Ed,

It's on the web -- info and URL below.

Dorothy

----- Begin Included Message -----
of the Clinton Administration's invasive and unworkable "Clipper Chip" and "Clipper II" key escrow policies. Under the guise of promoting so-called "voluntary" encryption standards, these Administration efforts have sought to use export controls to compel the adoption of key escrow encryption domestically, and have left Internet users without adequate privacy and security.

By relaxing export controls on "generally available" cryptographic applications such as PGP, popular Web browsers, and other programs, the Encrypted Communications Privacy Act of 1996 would encourage the development and use of strong privacy protecting technologies. Major provisions of the legislation would:

* Ease export controls on encryption products, allowing the export of 'mass market' or 'generally available' cryptography. This would include products such as PGP or many of the popular Web browser programs.

* Affirm the right of Americans to use any encryption domestically. The bills explicitly prohibit the government from imposing any limits on the domestic use or sale of encryption.

* (Senate version only) Provide protections to those who choose to store their encryption keys with third parties by creating criminal and civil penalties for the unauthorized disclosure of keys and strict requirements for law enforcement access. The bill does not in any way affect the ability of any person to use encryption without a key escrow function.

The legislation also contains several provisions which CDT believes require further clarification and consideration, including controversial language that would create a new federal crime for the use of encryption to willfully obstruct a law enforcement investigation. CDT will work with Senators Leahy and Burns and Representatives Goodlatte, Eshoo, and other interested members to address these concerns as the bill makes its way through the legislative process.

The full text of both the House and Senate versions of the bills, along with other relevant background information, is available on CDT's Crypto Issues World Wide Web page:

http://www.cdt.org/crypto/

CDT believes that the House and Senate encryption bills are an important step forward in the ongoing attempts to build better security into the information infrastructure through the widespread availability of encryption. Congressional action is particularly welcome as the Administration has continued to impose a flawed approach to encryption based upon export controls, key length limits, and key escrow policies all aimed at slowing the adoption of strong cryptography in the U.S. and throughout the world.

While CDT believes improvements can be made in both bills, they establish a solid framework for building a comprehensive, global cryptography policy. CDT believes the bills deserve careful consideration and support. We look
forward to working with Senator Leahy, Senator Burns, Rep. Goodlatte, Rep. Eshoo, individual Internet users, public interest advocates, and the computer and communications industry to develop a cryptography policy that protects privacy, security, and competitiveness on the Global Information Infrastructure.

SUMMARY OF THE LEGISLATION: WHAT THE BILLS WOULD DO

The House and Senate bills both modify Title 18 of the U.S. Code to clarify the status of encrypted communications, access to those communications by law enforcement, and the liability of third-party key holders. The bills would:

* SIGNIFICANTLY EASE EXPORT CONTROLS: The bills would remove all export restrictions on "mass market" or publicly accessible encryption software and similar hardware -- that is, products that are generally available to the public and sold for installation "as is," or that are in the public domain such as PGP or some popular web browsers. (For example, products commercially available "off the rack," or freely available to the public via the Internet, would all be exportable.) Other encryption hardware would be exportable to countries where hardware with similar capabilities is already commercially available. The bills also allow export of other encryption software if it is currently exportable under law for use by foreign financial institutions.

* PROHIBIT ANY RESTRICTION ON THE DOMESTIC USE OR SALE OF ENCRYPTION: The bills would affirmatively prohibit any government restrictions or attempts to mandate the domestic sale or use of any type of encryption.

* IMPOSE CIVIL AND CRIMINAL LIABILITY FOR UNAUTHORIZED KEY DISCLOSURES: (Senate Version Only) The Senate bill would lay down privacy guidelines to protect those users who choose to store their keys with third parties. The bill would impose civil and criminal penalties for the unauthorized release of decryption keys or other decryption assistance by third parties who individuals have entrusted with their keys. No privacy protections and only limited restrictions for law enforcement access currently exist for those who choose to store their keys with trusted third parties.

* PROVIDE LIMITS FOR ACCESS TO KEYS BY LAW ENFORCEMENT: (Senate Version Only) The Senate bill would also spell out limits and guidelines for law enforcement access to the keys of those users who have chosen to store their keys with third parties. Today, encryption keys held by third parties could be released to law enforcement with nothing more than a subpoena. Under the Senate bill, third parties could only provide assistance to law enforcement in decrypting communications if presented with a court order. The bill also limits the scope and duration of such assistance. Decryption keys for stored communications could be disclosed with a proper court order or subpoena.

* ESTABLISH A BROAD "PERSONAL USE EXEMPTION" FOR U.S. TRAVELERS: The bills would allow U.S. persons to use any form of encryption in a foreign country, establishing a less restrictive form of the "personal
use exemption" recently published by the State Department. The provision is intended to accommodate "U.S. citizens and permanent residents who have the need to temporarily export encryption products when leaving the U.S. for brief periods of time". While the intent of this provision is clear, CDT believes that the language of the bill should be further clarified.

*PROHIBIT THE USE OF ENCRYPTION TO CONCEAL THE COMMISSION OF A FELONY: Finally, the bills would criminalize the use of encryption to willfully obstruct justice. Anyone who "willfully endeavors" to use encryption for the purpose of obstructing, impeding, or preventing the communication to a law enforcement officer of information relating to a Federal felony would be subject to criminal penalties. CDT believes this new federal crime is unnecessary since it duplicates obstruction of justice crimes that are already available to prosecutors, and is unwise since it might be interpreted to discriminate against users of encryption.

BACKGROUND - BILLS ADDRESS LONG-STANDING FRUSTRATIONS WITH U.S. ENCRYPTION POLICY

Congressional action comes as Clinton Administration encryption restrictions continue to jeopardize the security of computer users. Encryption tools, which scramble electronic communications and data, are widely viewed as the key to providing security and privacy and encourage commerce on the Global Information Infrastructure.

Individuals need encryption in order to trust the GII with confidential data such as financial transactions, medical records, or private communications. Businesses need encryption to provide individuals with privacy protections they need and to protect their own proprietary information as it flows across vulnerable global networks. The lack of good encryption today has left computer users vulnerable to the prying eyes of hackers, corporate competitors, and even foreign governments.

Current Administration policy restricts the export of "strong" encryption hardware or software products with keys greater than 40 bits long. (The length of encryption "keys" is often used to indicate the security of a system.) Export controls actually influence the entire GII -- both domestically and internationally -- due to the difficulty of distributing and interoperating products with different strengths of encryption. The level of security permitted under the export controls, and hence the level of security largely available to domestic users as well, has been judged woefully inadequate by many experts. Even the most recent Administration "Clipper II" proposals would only allow the export of moderately stronger encryption, and then only with "key escrow" restrictions to guarantee U.S. government access to individual keys -- restrictions which raise real Constitutional issues and are bound to fail in the competitive international marketplace.

In recent months, groups from across the political spectrum have increasingly criticized the Clinton Administration's restrictive export controls. In November 40 companies, trade associations, and public interest groups wrote to Vice President Gore calling the latest Administration proposals flawed and inadequate. Last month a report by the CEOs of 13
leading U.S. technology companies found that U.S. industry stands to lose up to $60 billion dollars per year by the year 2000 due to restrictions on the export of cryptography. And several weeks ago a group of noted computer security experts released a report calling for the deployment of dramatically longer encryption key lengths of at least 75 to 90 bits.

The House and Senate bills give voice to this growing drumbeat of criticism demanding a radical departure from the flawed approach of the Clinton Administration's current encryption policies. CDT looks forward to working with members of Congress to push for a more comprehensive U.S. encryption policy that reflects the privacy and security needs of computer users.

FOR MORE INFORMATION

More information on the cryptography policy debate, including the text of the Senate and House bills, is available on CDT's Cryptography Issues Web Page:

http://www.cdt.org/crypto/

For More Information Contact:

Center for Democracy and Technology +1.202.637.9800
Daniel Weitzner, Deputy Director <djw@cdt.org>
Alan Davidson, Staff Counsel <abd@cdt.org>

(2) SUBSCRIPTION INFORMATION

Be sure you are up to date on the latest public policy issues affecting civil liberties online and how they will affect you! Subscribe to the CDT Policy Post news distribution list. CDT Policy Posts, the regular news publication of the Center For Democracy and Technology, are received by more than 9,000 Internet users, industry leaders, policy makers and activists, and have become the leading source for information about critical free speech and privacy issues affecting the Internet and other interactive communications media.

To subscribe to CDT's Policy Post list, send mail to

    policy-posts-request@cdt.org

with a subject:

    subscribe policy-posts

If you ever wish to remove yourself from the list, send mail to the above address with a subject of:

    unsubscribe policy-posts

(3) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US
The Center for Democracy and Technology is a non-profit public interest organization based in Washington, DC. The Center's mission is to develop and advocate public policies that advance democratic values and constitutional civil liberties in new computer and communications technologies.

Contacting us:

General information: info@cdt.org
World Wide Web: URL:http://www.cdt.org/

Snail Mail: The Center for Democracy and Technology
1634 Eye Street NW * Suite 1100 * Washington, DC 20006
(v) +1.202.637.9800 * (f) +1.202.637.0968

----- End Included Message -----

Printed for eaf@xom.hq.af.mil (Edward Feigenbaum)