& TECHNOLOGY: BACK PAGE OF THIS SECTION ▶

BUSINESS

MARKETS ◆ HIGH TECH ◆ ECONOMY

TALKING BUSINESS

"Who wouldn't love to have 100 percent of the automobile industry or the phone industry or whatever?"

DAVE OTTO, analyst, about SBC's planned takeover of Pacific Telesis

Peeking in the back door

■ E-mail: Business version of encryption program will open up 'private' communications.

BY SIMSON L. GARFINKEL
Special to the Mercury News

Business users of a popular computer encryption program that promises to keep electronic mail absolutely private may soon be in for a rude surprise: optional eavesdropping by the boss.

Viacrypt, an Arizona company that sells the popular program Pretty Good Privacy, or PGP, last month announced a new version tailored for businesses. The new program allows companies to "decrypt" — and then read — information sent to or received by employees without the employees' knowledge or consent.

The new version, Viacrypt PGP/Business Edition, has infuriated privacy advocates and the program's author, who says the new version violates the very reason he created PGP in the first place.

"Employees have privacy rights even in the on-line workplace," said Marc Rotenberg of the Electronic Privacy Information Center in Washington, D.C. "PGP is the gold standard for e-mail privacy.

"Viacrypt has taken PGP and done what the U.S. government could not — build in surveillance capability — and has damaged the good reputation of a product that symbolizes the privacy of personal communications."

The PGP program, developed by Philip R. Zimmermann in 1991, has become a cause celebre among privacy rights activists in recent years. The program allows a computer user to encrypt electronic mail and other files so they cannot be deciphered by anyone other than the intended recipient. Using mathematical equations with very long numbers, PGP's encryption system is so good that even the U.S. government's National Security Agency is helpless when given the task of decoding information PGP has protected.

But while that's fine for personal

See PRIVACY, Page 3E

TUESDAY FOCUS

San Jose Mercury News • **Business** • Tuesday, April 2, 1996

Viacrypt opens back door to privacy

PRIVACY

from Page 1E

use, PGP's strength has been a problem for business users, said Leonard E. Mikus, president of Lemcom Systems, Inc., Viacrypt's parent company.

"Employees have heart attacks. They have accidents. Businesses have a real need to get at encrypted information," he said.

PGP uses two encryption "keys" to unlock coded information. A "public" key is used for encrypting messages destined for a particular user. A "secret" key is used by the recipient to decode the message. The secret key is also used for digital signatures, a technique that allows a person to electronically "sign" a message so its authenticity can be proven.

Normally, users keep their secret keys to themselves but distribute their public keys to others with whom they correspond.

"Let me tell you what's happened with most of the corporations," said Mikus. "When they get standard PGP, they either require that the employee give them a copy (of the employee's secret key), or they generate the keys for the employee and give the employee the personal component. That's not good: The company can forge the employee's signature that way ... One of the main motivations for the Business Edition is to clean that up."

Viacrypt's Business Edition gives each user two secret keys: one for encryption, a second for creating electronic signatures. The business can keep a copy of the employee's encryption key, so that any information destined for or sent out by that employee can be monitored. Alternatively, the business can simply create keys for the user, or even disable encryption entirely, meaning the worker can use PGP only for digital signatures.

"In some places, they have no need (for such restrictions)," said Mikus. "In other places, such as financial institutions, they don't use our product unless they are guaranteed access to encrypted information."

The new version allows each business to set its own encryption policy, he said.

The version of PGP that is still freely available on the Internet for non-commercial use does not have the employer eavesdropping capability, which is frequently called a "back door."

An employee's right to privacy is nebulous at best. The Electronic Communications Privacy Act of 1986 specifically allows companies to monitor the electronic mail of their own employees. That has not stopped Zimmermann from complaining loudly about the PGP name being used in a product that allows someone other than the author or the intended recipient access to information. Viacrypt owns the licensing rights to sell the commercial versions of PGP.

"PGP does not stand for back doors," said Zimmermann. "I don't mind if they sell a program that has a back door in it, but they shouldn't call it PGP."

Viacrypt's use of the letters "PGP" in a program that takes a person's privacy out of his or her own hands could violate Zimmermann's PGP trademark.

"One of the things that trademark owners have is not only the right but the obligation to police other uses of the mark," said Pamela Samuelson, a visiting professor at Cornell University Law School and an expert on intellectual property law. Uses of trademarks must be "consistent with the product and goodwill associated to that product," she said.

"If your employer can read your mail anytime he wants, without your permission, that goes against the spirit of the PGP trademark," said Zimmermann.

Fighte