

THE VICE PRESIDENT  
WASHINGTON

July 20, 1994

The Honorable Maria Cantwell House of Representatives Washington, DC  
20515

"Dear Maria,

"I write today to express my sincere appreciation of your efforts to move the national debate forward on the issue of information security and export controls. I share your strong conviction for the need to develop a comprehensive policy regarding encryption, incorporating an export policy that does not disadvantage American software companies in world markets while preserving our law enforcement and national security goals.

"As you know, the Administration disagrees with you on the extent to which existing controls are harming U.S. industry in the short run and the extent to which their immediate relaxation would affect national security. For that reason we have supported a five-month Presidential study. In conducting this study, I want to assure you that the Administration will use the best available resources of the federal government. This will include the active participation of the National Economic Council and the Department of Commerce. In addition, consistent with the Senate-passed language, the first study will be completed within 150 days of passage of the Export Administration Act reauthorization bill, with the second study to be completed within one year after the completion of the first. I want to personally assure you that we will reassess our existing export controls based on the results of these studies. Moreover, all programs with encryption that can be exported today will continue to be exportable.

"On the other hand, we agree that we need to take action this year to ensure that over time American companies are able to include information security features in their program in order to maintain their international competitiveness. We can achieve this by entering into a new phase of cooperation among government, industry representatives and privacy advocates with a goal of trying to develop a key escrow encryption system that will provide strong encryption, be acceptable to computer users worldwide, and address our national security needs as well.

"Key escrow encryption offers a very effective way to

accomplish our mutual goals. That is why the Administration adopted the key escrow encryption standard in the "Clipper Chip" to provide very secure encryption for telephone communications while preserving the ability for law enforcement and national security. But the Clipper Chip is an approved federal standard for telephone communication and not for computer networks and video networks. For that reason, we are working with industry to investigate other technologies for these applications.

"The administration understands the concerns that industry has regarding the Clipper Chip. We welcome the opportunity to work with industry to design a more versatile, less expensive system. Such a key escrow scheme would be implementable in software, firmware or hardware, or any combination thereof, would not rely on a classified algorithm, would be voluntary, and would be exportable. While there are many severe challenges to developing such a system, we are committed to a diligent effort with industry and academics to achieve such a system. We welcome your offer to assist us in furthering this effort.

"We also want to assure users of key escrow encryption products that they will not be subject to unauthorized electronic surveillance. As we have done with the Clipper Chip, future key escrow schemes must contain safeguards to provide for key disclosure only under legal authorization and should have audit procedures to ensure the integrity of the system. Escrow holders should be strictly liable for releasing keys without legal authorization.

"We also recognize that a new key escrow encryption system must permit the use of private-sector key escrow agents as one option. It is also possible that as key escrow encryption technology spreads, companies may establish layered escrowing services for their own products. Having a number of escrow agents would give individuals and businesses more choice and flexibility in meeting their needs for secure communications.

"I assure you the President and I are acutely aware of the need to balance economic and privacy needs with law enforcement and national security. This is not an easy task, I think that our approach offers the best opportunity to strike an appropriate balance. I am looking forward to working with you and others who share our interest in developing a comprehensive national policy on encryption. I am convinced that our cooperative endeavors will open new creative solutions to this critical problems."

Sincerely  
Al Gore