

The Online Journal
GET 2 WEEKS FREE
[SUBSCRIBE NOW](#)

The Print Journal
GET 2 WEEKS FREE
[SUBSCRIBE NOW](#)

User Name: Password:
 Remember Me [Log In](#)
Forgot your username or password? | [Subscribe](#)

OTHER FREE CONTENT FROM THE WALL STREET JOURNAL

EDITORS' PICKS

- [Second Screening](#)
- [Capital Journal](#)
- [Vanishing Act](#)
- [The Middle Seat](#)
- [Racial Barrier](#)
- [That Syncing Feeling](#)
- [MORE EDITORS' PICKS](#)

BLOGS

- Most Popular Posts
1. [Obama Will Decide: Is the Democrats' 09 Message Flawed?](#)
 2. [Buzz Links: Remembering George Carlin, From 'Hippy Dippy' to '7 Words'](#)
 3. [You Know It's a Bear Market on Wall Street When...](#)

[SEE ALL BLOGS](#)

MORE FREE CONTENT

- [Personal Journal](#)
- [Personal Finance](#)
- [Leisure](#)
- [Markets Data Center](#)
- [Video](#)
- [Blogs](#)
- [Forums](#)
- [Interactives](#)
- [Autos](#)
- [Career Journal](#)
- [Real Estate](#)
- [Small Business](#)
- [Opinion Journal](#)
- [MarketWatch](#)
- [All Things Digital](#)

★ **A Daily Political Newsletter from WSJ.com's Opinion Editors** ★ [SIGN UP NOW](#) →

Targets of Spying Get Smart

By M.P. MCQUEEN
June 11, 2008; Page D1

Tiny electronic-surveillance gadgets that James Bond could only dream of are increasingly turning up in boardrooms, bedrooms and bathrooms.

Crooks are parking vans outside people's homes to steal bank-account passwords and credit-card numbers, using programs that tap into Wi-Fi connections. Paparazzi hide cameras and microphones in private jets, hoping to record embarrassing celebrity video. Corporate spies plant keystroke-recording software in executives' laptops and listen in on phone conversations as they travel.

Now, people are deploying counter-spy technology to fight back. Some celebrities and corporate executives get regular sweeps of their offices, limos and private jets in search of hidden devices. Others hire security experts to safeguard their phones and home computers. And corporate security experts are advising businesspeople on how to keep company secrets safe while traveling abroad.

Demand for counterspy services has been heightened by a series of recent snooping incidents. Last month, Hollywood sleuth Anthony Pellicano, 64 years old, was convicted in federal court in Los Angeles of multiple counts of racketeering and illegal wiretapping. He worked on behalf of celebrities and moguls who were involved in personal or business disputes, including Bertram Fields, one of Hollywood's top entertainment lawyers; Brad Grey, now head of [Viacom Inc.](#)'s Paramount Pictures movie studio; and talent agent Michael Ovitz, according to the indictment. The three have denied any wrongdoing and haven't been charged with any crimes.

Actors Sylvester Stallone and Keith Carradine were among those who were wiretapped. Mr. Pellicano paid off phone-company workers and used a computer-software program to intercept the actors' phone calls, according to his indictment.

In April, car maker [Porsche AG](#) disclosed it had found a baby-monitoring device concealed behind the hotel sofa of its president and chief executive, Wendelin Wiedeking, last fall during his trip to Wolfsburg, Germany, for meetings with executives at [Volkswagen AG](#). An investigation is continuing, said a company spokesman.

Kevin D. Murray, an Oldwick, N.J., counter-surveillance expert, said he received several calls from worried executives asking for sweeps of their offices and homes as soon as the Porsche incident surfaced. Mr. Murray said he handles 130 snooping investigations per year, generally charging between \$4,600 and \$24,000, depending on the scope of the case. His five-person operation finds devices in about 10% of the cases, a similar percentage to other firms.

Available, Affordable

The growing availability and affordability of digital surveillance equipment -- even primitive stuff such as baby monitors -- has caused mounting worries about spying, Mr. Murray says. Devices "that used to be super-duper a few years ago are ordinary now," he says. "There was a time when you had to know somebody or pay a lot of money to get the equipment. Now you can get a wireless camera for under \$100 -- tiny ones, too."

Indeed, for less than \$350 at spy shops and over the Internet, snoops can purchase a GPS-tracking device that is smaller than a pack of matches and includes a microphone. But because many telephones and computers are tied into network servers these days, some of the greatest threats come from malicious software and hacker attacks that reroute phone calls and steal

Behind success there's **EDS**
[SUCCESS STARTS HERE](#)

THE WALL STREET JOURNAL
GET THE ONLINE JOURNAL TODAY [Subscribe Now](#)

MORE FROM TODAY'S JOURNAL
 \$ Subscription may be required | [Subscribe Now](#)

PEOPLE WHO READ THIS...
 Also read these stories:

- ▶ WHAT'S NEWS**
- [Report: Iran Continues to Support Shiites](#)
 - [GM Slates Sweeping Rebates](#)
 - [SEC Aims to Rein In the Role of Ratings](#)
 - [United Will Furlough About 950 Pilots](#)
 - [Google to Offer Tool to Measure Web Hits](#)

MORE
▶ WHAT'S POPULAR

1. [Citigroup Plans Layoffs](#)
 2. [Opinion: Anti-Americanism Is Mostly Hype](#)
 3. [The Inside Scoop](#)
 4. [Google's Handset Plans Are Slowed](#)
 5. [Soros Now Warns of a 'Superbubble'](#)
- [MORE](#)

THINK BIGGER

NEW OPPORTUNITIES

Director of Finance
Robert Half Finance & Accounting - Toronto, ON, Canada

Director of Administration/Sales Operations
MetLife - Cranford, NJ

Government Contracts Accounting Director - Relo
Robert Half Finance & Accounting - BIRMINGHAM, AL

K12 Sales Executive, Business Intelligence
IBM - Eugene, OR

Account Executive
AON Corporation - SC

More Opportunities

THE WALL STREET JOURNAL
CareerJournal

computer passwords. Snoops install the software by sending messages with spyware attachments. Or they may steal sensitive data using programs or hardware to copy keystrokes entered onto a keyboard.

While there's anecdotal evidence that casual and malicious snooping is becoming more widespread, solid statistics are hard to come by. Many high-net-worth individuals and publicly traded companies try to keep incidents under wraps and don't report them to authorities, security experts say. The U.S. Department of Justice prosecutes only a handful of illegal-wiretapping cases annually.

Still, private-security companies say business is growing. Risk Control Strategies Inc., based in New York City, says sweeps have increased 25% in each of the past two years. It attributes the growth to a recent wave of mergers and plant closings that sometimes prompt attempts at insider trading and spying by anxious employees.

Companies also are increasingly worried about economic and industrial espionage by foreign governments and companies. Kroll Inc., a risk-control consulting company that is a unit of insurance brokerage [Marsh & McLennan Cos. Inc.](#), says inquiries in Japan have doubled in the past year. Associate Managing Director David Nagata, who is based in Tokyo, counsels visitors to have their hotel rooms swept for listening devices prior to check-in and make sure they're secured from unauthorized entry. For super-secret matters, he suggests closed-circuit cameras to monitor hallway traffic and an alarm that beeps when someone approaches the room.

Recorder in the Closet

Clyde Widrig, senior managing director for technical surveillance counter-measures at Risk Control Strategies, says his firm was hired recently by a Southern California law firm to sweep for stealth recording devices. In this case, an attorney had modified a conference-call telephone in the boardroom to pick up conversations and transmit them to a tape recorder hidden in a utility closet. Mr. Widrig, a former Los Angeles police detective, says the attorney was trying to discredit a rival in competition to become partner. Instead, the firm fired him after the recording device was discovered.

Security experts say there are some simple precautions that can be taken to prevent snooping. The easiest, of course, is to look for hidden cameras, which may be disguised as ordinary objects, such as fire sprinklers or smoke detectors. Also, don't leave cell phones and laptops where someone can take them to avoid tampering. Avoid using hotel telephones and wireless computer connections for sensitive communications. Finally, use the proper network firewalls and upgrade computers with the latest encryption and security software.

High-profile executives and celebrities may opt for counter-surveillance sweeps, but the service isn't cheap. Prices begin at about \$3,000 to \$5,000 for a private residence or small business, based on the complexity of the job.

During the sweeps, technicians inspect areas using thermal imaging cameras to search for hot spots that indicate concealed electronic circuits, such as transmitters hidden inside walls. They use spectrum analyzers to pick up video, voice and data transmissions. And they find eavesdropping equipment by using devices that flood an area with a high-frequency radio signal and listen for reflected signals from electronic components within the intercept device.

But sometimes, these elaborate measures are undone by executives chatting on unsecured cellphones with Bluetooth headsets and tapping on unencrypted laptops. Fred Burton, a counter-espionage expert at Stratfor Inc., suggests that companies tell executives, "You have to quit yakking on the cellphone because we're able to pick up what you're saying."

Counterintelligence

Some spying techniques and measures to avert them.

■ Keystroke-logging programs and hardware

How it works:

Copies keystrokes entered into a computer keyboard to monitor computer activity or obtain passwords. Software is installed manually or remotely via email attachments and rogue Web sites.

Countermeasures:

- Network firewalls block malicious content.
- Computer network security checks.

■ Wi-Fi interception

How it works:

Software is used to monitor wireless Internet communications.

Countermeasures:

- Encryption programs on computers make transmissions unreadable.
- Avoid Wi-Fi connections in hotels and public places for confidential communications.

■ GPS-tracking device or cellphone software

How it works:

Enables your whereabouts to be pinpointed.

Countermeasures:

GPS signal jamming devices, which are effective to about 160-feet away.

■ Hidden cameras, microphones and cellphones

How it works:

Transmitters allow eavesdroppers to listen in on confidential conversations; cameras capture digital images.

Countermeasures:

- Technical countersurveillance sweeps can detect video, voice and data transmissions using special equipment.
- Cellphone jammers can block calls up to 66-feet away.

Source: Security and countersurveillance experts

Write to M.P. McQueen at mp.mcqueen@wsj.com