

WHO'D WANT TO BUG YOU

A "bug" is an electronic device capable of recording or transmitting information without the knowledge of the victim. A recent Washington study reported that 25% of the Fortune 500 companies use "information gathering" techniques. Because state-of-the-art listening devices, although illegal, have become smaller and more sophisticated, they are unfortunately being more widely used. It is becoming increasingly necessary to check boardrooms, conference rooms, executives' office, etc., for listening devices so confidential information can be kept confidential.

With today's technology it is very simple to obtain the necessary electronic devices needed to wire a home or office. In fact, there are more phone calls received (4 out of 5) to put bugs in than to find them and take them out. Although installing them is a felony punishable by 5 years in jail and a \$10,000.00 fine, all indications are that this is a very lucrative venture as companies that sell this equipment are booming. A recent issue of an electronics magazine showed 21 advertisements for bugs in the classified ads alone!

When are you most likely to be a victim of an illegal bug?

- . If you or you're firm are involved (or about to become involved) with any litigation.
- . If you are having problems with a partner or corporate officer.
- . If you're firm is involved with a buyout, a stock purchase or sale, or an acquisition.
- . If you or you're firm is newsworthy, or involved in government or international contracts.
- . If there is a threat on your life or your family members' lives.

Indications that bugging might exist:

- . If you have a break in and little or nothing is taken.
- . If you have lost contracts or bids by a small margins.
- . If your competition seems to be one step ahead of you or mysteriously comes up with similar products or ideas.
- . If you have lost important or key clients unexplainably.

Because of the bug, are you more vulnerable? No one seems to be immune to this illegal form of information gathering, from the husband or wife that puts a recorder on the phone to incriminate their spouse, to the retailer who bugs his Competitor's fax machine to get copies of future ads. Recently, a most unique bug was found in an antique shop. The shop had several shipments high-jacked while in transit from New York to Atlanta. A "debugging sweep" was performed, turning up a transmitter inside an ornament of Santa Claus hanging innocently on the Christmas tree. There are numerous other cases, such as the case where a Jr. Vice President was blackmailed with exposure of his sexual indiscretions if he didn't help a person involved in litigation with his firm.

If you were bidding on a million dollar contract, would it be worthwhile to your competitor to pay a few thousand dollars for your bid information? Of course it would. So it then goes back to ethics. How ethical are your competitors? There was recently a case where a college professor was paid \$50,000 to design a transmitter for an ex-student, who is now a CEO of a large firm. He needed his competitor's bid before placing his on a billion dollar deal. If there is a physical protection problem for the executive, or fear of kidnapping of his family, a sweep is essential. If someone can obtain your travel plans, they can pick the best time for an attack. You are more vulnerable than you might think.