INTERNET PRIVACY COALITION
http://www.privacy.org/ipc/

April 28, 1997

The Hon. Robert W. Goodlatte
Committee on the Judiciary U.S. House of Representatives
2138 Rayburn House Office Building
Washington, DC 20515

Re: H.R. 695, The SAFE Act

Dear Representative Goodlatte:

We, the undersigned members of the Internet Privacy Coalition, write to you regarding the Security and Freedom Through Encryption (SAFE) Act (H.R. 695), the pending legislation that you have introduced to reform U.S. encryption policy. We first wish to express our strong support for your efforts to make available better encryption products to American citizens and users of the Internet around the world. We believe that the widespread availability of such products will be critical for our nation's continued leadership of the information industry and the protection of personal privacy.

The pending bill provides a positive framework for the reforms that are long overdue in this critical area. It makes clear that the sale or use of encryption, a vital technique to promote network security and individual privacy, should not be restricted in the United States. This is the view widely shared by users of the Internet and the computer and communications industry. It was also a central recommendation of the report of the National Research Council last year.

While expressing our support for the measure, we wish also to state our concern about one provision contained in the bill. We believe that this provision, which would create new criminal penalties for the use of encryption in furtherance of a crime, could undermine the otherwise laudable goals of the legislation. For the reasons set forth below, we recommend that this provision be reconsidered when the Committee considers the bill.

As currently drafted, H.R. 695 would establish a new offense for the use of encryption "in furtherance of the commission of a criminal offense." While well-intended, the provision could have a series of unintended consequences that would easily undermine the other desirable features of the bill.

First, we believe it is a mistake to create criminal penalties for the use of a particular technique or device. Such a provision tends to draw attention away from the underlying criminal act and casts a shadow over a valuable technology that should not be criminalized. It may, for instance, be the case that a typewritten ransom note poses a more difficult challenge for forensic investigators than a handwritten note. But it would be a mistake to criminalize the use of a typewriter simply because it could make it more difficult to investigate crime in some circumstances.

Second, a provision which criminalizes the use of encryption, even in furtherance of a crime, would give prosecutors wide latitude to investigate activity where the only indicia of criminal conduct may be the mere presence of encrypted data. In the digital age, where techniques to protect privacy and security will be widely deployed, we cannot afford to view encryption as the instrumentality of a crime, just as we would

not view the use of a typewriter in the current era.

Finally, the provision could also operate as a substantial disincentive to the widespread adoption of strong encryption techniques in the communications infrastructure. Recognizing, as the National Research Council has, that the availability of strong encryption is one of the best ways to reduce the risk of crime and to promote public safety, the retention of this provision in the legislation will send a mixed message to users and businesses — that we want people to be free to use encryption but will be suspicious when it is used.

If the concern is that encryption techniques may be used to obstruct access to evidence relevant to criminal investigations, we submit that the better approach may be, to the extent allowed by the Constitution, to rely on other provisions in the federal and state criminal codes (including sections relating to obstruction of justice or concealment) to address this problem if it arises.

We thank you for your leadership on this important issue and appreciate your consideration of our views.

Respectfully,

Donald Haines,
Legislative Counsel American Civil Liberties Union

James Lucier,
Director of Economic Research Americans for Tax Reform

Barbara Simons,
Chair Association for Computing, U.S. Public Policy Committee (USACM)

Chris Prokop,
Chief Executive Officer BitWrench, Incorporated

Jerry Berman,
Executive Director Center for Democracy and Technology

Jeffrey Chester,
Executive Director Center for Media Education

Marlo Lewis, Jr.,
Vice President for Policy Competitive Enterprise Institute

Aki Namioka,
President Computer Professionals for Social Responsibility

Stephen D. Crocker,

Chief Technology Officer CyberCash, Inc.

Doug Humphrey,
Chief Technology Officer Digex, Inc.

Phyllis Schlafly,
President Eagle Forum

Lori Fena,
Executive Director Electronic Frontier Foundation

Marc Rotenberg,
Director Electronic Privacy Information Center

Lisa S. Dean,
Vice President for Governance and Technology Free Congress Foundation

Jeff Taylor,
Executive Director Frontiers of Freedom

Conrad Martin, Executive
Director Fund for Constitutional Government

Paul Kostek, Vice Chair,
IEEE-USA USA Board Institute of Electrical & Electronics Engineers - United States Activities (IEEE-USA)

Paul E. Hoffman,
Director Internet Mail Consortium

Donald Heath,
Executive Director Internet Society

Jack King,
Director of Public Affairs National Association of Criminal Defense Lawyers

Kit Gage,
Washington Representative National Committee Against Repressive Legislation

Audrie Krause,
Executive Director NetAction

Kelly Huebner Blough,
Director of Government Relations Pretty Good Privacy, Inc.

Simon Davies,
Director General Privacy International

Evan Hendricks,

Chair U.S. Privacy Council

Shabbir J. Safdar,
Co-Founder Voters Telecommunications Watch

Todd Lappin,
Section Editor Wired Magazine

cc: Members of the Subcommittee on Courts & Intellectual Property, House Committee on the Judiciary