The New York Times
nytimes.com

September 25, 2006

THE MEDIA EQUATION

An Obsession With Leaks and Plugs

By DAVID CARR

It's been a busy week for leaks, a particularly apt metaphor for the events at Hewlett-Packard and in a San Francisco courtroom. First, leaks tend to afflict ships that aren't seaworthy to begin with. Second, leaks — by definition a nasty surprise — tend to bring out the panicky worst in people.

At Hewlett-Packard, the company's leadership responded to leaks on its own corporate board by ordering all hands to grab buckets and immediately start bailing water — into the boat. For two years, with its chief ethics officer often riding point, the company commissioned a set of black ops that included internal witch hunts, surveillance and warrantless searches of reporters' phone records, all in an effort to zealously guard the image of their company

Mark V. Hurd, the chief executive of Hewlett-Packard, maintained on Friday that "the intent of the investigation was absolutely proper and appropriate." One head of a well-known security firm I spoke to called the mission "outrageous" and said that if he had been asked to participate in such a scheme, he would have backed slowly out of the room, making sure not to leave fingerprints on any of the documents.

Just up the road in San Francisco in the same week, Judge Jeffrey S. White of United States District Court ruled that Mark Fainaru-Wada and Lance Williams, the two reporters from The San Francisco Chronicle who broke open the baseball steroid scandal, should receive more prison time than any of the defendants in the Balco drug case for using secret grand jury testimony in their reporting and refusing to divulge their sources. (They are still free on appeal.) Never mind that they got an "attaboy" from the president of the United States for helping baseball right itself, the act of reporting has again been criminalized.

While the contemporary obsession with leaks and the willingness to go to any lengths to plug them is widespread, the tone was set in Washington. The current administration has responded to critical stories, including two that won Pulitzer Prizes, by going after sources.

After Dana Priest, a reporter for The Washington Post, revealed the operations of secret C.I.A. prisons, the administration found and fired a woman who was alleged to be a source. And the administration is still working on the identity of sources who may have leaked information to James Risen and Eric Lichtblau, reporters for The New York Times, for their series on the National Security Agency's program to listen to domestic phone calls. And we should not forget that upon the death of the investigative reporter Jack Anderson, the F.B.I. sought to obtain records of his sources, posthumously.

The government, of course, need not go to the fuss of pretexting phone records. It can use subpoenas. Although no hard numbers are available, Lucy A. Dalglish, executive director of the Reporters Committee for Freedom of the Press, said that subpoenas from the Justice Department for reporters had gone from nonexistent to dozens in a few short years, while efforts are under way in Congress, supported by the administration, to drastically toughen sanctions for violating prohibitions against divulging government secrets.

"We are in new territory here," Ms. Dalglish said. "My job has changed considerably in just the past three years. We've gone from giving reporters tips on how to avoid being named in a libel suit to telling them how to avoid going to jail for 18 months or being charged with espionage."

The ability to cultivate confidential sources is one of the building blocks of journalism. Without it, the media world would run on press releases. No one knows how many stories are going unreported, how many whistles going unblown, as a result of the increase in subpoenas. A lawyer for the Hearst newspapers told The San Francisco Chronicle that one investigation had already

collapsed because of the pervasive chill in the air.

Many reporters are now forced to conduct themselves like C.I.A. operatives, encoding files, shredding notes and switching cellphones. But technology also makes forensics on determining where leaks came from far easier.

Some years ago, I was working on an article about a major entertainment figure. When I was getting started, I was briefed by a young, enterprising reporter who suggested that in the course of doing the story, my computer would be hacked, my phone would be tapped and that I would be followed. I did my best to contain laughter, saying that I had worked on stories about wise guys, bad cops and corrupt politicians and had managed to avoid becoming a target.

But soon after I began the story, the subject displayed a real-time understanding of much of my reporting efforts. Was he psychic? Probably not, although I can't prove it. But just in case I didn't catch the implication, a year after I did the story, I had a discussion with the subject in which he displayed a very comprehensive knowledge of my personal history.

In a way, being worthy of counterintelligence is a compliment. There were some hurt feelings on the part of those technology beat reporters who were not deemed worth of being spied upon by Hewlett-Packard, like finding out you were left off Nixon's enemies list.

"Other reporters have joked that they are professionally jealous," said John Markoff, a Silicon Valley reporter for The New York Times. In addition to having his phone records obtained, he was the subject of a particularly hilarious link-analysis chart that Hewlett-Packard investigators produced trying to tie him to dissidents on the board.

It's all old hat for Mr. Markoff, a veteran technology reporter whose e-mail was hacked 10 years ago while he was pursuing a story.

"I'm struck by the absurdity of the act, the amount of cluelessness," he said. "There was a lot of thrashing, but not much thinking. A lot of people are deeply offended by the invasion of privacy, but from what I have seen over the years, the practice may be quite frequent."

It seems to be getting more frequent. Whether the aggrieved is the government or private industry, shooting the messenger has become a blood sport.

"Every company and organization has a reflexive reaction to bad press," said Mark Rasch, a lawyer specializing in computer crime and security matters who formerly worked for the Justice Department. "They always seem to think the problem is not the underlying facts, but that they are being written about."