

Privacy: up in the air

Companies and government both underestimate the threat posed by eavesdropping / **Simson L. Garfinkel**

IAST WEEK, THE New York Times published excerpts from a telephone conference call between Newt Gingrich and 50 of his most trusted friends in the House of Representatives. The phone call was recorded by a Florida couple who overheard the conference call on their police scanner, made a tape of the conversation and apparently gave it to Rep. Jim McDermott (D-Wash.), the leading Democratic member of the House Ethics Committee.

Since then, there's been a lot of talk about security and cellular phone calls, and how the new digital wireless phones are more difficult to tap.

All of the talk has missed a few important points having to do with history, policy and possibility.

For years it has been widely known cellular telephone calls can easily be overheard with low-cost radio scanners available both within the United States and abroad.

Many famous people, from Prince Charles to ex-Gov. Douglas Wilder of Virginia, had their phone calls overheard and then published.

In the mid-1980s a number of radio stations entertained their

listeners by recording and rebroadcasting cell calls.

Eavesdropping of this sort is going on everywhere. In Silicon Valley, there are paid eavesdroppers who have listening stations close to Highway 101. It's a good source for information about the computer industry.

But cellular telephone calls didn't have to be so easy to intercept.

Back in the late 1970s and early 1980, when the cellular phone system was being designed and first deployed, the companies backing the technology could have added extra circuits, which would have scrambled any phone conversation sent through the air.

The industry decided against using such privacy-enhancing technology — the circuits would have added too much money to the cost of each phone. Likewise, the threat of eavesdropping wasn't really taken seriously.

After all, AT&T, which invented the original cellular systems, predicted there would be just a million or so car phones in the United States by the year 2000.

Today, when cell phones are being given away for a penny, it's easy to see that the industry made a mistake.

Unfortunately, the mistake of

deploying systems that are fundamentally insecure is a mistake that's been repeated over the past 20 years. Even today, companies continue to underestimate the threat of eavesdropping.

For example, Microsoft's Internet mail client, released with Internet Explorer 3.0, sends your user name and password clearly over the Net whenever you pick up your mail. Anybody listening can steal your password, as well as your data.

Businesses aren't the only bad guys here. Another stumbling block to building communications systems that are harder to tap has been the Clinton administration, which has done its best to prevent the widespread deployment of cryptography, the only real way to protect information that's sent through the airwaves or transmitted over a wire.

Encryption is a technique for mathematically scrambling information so it can only be unscrambled by the intended recipient.

Most people who want to use encryption are upright, law-abiding citizens. There are companies that want to do business overseas and are worried their communications might be intercepted by rival firms (or even by the government of the host country). There are lovers who wish to communicate privately, without the chance their

messages will be intercepted and seen or heard by somebody else. There are even politicians who want to discuss strategy.

But the Clinton administration is worried encryption will also be used by right-wing militias, terrorists, drug dealers and people trying to use the Internet to exchange child pornography. The administration says it needs to be able to eavesdrop on these groups, and so it has fought against the widespread adoption of strong cryptography.

In international organizations such as the Organization for Economic Cooperation and Development, the administration is lobbying our trading partners to do the same.

Lately, the Clinton administration has been advocating a system called key escrow or key recovery. These systems would let Americans use strong encryption, but would assure that the government could get a copy of the keys if it wished.

Republicans should be especially fearful of the Clinton administration's encryption proposals, says Bryan Hendricks, publisher of the Washington-based Privacy Times.

When you are talking key escrow, in practical terms, you are talking about the key being held by the Democratically controlled FBI.

But Hendricks hopes the intercepted Gingrich phone call will show Republicans that what's really

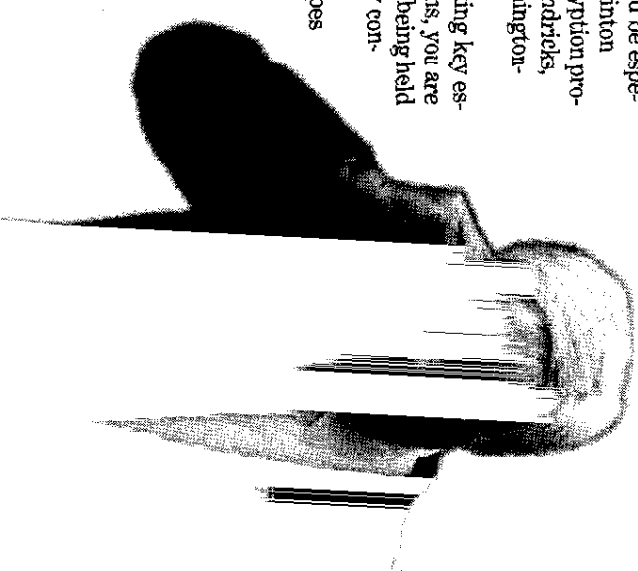
needed is a privacy czar.

If members of Congress were constantly hearing from an independent privacy commissioner on all of these issues, privacy would enter into the equation when these sorts of controversies and scandals arise.

Perhaps more important, a privacy commissioner would be charged with making sure the nation's communications systems are equipped with technology for protecting privacy from the start.

Without the technology, there's just too much incentive for people to go on fishing expeditions, trying to see what sort of juicy communique they might find.

Technology writer Simson L. Garfinkel can be reached at plaggar@simson.net.



A cellular telephone call made by Newt Gingrich to other members of the House of Representatives was intercepted and recorded recently by a Florida couple.