

AMERICAN CIVIL LIBERTIES UNION

WASHINGTON OFFICE

November 1, 1985

Mr. David Chaum
Centre for Mathematics and Computer Science
P.O. Box 4079
1009 AB Amsterdam

Dear Mr. Chaum:

Thank you for sending me a most interesting article. A society of individuals and organizations that would expend the time and resources to use a series of "digital pseudonyms" to avoid data linkage does not in my opinion make big brother obsolete but acts on the assumption that big brother is ever present. I view your system as a form of societal paranoia.

As a matter of principle, we are working to enact formal legal protections for individual privacy rather than relying on technical solutions. We want to assume a society of law which respects legal limits rather than a society that will disobey the law, requiring citizens to depend on technical solutions. e.g. require a judicial warrant for government interception of data communications rather than encrypt all messages on the assumption that regardless of the law, the government will abuse its power and invade privacy.

As a matter of practicality, I do not think your system offers much hope for privacy. First, the trend toward universal identifiers is as much a movement generated by government or industry's desire to keep track of all citizens as it is by citizens seeking simplicity and convenience in all transactions. At best, your system would benefit the sophisticated and most would opt for simplicity. The poor and the undereducated would never use or benefit from it.

Finally, where there's a will, there's a way. If government wants to link data bases, it will, by law, require the disclosure of various individual pseudonyms used by citizens or prohibit it for data bases which the government wants to link. Since corporations make money by trading commercial lists with one another, they will never adopt the system or if it is adopted, will use "fine print" contracts to permit selling various codes used by their customers to other firms.

122 Maryland Avenue, NE
Washington, DC 20002

National Headquarters
132 West 43rd Street
New York, NY 10036
(212) 944-9800

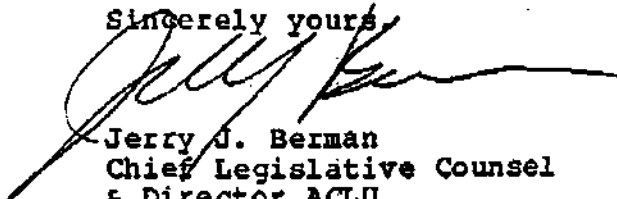
Norman Dorsen
PRESIDENT

Ira Glasser
EXECUTIVE DIRECTOR

Eleanor Holmes Norton
CHAIR
NATIONAL ADVISORY COUNCIL

The solution remains law, policy, and consensus about limits on government or corporate intrusion into areas of individual autonomy. Technique can be used to enforce that consensus or to override it. It cannot be used as a substitute for such consensus.

Sincerely yours,



Jerry J. Berman
Chief Legislative Counsel
& Director ACLU
Privacy Technology Project

cc: John Shattuck

DIGITAL PRIVACY AND SECURITY WORKING GROUP

1001 G Street, NW
Suite 950 East
Washington, DC 20001

Jerry Berman 202/347-5400
Leah Gurowitz 202/393-1010

December 6, 1993

The President
The White House
Washington, DC 20500

Dear Mr. President:

On April 16, 1993, you initiated a broad industry/government review of privacy and cryptography policies at the same time that the Administration unveiled its Clipper Chip proposal. The Digital Privacy and Security Working Group -- a coalition of over 50 communications and computer companies and associations, and consumer and privacy advocates -- has been working with members of your Administration to develop policies which will reflect the realities of the digital information age, the need to provide individuals at work and home with information security and privacy, and the importance of preserving American competitiveness.

The Digital Privacy and Security Working Group is committed to the proposition that computer users worldwide should be able to choose their encryption programs and products, and that American programs and products should be allowed to compete in the world marketplace. In our discussions with Administration officials, we have expressed the Coalition's tentative acceptance of the Clipper Chip's encryption scheme (as announced on April 16, 1993), but only if it is available as a voluntary alternative to widely-available, commercially-accepted, encryption programs and products.

Thus, we applaud repeated statements by Administration officials that there is no intent to make the Clipper Chip mandatory. One key indication of whether the choice of encryption regimes will be truly voluntary, however, is the ability of American companies to export computer programs and products employing other strong encryption algorithms (e.g. DES and RC2/RC4 at comparable strengths) demanded by customers worldwide. In this regard, we commend to your attention legislation introduced by Rep. Maria Cantwell (H.R. 3627) that would liberalize existing export controls on software with encryption capabilities. Of course, such legislation would not be necessary if the Administration acts to accomplish such export control liberalization on its own. As part of your on-going encryption review and decision-making, we strongly urge you to do so.

As your Administration concludes its review of this issue, representatives of the Digital Privacy and Security Working Group remain available to meet with Administration officials at any time.

Sincerely,

American Civil Liberties Union IBM
Apple Computer, Inc. Information Industry Association
Business Software Alliance Information Technology Association of
America
Committee on Communications and
Information Policy, IEEE-USA Iris Associates, Inc.
Computer and Business Equipment Lotus Development Corporation
Manufacturers Association
Microsoft Corporation
Crest Industries, Inc. Oracle Corporation
Digital Equipment Corporation
Prodigy Services Company
EDUCOM Software Publishers Association
Electronic Frontier Foundation
Sun Microsystems, Inc.
Electronic Messaging Association
Telecommunications Industry Association
GKI Cryptek Division Trusted Information Systems
Hewlett-Packard Company

cc: John Podesta, Office of the President
George Tenet, National Security Council
Mike Nelson, Office of Science and Technology Policy
Ray Kammer, National Institute of Standards and Technology
Steve Aoki, National Security Council
Geoff Greiveldinger, Department of Justice

This document and others on related topics are archived at [ftp.eff.org](ftp://ftp.eff.org/~ftp/pub/eff/crypto-policy),
~ftp/pub/eff/crypto-policy.

OUR RESPONSE TO THE EFF LTR

December 8, 1993

The President
The White House
Washington, DC 20500

Dear Mr. President:

We are writing to you regarding the Clipper cryptography proposal now under consideration by the White House and a letter you may have received about the proposal from a group called the "Digital Privacy and Security Working Group."

This group wrote to you recently and expressed their "tentative acceptance" of the Clipper Chip encryption scheme. We disagree with their views. This group has made a grave mistake and does not speak for the many users of computer networks and developers of network services who have vigorously opposed this proposal.

We are very much concerned about the Clipper proposal. At its core is the dubious premise that the government should have the authority to design communications networks that facilitate wire surveillance. The plan was developed in secret by the National Security Agency over the objection of U.S. firms, professional associations and public interest organizations. Key details about the proposal remain classified.

This proposal must not be endorsed. The development of open, unclassified standards is critical for the future of the nation's communications infrastructure. Progress and innovation depend on the free exchange of scientific and technical information. It is essential to the integrity of the scientific process that standards are openly created and available for public review.

There is also a great need to ensure that future networks are designed with the highest levels of privacy and security possible. As our country becomes ever more dependent on the high-speed network, the need for secure systems will only increase. The Clipper proposal purposefully cripples the security of the network and reduces the privacy protection that users could otherwise obtain.

There is another still more serious problem with the Clipper proposal. An agency with the authority to conduct wiretaps must not be allowed to impose technical standards to facilitate wire surveillance.

The President
December 8, 1993
Page two

The threat to Constitutional democracy is clear. A system of checks and balances is essential to ensure that the powerful investigative tools of government are properly controlled.

We have followed the development of this proposal with great concern. We have testified before Congressional committees. We have appeared before agency panels, provided reports on wire surveillance, and debated the former FBI Director on national television. We have also sponsored conferences with full participation from across the federal government. We believe that the best policies will result from an open and unrestricted exchange of views.

It is our assessment that you must not permit adoption of the Clipper technical standard, even on a voluntary basis. At a time when the country should be moving toward open standards designed for commercial networks, the Clipper proposal asks future users of the nation's information infrastructure to accept a standard intended for the Cold War era. It is a backward-looking plan that serves neither the interests of the American people nor American business.

The adoption of the Clipper proposal would also ratify an unlawful process that has undermined the authority of Congress and weakened the mechanisms of government accountability. The proper authority for the development of this standard never rested with the NSA. Under the Computer Security Act of 1987, it was a civilian agency that was to develop appropriate standards for the nation's commercial networks. Through a series of secret executive orders, the NSA usurped the authority of the National Institute of Standards and Technology, substituted its own proposal for those of NIST, and effectively derailed this important policy process.

When the computer user community had the opportunity to voice its position on this proposal, it rejected the plan overwhelmingly. The notice and comment process conducted by the Department of Commerce earlier this year resulted in nearly uniform opposition to the Clipper proposal. It would be hard to find a technical standard more disliked by the potential user community.

While we support the relaxation of export controls on cryptography, we are not willing to concede to the NSA the right to develop secret standards. It is only because the National Security Agency also exerts influence on export control policy that the Digital Privacy coalition is prepared to endorse the Clipper standard in exchange for new opportunities to market products. It may be a good deal for

The President
December 8, 1993
Page three

the coalition members, but it is a terrible outcome for the rest of the country.

We very much appreciate your efforts on behalf of open government, and your work with the Vice President and the Secretary of Commerce to develop the nation's information infrastructure. We believe that these efforts are sending our country in the right direction, helping to develop advanced technologies appropriate for a democratic nation and to preserve open and accountable government.

But the Clipper proposal was not a creation of your administration. It is a relic from a period that is now moving rapidly into the history books, a time when secret agencies made secret decisions and when backroom deals with powerful, private interests sustained these arrangements.

It is time to end this cynical form of policy making.

We ask you to reject the deal put forward by the Digital Privacy and Security Working Group. The Clipper proposal should not go forward.

We would be pleased to meet with members of your administration to discuss this matter further.

Sincerely yours,

Marc Rotenberg, Director
David Sobel, Legal Counsel
Dave Banisar, Policy Analyst
CPSR Washington office

cc: The Vice President
Secretary Ron Brown, Department of Commerce
Anthony Lake, National Security Council
Computer System Security and Privacy Advisory Board

encl: CPSR Cryptography Resolution, October 18, 1993