniques and been unable to secure adequate evidence to prosecute the defendants. Another way of putting it, the federal agents have to show that there is really no other way to investigate and prosecute the individuals involved in the criminal activity.

Second, defense counsel need to carefully review the application and affidavit to ensure that the agent did not make any material misstatements or omissions in the written materials. Even if there are such misstatements and omissions, a judge will be reluctant to suppress the wiretap evidence. However, it is important for the defense to attack the investigation by showing that the agent cut corners, was sloppy or even unethical.

Third, it is important to review how the wiretap was conducted. There are specific requirements with regard to minimization which require agents to turn off wiretapping equipment during conversations which have no relevance to the authorized investigation. Agents are notorious for listening in on entertaining personal conversations, especially sexual ones, which should be minimized. Again, defense counsel need to highlight any instances of misconduct or unauthorized interceptions to undermine the integrity of the agents and the investigation.

Most agents are careful when conducting wiretap investigations. Some are not and they give the defense an opportunity to challenge the wiretap. Companies should assume that the possibility of a wiretap is a real risk in the anti-corruption area and plan accordingly. It may

sound scary to directors, officers and employees, but it is a reality in today's enforcement environment.