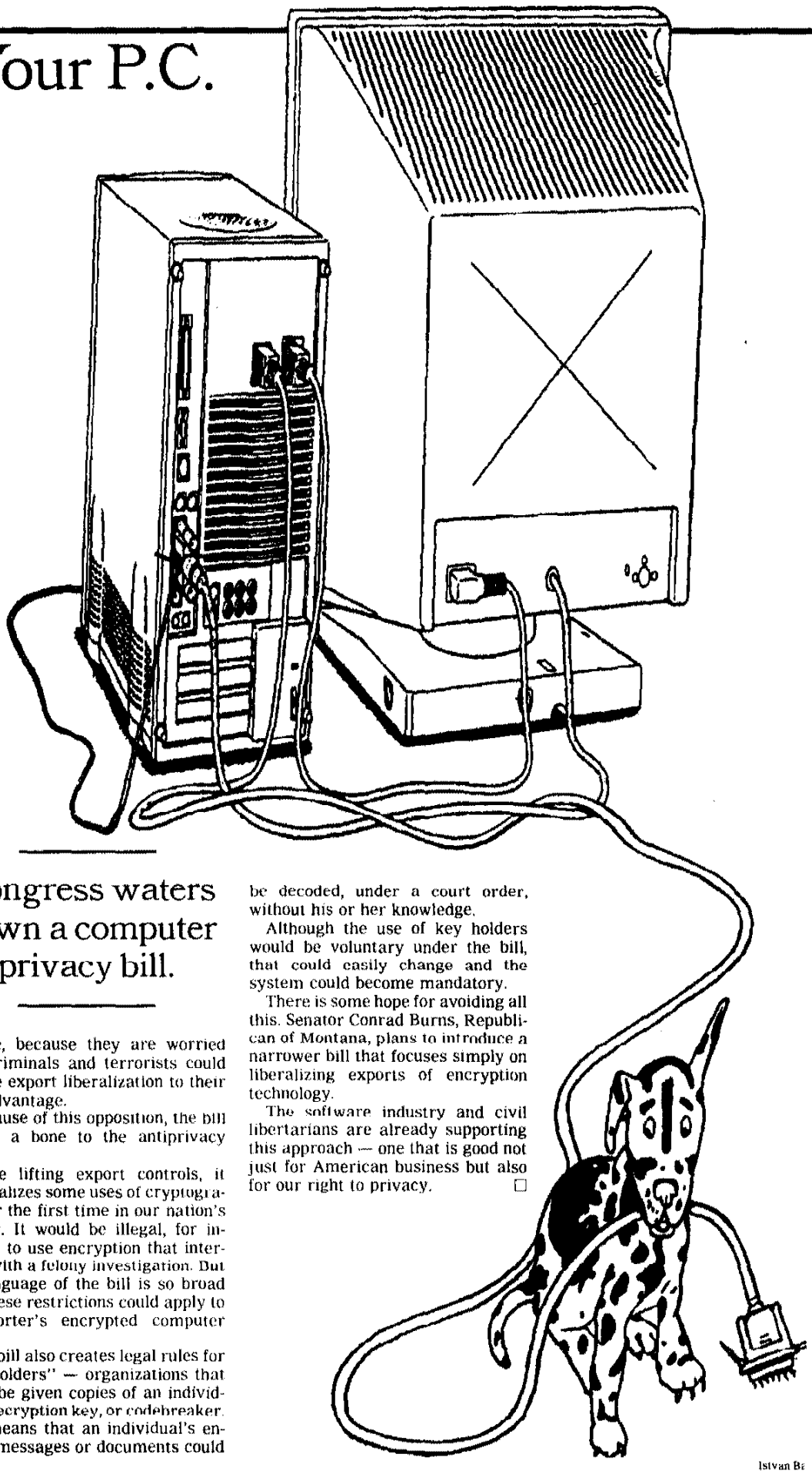
Peeking at Your P.C.

By Simson L. Garfinkel



Congress waters down a computer privacy bill.

CAMBRIDGE, Mass.

As more Americans use electronic mail, buy products over the Internet and keep their most personal records on desktop computers, there is increasing demand for cryptography software that can insure the privacy of personal electronic communication.

This technology already exists, but the Government, through export-control regulations, effectively bars citizens from using it.

The Government classifies encryption software as munitions, because foreign countries can use such programs to hide their communications during times of war. To prevent this, American companies are largely prohibited from selling to foreign customers any programs that include strong coding features.

Unfortunately, that has stifled the domestic market.

Encryption-software developers find it too expensive to create two versions of their programs — one with strong cryptography for domestic use and one with cryptography that is weak enough for export. So in the United States, developers sell only the weaker cryptography software.

Last month, a bipartisan group of lawmakers introduced "The Encrypted Communications Privacy Act of 1996" to combat this problem. But while this measure would increase the availability of good cryptography at home, it would limit our freedoms in other ways.

The act would legalize the export of any mass-market software if similar technology is already available overseas. This would put an end to the futility of forbidding such exports at a time when cryptography technology is increasingly available around the globe — in libraries and on the Internet. Indeed, the Software Publishers Association says that the main result of the export regulations simply has been to shift the overseas marketing of military-grade cryptography to foreign companies.

So although the new bill would still prohibit American companies from exporting innovative programs, it would at least allow them to compete with foreign companies on an equal footing.

However, the Clinton Administration and others oppose this minor change, because they are worried that criminals and terrorists could use the export liberalization to their own advantage.

Because of this opposition, the bill throws a bone to the antiprivacy forces.

While lifting export controls, it criminalizes some uses of cryptography for the first time in our nation's history. It would be illegal, for instance, to use encryption that interferes with a felony investigation. But the language of the bill is so broad that these restrictions could apply to a reporter's encrypted computer files.

The bill also creates legal rules for "key holders" — organizations that would be given copies of an individual's decryption key, or codebreaker. This means that an individual's encoded messages or documents could be decoded, under a court order, without his or her knowledge.

Although the use of key holders would be voluntary under the bill, that could easily change and the system could become mandatory.

There is some hope for avoiding all this. Senator Conrad Burns, Republican of Montana, plans to introduce a narrower bill that focuses simply on liberalizing exports of encryption technology.

The software industry and civil libertarians are already supporting this approach — one that is good not just for American business but also for our right to privacy. □

Simson L. Garfinkel is the author of the book "PGP: Pretty Good Privacy."

Istvan Ba