Statement of

The Honorable Patrick Leahy

United States Senator
Vermont
September 25, 2003

Statement of Senator Patrick Leahy
On the Nomination of Charles Pickering
September 25, 2003

Today, the Republican majority has decided to place the nomination of Charles Pickering to the United States Court of Appeals for the Fifth Circuit on the Committee markup agenda. After full and fair hearings, and full and fair debate, this Committee rejected that nomination to that same position last year. We did so for good reason and we set forth those reasons during the course of our debate. Despite the religious McCarthyism that ensued and the mischaracterizations of our actions for partisan political purposes by the Administration and others, the record shows that Judge Pickering was treated fairly by this Committee at that time.

Never in the history of this Republic has a President renominated to the same post a judicial nominee voted down by this Committee--never until this Administration chose to renominate Judge Pickering and Justice Owen this year. Until this President, the Committee's rejection of a judicial nominee on the merits was respected as a function of the Senate's process of advice and consent. When the Senate Judiciary Committee held hearings and took a vote and determined not to report a nominee, the Senate abided by that decision and every President until this one has, as well.

The President's renomination of Judge Pickering in January was itself controversial. It followed the controversy that led to the resignation of the Republican Majority Leader and the White House's designation of his successor.

I was surprised to see this nomination added to the middle of the agenda we had for our meeting last week that was cancelled because of the hurricane that hit the area. I was relying on the Chairman's previous statements about his intentions to proceed on the Pickering renomination, as extraordinary as it is, in the normal course and through regular order. His appearance on the agenda today, on less than two days notice, came as something of a surprise. Of course it was not a total surprise - the reporter from Fox News to whom the information was leaked did call to ask my office about it hours before any official notice was transmitted.

I am particularly sorry that the Republican majority has chosen this week to proceed because of the insensitivity it shows to the Congressional Black Caucus Foundation and to their strong and abiding opposition to this nomination. The Congressional Black Caucus Foundation has its annual meetings this week and weekend. The Honorable Bennie Thompson, a Representative from Mississippi, is a respected member of the Congressional Black Caucus Foundation and has

opposed this nomination. I know the Chairman to be sensitive to other members and know that he would not go out of his way to offend another Member of Congress, so I am left to wonder why this was added to the agenda in such haste and without consultation with me or others, and why Republicans are proceeding as they are.
Given the many concerns about Judge Pickering voiced by African-Americans in Mississippi and all over the country, including every one of the 160 chapters of the Mississippi NAACP, the Magnolia Bar Association and the Mississippi State Black Legislative Caucus, it was most ill-advised to abruptly list the nomination at the time that the Congressional Black Caucus Foundation is involved in its Annual Legislative Conference.
In January of this year, at our first meeting, the Chairman expressed his clear intention of holding another hearing for Judge Pickering, not of moving him out of Committee without further consideration. Specifically, he told us all that, "we . . . will have hearings in due course for Priscilla Owen and for Judge Pickering."

This certainly seemed to remain his plan through at least this past April, when he announced that, "I held a hearing for Priscilla Owen . . . and I am hopeful that we will do the same for Judge Pickering." Indeed, we have seen press accounts of elaborate preparations being made for another hearing. Although we had discussed the need for additional hearings if Republicans intended to proceed earlier this year, I was not consulted before this alternative course was selected. The Chairman, who certainly has wide-ranging discretion in these matters, has unilaterally decided not to hold a hearing for this extraordinary nomination. I cannot help but wonder why not.

With the Owen nomination, Republicans contended that the record was misleading and needed to be corrected. I disagreed and thought that the hearing chaired by Senator Feinstein was fair and thorough. I think my view was borne out by the subsequent hearing held by Senator Hatch on that nomination earlier this year and by the tremendous opposition and controversy that nomination continues to generate.

That raises the question, if the record before the Committee on the Pickering nomination was fair, adequate and sufficient, why proceed at all with this nomination. It was based on that record that this Committee has already rejected the nomination. Unlike more than 50 of President Clinton's nominees, Judge Pickering had the chance to come to the Committee, answer our questions and explain himself. We debated the nomination in open session and we voted. His nomination was rejected. If the record was not complete and if this Committee is being called upon to reconsider this nomination, something that was unprecedented until this year, why not schedule another hearing? What is it about Judge Pickering's record or background that my colleagues on the other side of the aisle, and their colleagues in the White House do not want to open to public scrutiny? In the previous debate we have pointed out many examples of his injecting his personal views into his legal opinions. We have shown the scores of times he has been reversed for repeating the same errors. We have heard from him confirmation of his solicitation of support from those who appear before him and seen the opinions that these actions violate legal ethics. We have looked carefully at his handling of a highly charged case of a convicted arsonist and hate criminal.

What does seem certain is that suddenly listing Judge Pickering's nomination for Committee action is a political ploy. Whether or not the nomination survives a fight on the Senate floor, the political calculation must be that this move somehow benefits the Republican Party or certain Republican candidates. If Republicans really wanted this nomination seriously considered, it would have been a subject of significant discussion before it was listed for action. All the necessary paperwork would have been discussed and been in place. We would have updated the nominee's file and moved forward together. As far as I know Judge Pickering was not even asked to update his nomination materials, he was not asked to submit the many unpublished opinions he has written since the time of his last consideration. That did not happen here.

Whatever the reason for this turnaround in strategy, the facts and my conclusions about Judge Pickering's fitness for the appellate court have not changed and we have been given no basis on which to reconsider this matter.

Given the unavailability of Senators this morning who wish to be heard on this matter, it must be held over until another time under our rules. I would hope that during that time, however long it takes, the nominee will at least provide the Committee with copies of unpublished opinions not previously furnished.
# # # # #

Statement of Senator Patrick Leahy
On the nomination of Mauricio Tamargo
September 25, 2003

I intend to vote for the nomination of Mr. Tamargo to another three-year term as Chairman of the Foreign Claims Settlement Commission, although I have concerns about the workload of this Commission. According to Mr. Tamargo's answers to my questions, there have been no new claims filed in 2003, 2002, 2001, and 2000. Mr. Tamargo advised us that, with no claims filed in the past four years, he has been "implementing a new database" to "digitize" and process future claims.

I believe the argument could be made that it is worth having a Chairman of this historically important tribunal in case any new claims get created by statute, but I would hesitate to vote in favor of any other nominee to this Commission, given the amount of tax payer money being directed at an entity that has no claims and has had none for at least four years.

# # # #

Statement of Senator Patrick Leahy
Ranking Member, Senate Judiciary Committee

S. 1451, The Runaway, Homeless, and Missing Children Protection Act
Executive Business Meeting
September 25, 2003

I am pleased to cosponsor this legislation to reauthorize and improve the Runaway and Homeless Youth Act, and to extend the authorization of the Missing Children's Assistance Act. This bill follows in the footsteps of the recently enacted PROTECT Act legislation, and presents another milestone in our efforts to safeguard all of our children.

In the 29 years since it became law, the Runaway and Homeless Youth Act has helped some of the most vulnerable children in our country. A Justice Department report released last year estimated that 1.7 million young people either ran away from or were thrown out of their homes in 1999 alone. Other studies have suggested an even higher number. This law and the programs it funds provide a safety net that helps give these young people a chance to build lives for themselves. It is slated to expire at the end of this fiscal year, and we should not allow that to happen.

In my state, both the Vermont Coalition for Runaway and Homeless Youth and Spectrum Youth and Family Services in Burlington receive grants under this law, and they have provided excellent services both to young people trying to build lives on their own and to those who are struggling on the streets. Reauthorizing this law will allow them to continue their enormously important work.

This bill would improve the law by extending the period during which older homeless youth can receive services under the Transitional Living Program, to ensure that all homeless youth can take advantage of services at least until they turn 18. The bill would also make permanent the Secretary of Health and Human Services' authority to make grants explicitly to help rural areas meet the unique stresses of providing services to runaway and homeless youth. Programs serving runaway and homeless youth have found that those in rural areas are particularly difficult to reach and serve effectively, and this bill recognizes that fact.

The improvements proposed in this bill to the Missing Children's Assistance Act build on provisions included in the PROTECT Act legislation that we enacted earlier this year. In that bill, we authorized National Center for Missing and Exploited Children ("NCMEC") activities through 2005 and authorized the Center to strengthen its CyberTipline to provide online users an effective means of reporting Internet-related child sexual exploitation in distribution of child pornography, online enticement of children for sexual acts, and child prostitution. This bill would extend NCMEC through 2008. Now more than ever, it is critical for Congress to give the Center the resources it needs in order to pursue its important work. A missing or abducted child is the worst nightmare of any parent or grandparent, and NCMEC has proved to be an invaluable resource in Federal, state, and local efforts to recover children who have disappeared.

Although this is a good bill on the whole, I am very disappointed that Senator Hatch did not agree to remove a provision that was included in the House bill that prohibits grantees from using any funds provided under this program for needle distribution programs. This is a superfluous provision that simply repeats what is already law. In addition, it is unnecessary because no grantee under this program operates needle exchange programs or has expressed

interest in doing so. The inclusion of this needless provision, however, does not change the fact that this is still a good bill.

The Runaway and Homeless Youth Act programs have received tremendous bipartisan support over the years, and the House has already passed this bill by a vote of 404-14. I urge the Committee to give its approval to this bill today.

# # # #

STATEMENT OF SENATOR PATRICK LEAHY,
RANKING MEMBER, SENATE COMMITTEE ON THE JUDICIARY
ON S.1293, THE "CRIMINAL SPAM ACT OF 2003"
September 25, 2003

I am pleased that the Committee is taking up S.1293, the bipartisan Criminal Spam Act of 2003. Chairman Hatch and I introduced this bill on June 19th along with several members of this Committee -- Senator Schumer, Senator Grassley, Senator Feinstein, Senator DeWine, and Senator Edwards. I thank all of our cosponsors for their help and support on this bill and am grateful to Senators Hatch and Schumer for their efforts. I hope we can report it to the floor without delay, and pass it before the end of the year.

BACKGROUND
Without a doubt, spam is a serious problem today - one that threatens to undermine the vast potential of the Internet to foster the free exchange of information and commerce. I have long recognized that we must be vigilant in keeping our computer crime laws up-to-date as new technologies spawn ever more sophisticated scams and frauds. Computer security and unauthorized intrusions into responsible net commerce should be at the forefront of any discussion of information technology in the 21st Century.

Many of us on this Committee have worked on cyber crime issues for years.

In 1984, we passed the Computer Fraud and Abuse Act, to criminalize certain conduct when carried out by means of unauthorized access to a computer.

In 1986, we passed the Electronic Communications Privacy Act, which I was proud to sponsor, to criminalize tampering with electronic mail systems and remote data processing systems and to protect the privacy of computer users.

In 1994, the Violent Crime Control and Law Enforcement Act included the Computer Abuse Amendments, which I authored, to make illegal the intentional transmission of computer viruses.

This statute was used last week to prosecute the Minnesota man who is charged with developing and releasing onto the Internet a variant of the Blaster computer worm, which is believed to have infected at least 7,000 individual Internet users' computers, turning them into drones that attacked or attempted to attack Microsoft, and causing substantial financial damage.

In the 104th Congress, Senators Kyl, Grassley and I worked together to enact the National Information Infrastructure Protection Act, to increase protection under Federal criminal law for both government and private computers, and to address the problem of computer-age blackmail, in which a criminal threatens to harm or shut down a computer system unless his extortionate demands are met. Senator Kyl and I also worked together in the 105th Congress on criminal copyright amendments that became law.

Most recently, in the 106th Congress, I worked with Senator DeWine to pass the Computer Crime Enforcement Act, which authorized grants to State and local law enforcement to investigate and prosecute computer crime.

The current bill is designed to address spam, the most objectionable form of email marketing. In an effort to clear electronic channels for legitimate communications, the bill targets those spammers who deceive Internet Service Providers ("ISPs") and email recipients into thinking that messages come from someone other than a spammer -- a ploy many spammers use to increase the likelihood that their unwanted ads will evade filtering software and be opened

THE PROBLEM
Businesses and individuals currently wade through tremendous amounts of spam in order to access email that is of relevance to them--and this is after ISPs, businesses, and individuals have spent time and money blocking a large percentage of spam from reaching its intended recipients.

Email users are having the online equivalent of the experience of the woman in the Monty Python skit, who seeks to order a Spam-free breakfast at a restaurant. Try as she might, she cannot get the waitress to bring her the meal she desires. Every dish in the restaurant comes with Spam; it's just a matter of how much. There's "egg, bacon and Spam"; "egg, bacon, sausage and Spam"; "Spam, bacon, sausage and Spam"; "Spam, egg, Spam, Spam, bacon and Spam"; "Spam, sausage, Spam, Spam, Spam, bacon, Spam, tomato and Spam"; and so on. Exasperated, the woman finally cries out: "I don't like Spam!... I don't want ANY Spam!"

Individuals and businesses are reacting similarly to electronic spam. A Harris poll taken late last year found that 80 percent of respondents view spam as "very annoying," and fully 74 percent of respondents favor making mass spamming illegal. Earlier this month, more than 3 out of 4 people surveyed by Yahoo! Mail said it was "less aggravating to clean a toilet" than to sort through spam. Americans are fed up.

ISPs are doing their best to shield customers from spam, blocking billions of spam each day, but the spammers are winning the battle. Millions of unwanted, unsolicited commercial emails are received by American businesses and individuals each day, despite their own, additional filtering efforts. A recent study by Ferris Research estimates that spam costs U.S. businesses $8.9 billion annually as a result of lost productivity and the need to purchase more powerful servers and additional bandwidth; to configure and run spam filters; and to provide help-desk support for

spam recipients. The costs of spam are significant to individuals as well, including time spent identifying and deleting spam, inadvertently opening spam, installing and maintaining anti-spam filters, tracking down legitimate messages mistakenly deleted by spam filters, and paying for the ISPs' blocking efforts.

And there are other prominent and equally important costs of spam. It may introduce viruses, worms, and Trojan horses into personal and business computer systems, including those that support our national infrastructure.

The public has recently witnessed the potentially staggering affects of a virus, not only through the Blaster case I discussed earlier, but with the appearance of the SoBigF virus just eight days after Blaster began chewing its way through the Internet. This variant also infected Windows machines via e-mail, then sent out dozens of copies of itself. Anti-virus experts say one of the main reasons virus writers continue to modify and re-release this particular piece of "malware" is that it downloads a Trojan horse to infected computers, which are then used to send spam.

Spammers are constantly in need of new machines through which to route their garbage e-mail, and a virus makes a perfect delivery mechanism for the engine they use for their mass mailings. Some analysts said the SoBigF virus may have been created with a more malicious intent than most viruses, and may even be linked to spam email schemes that could be a source of cash for those involved in the scheme.

The interconnection between computer viruses and spam is readily apparent: Both flood the Internet in an attempt to force a message on people who would not otherwise choose to receive it. Criminal laws I wrote prohibiting the former have been invoked and enforced from the time they were passed - it is the latter dilemma we must now confront head-on.

Spam is also fertile ground for deceptive trade practices. The FTC has estimated that 96 percent of the spam involving investment and business opportunities, and nearly half of the spam advertising health services and products, and travel and leisure, contains false or misleading information.

This rampant deception has the potential to undermine Americans' trust of valid information on the Internet. Indeed, it has already caused some Americans to refrain from using the Internet to the extent that they otherwise would. For example, some have chosen not to participate in public discussion forums, and are hesitant to provide their addresses in legitimate business transactions, for fear that their email addresses will be harvested for junk email lists. And they are right to be concerned. The FTC found spam arriving at its computer system just nine minutes after posting an email address in an online chat room.

THE NEED FOR FEDERAL INTERVENTION

At a recent FTC forum on spam, experts agreed that the issue is ripe for Federal action. Some 30 states now have anti-spam laws, but the nature of email makes it difficult to discern where any given piece of spam originated, and, thus, what state has jurisdiction and what state law applies. This may explain why spammers continue to flout state laws. For example, several states require that spam begin the subject line with "ADV," but the FTC has found that only 2 percent of spam contains this label.

Technology will undoubtedly play a key role in fighting spam. However, a technological solution to the problem is not predicted in the foreseeable future. In addition, given the adroitness with which spammers adapt to anti-spam technologies, the development and implementation of technological fixes to spam entail constant vigilance and substantial financial investment. This raises the question: Why should individuals and businesses be forced to invest large amounts of time and money in buying, installing, and maintaining generation after generation of anti-spam technologies?

THE CRIMINAL SPAM ACT

I have often said that the government should regulate the Internet only when absolutely necessary. Unfortunately, spammers have caused this to be one of those times. Congress needs to address the spam problem quickly and prudently, and the Hatch-Leahy-Schumer Criminal Spam Act, by targeting the most injurious types of spam, is a good start. Our bill would prohibit five principal techniques that spammers use to evade filtering software and hide their trails.

First, the bill would prohibit hacking into another person's computer system and sending bulk spam from or through that system. This would criminalize the common spammer technique of obtaining access to other people's email accounts on an ISP's email network, whether by password theft or by inserting a "Trojan horse" program - that is, a program that unsuspecting users download onto their computers and that then takes control of those computers -- to send bulk spam.

Second, the bill would prohibit using a computer system that the owner makes available for other purposes as a conduit for bulk spam, with the intent of deceiving recipients as to the spam's origins. This prohibition would criminalize another common spammer technique -- the abuse of third parties' "open" servers, such as email servers that have the capability to relay mail, or Web proxy servers that have the ability to generate "form" mail. Spammers commandeer these servers to send bulk commercial email without the server owner's knowledge, either by "relaying" their email through an "open" email server, or by abusing an "open" Web proxy server's capability to generate form emails as a means to originate spam, thereby exceeding the owner's authorization for use of that email or Web server. In some instances the hijacked servers are even completely shut down as a result of tens of thousands of undeliverable messages generated from the spammer's email list.

The bill's third prohibition targets another way that outlaw spammers evade ISP filters: falsifying the "header information" that accompanies every email, and sending bulk spam containing that fake header information. More specifically, the bill prohibits forging information regarding the origin of the email message, the route through which the message attempted to penetrate the ISP filters, and information authenticating the user as a "trusted sender" who abides by appropriate consumer protection rules. The last type of forgery will be particularly important in the future, as ISPs and legitimate marketers develop "white list" rules whereby emailers who abide by self-regulatory codes of good practices will be allowed to send email to users without being subject to anti-spamming filters. There is currently substantial interest among marketers and email service providers in "white list" technology solutions to spam. However, such "white list" systems would be useless if outlaw spammers are allowed to counterfeit the authentication mechanisms used by legitimate emailers.

Fourth, the Criminal Spam Act prohibits registering for multiple email accounts or Internet domain names, and sending bulk email from those accounts or domains. This provision targets deceptive "account churning," a common outlaw spammer technique that works as follows. The spammer registers (usually by means of an automatic computer program) for large numbers of email accounts or domain names, using false registration information, then sends bulk spam from one account or domain after another. This technique stays ahead of ISP filters by hiding the source, size, and scope of the sender's mailings, and prevents the email account provider or domain name registrar from identifying the registrant as a spammer and denying his registration request. Falsifying registration information for domain names also violates a basic contractual requirement for domain name registration falsification.

Fifth and finally, our bill addresses a major hacker spammer technique for hiding identity that is a common and pernicious alternative to domain name registration - hijacking unused expanses of Internet address space and using them as launch pads for junk email. Hijacking Internet Protocol ("IP") addresses is not difficult: Spammers simply falsely assert that they have the right to use a block of IP addresses, and obtain an Internet connection for those addresses. Hiding behind those addresses, they can then send vast amounts of spam that is extremely difficult to trace.

Penalties for violations of the bill's new criminal prohibitions are tough but measured. Recidivists and those who send spam in furtherance of another felony may be imprisoned for up to five years. Large-volume spammers, those who hack into another person's computer system to send bulk spam, and spam "kingpins" who use others to operate their spamming operations may be imprisoned for up to three years. Other offenders may be fined and imprisoned for no more than one year. Convicted offenders are also subject to forfeiture of proceeds and instrumentalities of the offense.

In addition to these criminal penalties, offenders are also subject to civil enforcement actions, which may be brought by either the Department of Justice or by an ISP. Civil remedies are important as a supplement to criminal enforcement for several reasons. First, bringing cases against outlaw spammers is very resource intensive because of the extensive forensic work involved in building a case; providing for civil enforcement will allow ISPs to assemble evidence to make prosecutors' jobs easier. Second, although criminal prosecutions are a critical deterrent against the most egregious spammers, the Justice Department is unlikely to prosecute all outlaw spam cases; civil enforcement, backed by strong financial penalties, will serve as a second layer of deterrence. Third, criminal penalties may not be appropriate in all cases, as for example in the case of teenagers hired by professional outlaw spammers to send out email for them; civil enforcement gives the Justice Department a more complete and refined range of tools to address specific outlaw spam problems.

That describes the main provisions of our bill. In addition, because commercial email can be, and is being, sent from all over the world into the virtual mailboxes of Americans, the bill directs the Administration to report on its efforts to achieve international cooperation in the investigation and prosecution of outlaw spammers.

OTHER APPROACHES

Again, the purpose of the Criminal Spam Act is to deter the most pernicious and unscrupulous types of spammers - those who use trickery and deception to induce others to relay and view

their messages. Ridding America's inboxes of deceptively delivered spam will significantly advance our fight against junk email. But the Criminal Spam Act is not a cure-all for the spam pandemic.

The fundamental problem inherent to spam -- its sheer volume - may well persist even in the absence of fraudulent routing information and false identities. In a recent survey, 82 percent of respondents considered unsolicited bulk email, even from legitimate businesses, to be unwelcome spam. Given this public opinion, and in light of the fact that spam is, in essence, cost-shifted advertising, it may be wise to take a broader approach to our fight against spam.

One approach that has achieved substantial support is to require all commercial email to include an "opt out" mechanism, that is, a mechanism for consumers to opt out of receiving further unwanted spam. At the recent FTC forum, several experts expressed concerns about this approach, which permits spammers to send at least one piece of spam to each email address in their database, while placing the burden on email recipients to respond. People who receive dozens, even hundreds, of unwanted emails each day would have little time or energy for anything other than opting-out from unwanted spam.

According to one organization's calculations, if just one percent of the approximately 24 million small businesses in the U.S. sent every American just one spam a year, that would amount to over 600 pieces of spam for each person to sift through and opt-out of each day. And this figure may be conservative, as it does not include the large businesses that also engage in on-line advertising.

A second possible approach to spam - a national "Do Not Spam" registry - raises a different but no less difficult set of concerns. The FTC has questioned the potential of a national registry to alleviate the spam problem. Although this approach would place a smaller burden on consumers than would an opt-out system, it would entail immense costs, complexity, and delay, all of which work in the spammers' favor.

A third way of attacking spam - and one that was favored by many panelists and audience members at the FTC forum -- is to establish an opt-in system, whereby bulk commercial email may only be sent to individuals and businesses who have invited or consented to it. This approach -- which has already been adopted by the European Union -- has strong precedent in the Telephone Consumer Protection Act of 1991, which Congress passed to eliminate similar cost-shifting, interference, and privacy problems associated with unsolicited commercial faxes, and which has withstood First Amendment challenges in the courts.

CONCLUSION

I have discussed three possible approaches to the spam problem, and there are several others, some of which have already been codified in state law. I encourage the consideration of all these anti-spam approaches in the weeks and months to come.

Reducing the volume of junk commercial email, and so protecting legitimate Internet communications, will not be easy. There are important First Amendment interests to consider, as well as the need to preserve the ability of legitimate marketers to use email responsibly. If Congress does act, it must get it right, so as not to exacerbate an already terribly vexing problem.

The Criminal Spam Act is a first step in countering spam. If we can shut down the spammers who use deception to evade filters and confuse consumers, we will give the next generation of anti-spam technologies a chance to do their work. Our bill targets the most egregious offenders, it provides a much-needed federal cause of action, and it allows the states to continue to serve as a "laboratory" for tough anti-spamming regulation. I urge its speedy enactment into law.