Encryption is Vital to the Net

BY RICHARD A. GEPHARDT

THE Clinton administration's recent call for a "non-regulatory, market-oriented" approach to promoting Internet commerce includes many constructive initiatives. However, if we are to realize the full potential of the Internet, we must also end the outdated restrictions on U.S. exports of encryption products.

Encryption, which encodes electronic messages so that only a recipient with the ability to decode the message can read it, is vital to the future of Internet commerce. It prevents crime by keeping hackers from reading your e-mail or stooling your credit card numbers. It helps companies protect trade secrets. As more information flows over the open networks that constitute the Internet, people increasingly need encryption to keep their information secure.

Because encryption is not restricted domestically, you would think American companies would be global leaders in world markets. But often they aren't allowed to compete. Fearing the availability of encryption abroad could make it more difficult for the U.S. government to intercept the communications of criminals and gather intelligence, the current and past Administrations have chosen to maintain strict export controls on encryption. The level of encryption U.S. companies are permitted to export is now so weak that a college hacker can break it in less than four hours.

If export controls could keep encryption from criminals, controls would make sense. But U.S. self-restraint has simply encouraged foreign producers of strong encryption, who are not covered by export limits, to fill the vacuum. Hundreds of strong encryption products, many developed in countries like Canada, Ireland, Germany and Russia, are increasingly available abroad. And as foreign competitors use their advantage in encryption to win more high-tech sales, we lose jobs.

The National Research Council's blue-ribbon panel on encryption policy recently warned that "foreign competition could emerge at a level significant enough to damage the present U.S. world leadership" in the software industry. Such damage could jeopardize hundreds of thousands of high-paying jobs. It could also undermine our national security, according to the Council, by making it harder for the U.S. government to keep abreast of

evolving encryption technology in the future. The Council endorsed a relaxation of export controls in order to maintain the U.S. lead in this vital sector.

The Administration has proposed a "key recovery" system to require users to make available to governments the "keys"' to decode their private communications. But giving governments worldwide ready access to individuals' private information and to corporate secrets raises difficult issues. Will U.S. firms operating in China be forced to trust that government with the keys to their trade secrets? Will human rights groups abroad, where U.S. constitutional protections do not apply, be forced to give authoritarian governments the keys to their membership lists? Can we really expect criminals to give up their keys so that they may be made available to the government?

Key recovery won't work unless the many countries that produce encryption adopt it. Otherwise criminals could still obtain encryption from non-complying countries. But countries like Germany have refused to support key recovery. Indeed, they have a strong economic incentive to resist. As long as the international disagreements persist and we hog-tie our industry, their's will enjoy an advantage in world markets.

The National Research Council urged a balanced approach to this problem: improve security on the Internet and prevent crime by relaxing exports controls and allowing U.S. exporters to meet the competition. Maintain robust controls against rogue nations. Impose penalties for misusing encryption to commit crime. And invest in additional technical capabilities to help our intelligence agencies adjust to the information age.

Led by Members like Congresswoman Zoe Lofgren, D-San Jose, more than 250 Democrats and Republicans in the House of Representatives -- myself included -- have joined in support of the Security and Freedom through Encryption (SAFE) bill to relax export controls and advance many of the recommendations of the National Research Council.

With growing support, the SAFE bill makes it clear that the Congress will not tolerate the continued shackling of our high-tech sector. We are willing to work with all sides to develop a consensus on a workable, market-oriented approach that can advance our law enforcement interests and win international acceptance. But we aren't willing to simply watch the current stalemate continue and keep U.S. industry on the sidelines. It is

time to move forward and modernize our export policies for the information age.

Rep. Richard A. Gephardt, D-Mo., is the House Democratic leader.