We see that on this chart. We show a $52 billion surplus, but the fact is, we are truly in deficit because we will be using $122 billion of Social Security in 2002, $125 billion in 2003, and so forth. So we are going to be using the Social Security surplus, according to this chart, all the way out to the year 2006.

I remind my colleagues the projected $52 billion unified surplus is a gross exaggeration of the possible surplus this year because we have pledged we are going to use $60 to $75 billion to stimulate the economy, which means we are going to wipe out this $52 billion surplus in 2002. In fact, we are going to have to borrow the money from the public to pay for the things we want to do.

I would like to remind my colleagues the bleak budget outlook I described goes way out into future years. The Senate Budget Committee projected we will spend significant portions of Social Security surpluses, as I mentioned, in 2003 to 2006.

I further remind my colleagues that these figures on this chart, as bad as they are, do not tell the whole story. These we are showing are based on a cost-of-living increase in spending based on inflation. Remember Congress spent 14.5 percent more in fiscal 2001 on nondefense discretionary spending than they did in fiscal year 2000. We should have no illusions that Congress is going to spend at the rate of inflation. I don't know of any time that Congress has spent money at the rate of inflation. As to these numbers on this chart, you might as well forget them. They are gone because the projections are based on inflationary increases and we know that is not going to be the case.

Our current crisis should not be used as an excuse to run up the tab for programs and projects not related to the war on terrorism or stimulating our economy. Now more than ever before we have to prioritize our funding and make tough choices. Do our spending choices put the safety of American lives at home and abroad front and center? Will they truly boost the economy? These are the questions that should be applied to every dollar Congress spends. Our current fiscal position does not allow for any unnecessary spending. Domestic needs must be reprioritized. Those of us who have been concerned about fiscal responsibility have to recommit ourselves to fiscal discipline. We have to make the tough choices to keep in check the urge to spend, keeping in mind we are spending the Nation's Social Security money with every additional dollar that goes out the door. Once it has gone out the door, we are then going to borrow that money from the public.

I am concerned that some proposals being considered in this Senate are inappropriate, given the long-term budget pressures we face. You will be hearing from me and hopefully many others about some of those proposals. If the stimulus package we put in place results in chronic budget deficits, it is going to drive up interest rates. And make no mistake about it, the financial markets are closely watching what we do. If they see Congress taking actions that will steer the Federal Government towards persistent deficits, they will drive interest rates higher. Higher interest rates will have exactly the opposite effect on the economy from what we want. They would put a brake on the economy by raising consumers' interest payments and discouraging economic activity.

Remember, low interest rates are important to the economy. In fact, Federal Reserve Chairman Alan Greenspan has been quite clear about this as he has highlighted this to many of us.

I think this is very important. This is not merely an academic exercise. The recent rise in long-term interest rates is attributed to the deteriorating budget condition of the Federal Government in the past few weeks. As my colleagues know, Congress will consider a true stimulus package in the near future. Helping America's workers, all workers, should be and will be a part of that package and should be our No. 1 priority.

The stimulus package can only be so big. So it is critical that we touch as many Americans as possible. All of them should participate in that economic stimulus package. That same message applies to the money we allocate to fight terrorism at home and abroad. We need to prioritize and we need to get the biggest bang for our buck, literally and figuratively.

We in this body must never lose sight that the day of reckoning with the baby boomer retirement has not been put off by our current crisis. Like it or not, the baby boomers will begin to retire in about 10 years, and if we fail to act, we will put an unacceptable burden on our children and grandchildren. We face an important challenge in preparing for that day. Our goal should be to fund our war on terrorism at home and abroad, respond to the needs of the victims of the terrorist attack in New York and here in Washington, get our economy going, and as soon as possible end deficit spending. We owe it to our children and grandchildren.

I yield the floor.

The PRESIDING OFFICER. The Senator from Utah is recognized.

Mr. HATCH. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. LEAHY. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. LEAHY. Mr. President, what is the parliamentary situation under the unanimous consent request?

The PRESIDING OFFICER. There is nothing pending before the Senate.

Mr. LEAHY. Mr. President, I yield to the Democratic leader.

Mr. REID. Mr. President, I appreciate the Senator yielding.

On behalf of Senator DASCHLE, I now ask that the Senate consider S. 1510.

UNITING AND STRENGTHENING AMERICA ACT

The PRESIDING OFFICER. The clerk will report the bill by title.

The legislative clerk read as follows:

A bill (S. 1510) to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.

Mr. LEAHY. Mr. President, what is the time agreement that we are now operating under?

The PRESIDING OFFICER. There are 4 hours equally divided. In addition, there are 40 minutes on each of the four amendments to be offered by the Senator from Wisconsin, Mr. FEINGOLD.

Mr. LEAHY. I thank the distinguished Presiding Officer.

I cannot help but think in looking at our distinguished Presiding Officer, the senior Senator from New York, how much his State has suffered. Both he and his distinguished colleague, Senator CLINTON, have spoken so eloquently, both on the floor and elsewhere, about that. I know in my own private conversations with the distinguished Presiding Officer I felt the depth of his grief and emotion for a city that he obviously and unabashedly loves. His references to New York City over the years are almost similar to the kind of comments I make about Vermont. But I do note the accent is somewhat different. I assume it is because of the Vermont accent.

But I think the Senators from New York, and the Senators from New Jersey and Connecticut have especially spoken of the effect on families and loved ones in the New York City area. People who work there are from New York, New Jersey, and Connecticut. I know how sad they feel.

I think of the people who died in Pennsylvania in an airplane that was probably planning to strike the very building we are in—this symbol of democracy. Only with a great loss of life did it not happen. But there would be an enormous disruption in our Government. The next day, the view that most people around the world have—our symbol of democracy—would be gone.

I think of the brave men and women who died, as the President and others have said, doing their duty at the Pentagon, and the hundreds—even thousands—of children who went to school happily in the morning and came home to find that they were orphans.

It was a terrible, terrible day.

I think back to what happened in Oklahoma City in 1995 and the actions we took then. We are moving, of course, much faster now than we did at that time, and I hope perhaps with more care on legislation.

We have before us the USA Act of 2001. I worked with Chairman SENSENBRENNER and Congressman CONYERS

and Republican and Democratic leaders in the House because I hope Congress can act swiftly to enact this measure.

Some may be concerned if we have a conference—because the House is somewhat different than the Senate—that we could take a year or more to resolve these issues. That happened after Oklahoma City. That legislation took nearly a year to reconcile.

I believe the American people and my fellow Senators, both Republican and Democratic, deserve faster final action.

I assure the Senate, when we go to conference, we will complete that conference very quickly. We have demonstrated the ability in this body—and also Senators who have worked with me on both sides of the aisle and our staff—that we can work around the clock.

The distinguished senior Senator from Utah, Mr. HATCH, and I have been working together in constant communication with our staffs.

Last Thursday, October 4, I was pleased to introduce, along with the majority leader, Senator DASCHLE, and the Republican leader, Senator LOTT, also the chairmen of the Banking and Intelligence Committees, Senator SARBANES, Senator GRAHAM of Florida, Senator HATCH, and Senator SHELBY, the USA Act.

I must say this bill is not the bill I would have written if I were the only one writing it. I daresay it is not the bill the distinguished Presiding Officer, one of the brightest and most accomplished people I know, would have written, if he were writing it. It is not the bill the distinguished chairman of the Banking Committee would have written if he were writing it. It is not the bill the distinguished ranking member, Mr. HATCH, would have written when he was chairman, if he was solely writing the bill. It is really not the bill that any one of the other Members would have written. We can't pass 100 bills.

We have tried to put together the best possible bill. Of course, Republican and Democratic colleagues must come together, and that is what we did.

I should point out that this is not the bill the administration, through the Attorney General, delivered to us and asked for immediate passage. We actually did the administration a favor because rather than take the bill they dropped in our laps and said pass immediately, we did something that apparently they had not done. We read it and were able to refine and supplement their proposal in a number of ways. We were able to remove a number of unconstitutional parts. The administration accepted a number of practical steps that I proposed to improve our security on the Northern Border to assist our State, Federal, and local law enforcement officers and provide compensation to the victims of terrorist acts and to the public safety officers that gave their lives to protect us.

It also provides proposed checks on Government powers—checks that were not contained in the Attorney General's initial proposal.

In negotiations with the administration, I have done my best to strike a reasonable balance between the need to address the threat of terrorism, which we all keenly feel at the present time, and the need to protect our constitutional freedoms. Despite my misgivings, I have acquiesced in some of the administration's proposals because it is important to preserve national unity in this time of national crisis and to move the legislative process forward.

We still have room for improvement. Even after the Senate passes judgment on this bill—I believe it will tonight—the debate is not going to be finished because we have to consider those important things done in the other body.

What I have done throughout this time is to remember the words of Benjamin Franklin—when he literally had his neck on the line because if the Revolution had failed, he and the others would have been hanged—when he said: A people who would trade their liberty for security deserve neither.

We protected our security, but I am not going to give up the liberties that Americans have spent 220 years to obtain.

Moreover, our ability to make rapid progress was impeded because the negotiations with the Administration did not progress in a straight line. On several key issues that are of particular concern to me, we had reached an agreement with the Administration on Sunday, September 30. Unfortunately, within two days, the Administration announced that it was reneging on the deal. I appreciate the complex task of considering the concerns and missions of multiple federal agencies, and that sometimes agreements must be modified as their implications are scrutinized by affected agencies. When agreements made by the Administration must be withdrawn and negotiations on resolved issues reopened, those in the Administration who blame the Congress for delay with what the New York Times described last week as "scurrilous remarks," do not help the process move forward.

Hearings. We have expedited the legislative process in the Judiciary Committee to consider the Administration's proposals. In daily news conferences, the Attorney General has referred to the need for such prompt consideration. I commend him for making the time to appear before the Judiciary Committee at a hearing September 25 to respond to questions that Members from both parties have about the Administration's initial proposals. I also thank the Attorney General for extending the hour and a half he was able to make in his schedule for the hearing for another fifteen minutes so that Senator FEINSTEIN and Senator SPECTER were able to ask questions before his departure. I regret that the Attorney General did not have the time to respond to questions from all the Members of the committee either on September 25 or last week, but again thank him for the attention he promised to give to written questions Members submitted about the legislation. We have not received answers to those written questions yet, but I will make them a part of the hearing whenever they are sent.

The Chairman of the Constitution Subcommittee, Senator FEINGOLD, also held an important hearing on October 3 on the civil liberties ramifications of the expanded surveillance powers requested by the Administration. I thank him for his assistance in illuminating these critical issues for the Senate.

Rule 14. To accede to the Administration's request for prompt consideration of this legislation, the Leaders decided to hold the USA Act at the desk rather than refer the bill to the Committee for mark-up, as is regular practice. Senator HATCH specifically urged that this occur and I support this decision. Indeed, when the Senate considered the anti-terrorism act in 1995 after the Oklahoma City bombing, we bypassed Committee in order to deal with the legislation more promptly on the floor.

Given the expedited process that we have used to move this bill, I will take more time than usual to detail its provisions.

Victims. The heart of every American aches for those who died or have been injured because of the tragic terrorist attacks in New York, Virginia, and Pennsylvania on September 11th. Even now, we cannot assess the full measure of this attack in terms of human lives, but we know that the number of casualties is extraordinarily high.

Congress acted swiftly to help the victims of September 11th. Within 10 days, we passed legislation to establish a Victims Compensation Program, which will provide fair compensation to those most affected by this national tragedy. I am proud of our work on that legislation, which will expedite payments to thousands of Americans whose lives were so suddenly shattered.

But now more than ever, we should remember the tens of thousands of Americans whose needs are not being met—the victims of crimes that have not made the national headlines. Just one day before the events that have so transformed our nation, I came before this body to express my concern that we were not doing more for crime victims. I noted that the pace of victims legislation has slowed, and that many opportunities for progress had been squandered. I suggested that this year, we had a golden opportunity to make significant progress in this area by passing S. 783, the Leahy-Kennedy Crime Victims Assistance Act of 2001.

I am pleased, therefore, that the antiterrorism package now before the Senate contains substantial portions of S. 783 aimed at refining the Victims of Crime Act of 1984 (VOCA), and improving the manner in which the Crime Victims Fund is managed and preserved. Most significantly, section 621

of the USA Act will eliminate the cap on VOCA spending, which has prevented more than $700 million in Fund deposits from reaching victims and supporting essential services.

Congress has capped spending from the Fund for the last two fiscal year, and President Bush has proposed a third cap for fiscal year 2002. These limits on VOCA spending have created a growing sense of confusion and unease by many of those concerned about the future of the Fund.

We should not be imposing artificial caps on VOCA spending while substantial unmet needs continue to exist. Section 621 of the USA Act replaces the cap with a self-regulating system that will ensure stability and protection of Fund assets, while allowing more money to be distributed to the States for victim compensation and assistance.

Other provisions included from S. 783 will also make an immediate difference in the lives of victims, including victims of terrorism. Shortly after the Oklahoma City bombing, I proposed and the Congress adopted the Victims of Terrorism Act of 1995. This legislation authorized the Office for Victims of Crime (OVC) to set aside an emergency reserve of up to $50 million as part of the Crime Victims Fund. The emergency reserve was intended to serve as a "rainy day" fund to supplement compensation and assistance grants to States to provide emergency relief in the wake of an act of terrorism or mass violence that might otherwise overwhelm the resources of a State's crime victim compensation program and crime victim assistance services. Last month's disaster created vast needs that have all but depleted the reserve. Section 621 of the USA Act authorizes OVC to replenish the reserve with up to $50 million, and streamlines the mechanism for replenishment in future years.

Another critical provision of the USA Act will enable OVC to provide more immediate and effective assistance to victims of terrorism and mass violence occurring within the United States. I proposed this measure last year as an amendment to the Justice for Victims of Terrorism Act, but was compelled to drop it to achieve bipartisan consensus. I am pleased that we are finally getting it done this year.

These and other VOCA reforms in the USA Act are long overdue. Yet, I regret that we are not doing more. In my view, we should pass the Crime Victims Assistance Act in its entirety. In addition to the provisions that are included in today's antiterrorism package, this legislation provides for comprehensive reform of Federal law to establish enhanced rights and protections for victims of Federal crime. It also proposes several programs to help States provide better assistance for victims of State crimes.

I also regret that we have not done more for other victims of recent terrorist attacks. While all Americans are numbed by the heinous acts of September 11th, we should not forget the victims of the 1998 embassy bombings in East Africa. Eleven Americans and many Kenyan and Tanzanian nationals employed by the United States lost their lives in that tragic incident. It is my understanding that compensation to the families of these victims has in many instances fallen short. It is my hope that OVC will use a portion of the newly replenished reserve fund to remedy any inequity in the way that these individuals have been treated.

Hate crimes. We cannot speak of the victims of the September 11 without also noting that Arab-Americans and Muslims in this country have become the targets of hate crimes, harassment, and intimidation. I applaud the President for speaking out against and condemning such acts, and visiting a mosque to demonstrate by action that all religions are embraced in this country. I also commend the FBI Director for his periodic reports on the number of hate crime incidents against Arab-American and Muslims that the FBI is aggressively investigating and making clear that this conduct is taken seriously and will be punished.

The USA Act contains, in section 102, a sense of the Congress that crimes and discrimination against Arab and Muslim Americans are condemned. Many of us would like to do more, and finally enact effective hate crimes legislation, but the Administration has asked that the debate on that legislation be postponed. One of my greatest regrets regarding the negotiations in this bill was the objections that prevented the Local Law Enforcement Enhancement Act, S. 625, from being included in the USA Act.

State and local law enforcement. The Administration's initial proposal was entirely focused on Federal law enforcement. Yet, we must remember that state and local law enforcement officers have critical roles to play in preventing and investigating terrorist acts. I am pleased that the USA Act we consider today recognizes this fact.

As a former State prosecutor, I know that State and local law enforcement officers are often the first responders to a crime. On September 11th, the nation saw that the first on the scene were the heroic firefighters, police officers and emergency personnel in New York City. These New York public safety officers, many of whom gave the ultimate sacrifice, remind us of how important it is to support our State and local law enforcement partners. The USA Act provides three critical measures of Federal support for our State and local law enforcement officers in the war against terrorism.

First, we streamline and expedite the Public Safety Officers' Benefits application process for family members of fire fighters, police officers and rescue workers who perish or suffer a disabling injury in connection with prevention, investigation, rescue or recovery efforts related to a future terrorist attack.

The Public Safety Officers' Benefits Program provides benefits for each of the families of law enforcement officers, firefighters, and emergency response crew members who are killed or disabled in the line of duty. Current regulations, however, require the families of public safety officers who have fallen in the line of duty to go through a cumbersome and time-consuming application process. In the face of our national fight against terrorism, it is important that we provide a quick process to support the families of brave Americans who selflessly give their lives so that others might live before, during and after a terrorist attack.

This provision builds on the new law championed by Senator CLINTON, Senator SCHUMER and Congressman NADLER to speed the benefit payment process for families of public safety officers killed in the line of duty in New York City, Virginia, and Western Pennsylvania, on September 11.

Second, we have raised the total amount of Public Safety Officers' Benefit Program payments from approximately $150,000 to $250,000. This provision retroactively goes into effort to provide much-needed relief for the families of the brave men and women who sacrificed their own lives for their fellow Americans during the year. Although this increase in benefits can never replace a family's tragic loss, it is the right thing to do for the families of our fallen heroes. I want to thank Senator BIDEN and Senator HATCH for their bipartisan leadership on this provision.

Third, we expand the Department of Justice Regional Information Sharing Systems Program to promote information sharing among Federal, State and local law enforcement agencies to investigate and prosecute terrorist conspiracies and activities and authorize a doubling of funding for this year and next year. The RISS Secure Intranet is a nationwide law enforcement network that already allows secure communications among the more than 5,700 Federal, State and local law enforcement agencies. Effective communication is key to effective law enforcement efforts and will be essential in our national fight against terrorism.

The RISS program enables its member agencies to send secure, encrypted communications—whether within just one agency or from one agency to another. Federal agencies, such as the FBI, do not have this capability, but recognize the need for it. Indeed, on September 11, 2001, immediately after the terrorist attacks, FBI Headquarters called RISS officials to request "Smartgate" cards and readers to secure their communications systems. The FBI agency in Philadelphia called soon after to request more Smartgate cards and readers as well.

The Regional Information sharing Systems Program is a proven success that we need to expand to improve secure information sharing among Federal, State and local law enforcement

agencies to coordinate their counter-terrorism efforts.

Our State and local law enforcement partners welcome the challenge to join in our national mission to combat terrorism. We cannot ask State and local law enforcement officers to assume these new national responsibilities without also providing new Federal support. The USA Act provides the necessary Federal support for our State and local law enforcement officers to serve as full partners in our fight against terrorism.

I am deeply troubled by continuing reports that information is not being shared with state local law enforcement. In particular, the testimony of Baltimore Police Chief Ed Norris before the House Government Reform Committee last week highlighted the current problem.

Northern borders. The unfolding facts about how the terrorists who committed the September 11 attack were able to enter this country without difficulty are chilling. Since the attacks many have pointed to our northern border as vulnerable to the entry of future terrorists. This is not surprising when a simple review of the numbers shows that the northern border has been routinely short-changed in personnel. While the number of border patrol agents along the southern border has increased over the last few years to over 8,000, the number at the northern border has remained the same as a decade ago at 300. This remains true despite the fact that Admad Ressam, the Algerian who planned to blow up the Los Angeles International Airport in 1999, and who has been linked to those involved in the September 11 attacks, chose to enter the United States at our northern border. It will remain an inviting target until we dramatically improve our security.

The USA Act includes my proposals to provide the substantial and long overdue assistance for our law enforcement and border control efforts along the Northern Border. My home state of Vermont has seen huge increases in customs and INS activity since the signing of NAFTA. The number of people coming through our borders has risen steeply over the years, but our staff and our resources have not.

I proposed—and this legislation authorizes in section 402—tripling the number of Border Patrol, INS inspectors, and customs Service employees in each of the States along the 4,000-mile Northern Border. I was gratified when 22 Senators—Democrats and Republicans—wrote to the President supporting such an increase, and I am pleased that the Administration agreed that this critical law enforcement improvement should be included in the bill. Senators CANTWELL and SCHUMER in the Committee and Senators MURRAY and DORGAN have been especially strong advocates of these provisions and I thank them for their leadership. In addition, the USA Act, in section 401, authorizes the Attorney General to waive the FTE cap on INS personnel in order to address the national security needs of the United States on the northern border. Now more than ever, we must patrol our border vigilantly and prevent those who wish America harm from gaining entry. At the same time, we must work with the Canadians to allow speedy crossing to legitimate visitors and foster the continued growth of trade which is beneficial to both countries.

In addition to providing for more personnel, this bill also includes, in section 402(4), my proposal to provide $100 million in funding for both the INS and the Customs Service to improve the technology used to monitor the Northern Border and to purchase additional equipment. The bill also includes, in section 403(c), an important provisions from Senator CANTWELL directing the Attorney General, in consultation with other agencies, to develop a technical standard for identifying electronically the identity of persons applying for visas or seeking to enter the United States. In short, this bill provides a comprehensive high-tech boost for the security of our nation.

This bill also includes important proposals to enhance data sharing. The bill, in section 403, directs the Attorney General and the FBI Director to give the State Department and INS access to the criminal history information in the FBI's National Crime Information Center (NCIC) database, as the Administration and I both proposed. The Attorney General is directed to report back to the Congress in two years on progress in implementing this requirement. We have also adopted the Administration's language, in section 413, to make it easier for the State Department to share information with foreign governments for aid in terrorist investigations.

Criminal justice improvements. The USA Act contains a number of provisions intended to improve and update the federal criminal code to address better the nature of terrorist activity, assist the FBI in translating foreign language information collected, and ensure that federal prosecutors are unhindered by conflicting local rules of conduct to get the job done. I will mention just a few of these provisions.

FBI translators. The truth certainly seems self-evident that all the best surveillance techniques in the world will not help this country defend itself from terrorist attack if the information cannot be understood in a timely fashion. Indeed, within days of the September 11, the FBI Director issued an employment ad on national TV by calling upon those who speak Arabic to apply for a job as an FBI translator. This is a dire situation that needs attention. I am therefore gratified that the Administration accepted by proposal, in section 205, to waive any federal personnel requirements and limitations imposed by any other law in order to expedite the hiring of translators at the FBI.

This bill also directs the FBI Director to establish such security requirements as are necessary for the personnel employed as translators. We know the effort to recruit translators has a high priority, and the Congress should provide all possible support. Therefore, the bill calls on the Attorney General to report to the Judiciary Committees on the number of translators employed by the Justice Department, any legal or practical impediments to using translators employed by other Federal, State, or local agencies, on a full, part-time, or shared basis; and the needs of the FBI for specific translation services in certain languages, and recommendations for meeting those needs.

Federal crime of terrorism. The Administration's initial proposal assembled a laundry list of more than 40 Federal crimes ranging from computer hacking to malicious mischief to the use of weapons of mass destruction, and designated them as "Federal terrorism offenses," regardless of the circumstances under which they were committed. For example, a teenager who spammed the NASA website and, as a result, recklessly caused damage, would be deemed to have committed this new "terrorism" offense. Under the Administration's proposal, the consequences of this designation were severe. Crimes on the list would carry no statute of limitations. The maximum penalties would shoot up to life imprisonment, and those released earlier would be subject to a lifetime of supervised release. Moreover, anyone who harbored a person whom he had "reasonable grounds to suspect" had committed, or was about to commit, a "Federal terrorism offense"—whether it was the Taliban or the mother of my hypothetical teenage computer hacker—would be subject to stiff criminal penalties. I worked closely with the Administration to ensure that the definition of "terrorism" in the USA Act fit the crime.

First, we have trimmed the list of crimes that may be considered as terrorism predicates in section 808 of the bill. This shorter, more focused list, to be codified at 18 U.S.C. §2332(g)(5)(B), more closely reflects the sorts of offenses committed by terrorists.

Second, we have provided, in section 810, that the current 8-year limitations period for this new set of offenses will remain in place, except where the commission of the offense resulted in, or created a risk of, death or serious bodily injury.

Third, rather than make an across-the-board, one-size-fits-all increase of the penalties for every offense on the list, without regard to the severity of the offense, we have made, in section 811, more measured increases in maximum penalties where appropriate, including life imprisonment or lifetime supervised release in cases in which the offense resulted in death. We have also added, in section 812, conspiracy provisions to a few criminal statutes where appropriate, with penalties equal to the penalties for the object offense, up to life imprisonment.

Finally, we have more carefully defined the new crime of harboring terrorists in section 804, so that it applies only to those harboring people who have committed, or are about to commit, the most serious of federal terrorism-related crimes, such as the use of weapons of mass destruction. Moreover, it is not enough that the defendant had "reasonable grounds to suspect" that the person he was harboring had committed, or was about to commit, such a crime; the government must prove that the defendant knew or had "reasonable grounds to believe" that this was so.

McDade fix. The massive investigation underway into who was responsible for and assisted in carrying out the September 11 attacks stretches across state and national boundaries. While the scope of the tragedy is unsurpassed, the disregard for state and national borders of this criminal conspiracy is not unusual. Federal investigative officers and prosecutors often must follow leads and conduct investigations outside their assigned jurisdictions. At the end of the 105th Congress, a legal impediment to such multi-jurisdiction investigations was slipped into the omnibus appropriations bill, over the objection at the time of every member of the Senate Judiciary Committee.

I have spoken many times over the past two years of the problems caused by the so-called McDade law, 28 U.S.C. §530B. According to the Justice Department, the McDade law has delayed important criminal investigations, prevented the use of effective and traditionally-accepted investigative techniques, and served as the basis of litigation to interfere with legitimate federal prosecutions. At a time when we need federal law enforcement authorities to move quickly to catch those responsible for the September 11th attacks, and to prevent further attacks on our country, we can no longer tolerate the drag on federal investigations and prosecutions caused by this ill-considered legislation.

On September 19th, I introduced S. 1437, the Professional Standards for Government Attorneys Act of 2001, along with Senators HATCH and WYDEN. This bill proposes to modify the McDade law by establishing a set of rules that clarify the professional standards applicable to government attorneys. I am delighted that the Administration recognized the importance of S. 1437 for improving federal law enforcement and combating terrorism, and agreed to its inclusion as section 501 of the USA Act.

The first part of section 501 embodies the traditional understanding that when lawyers handle cases before a Federal court, they should be subject to the Federal court's standards of professional responsibility, and not to the possibly inconsistent standards of other jurisdictions. By incorporating this ordinary choice-of-law principle, the bill preserves the Federal courts' traditional authority to oversee the professional conduct of Federal trial lawyers, including Federal prosecutors. It thus avoids the uncertainties presented by the McDade law, which potentially subjects Federal prosecutors to State laws, rules of criminal procedure, and judicial decisions which differ from existing Federal law.

Another part of section 501 specifically addresses the situation in Oregon, where a state court ruling has seriously impeded the ability of Federal agents to engage in undercover operations and other covert activities. See In re Gatti, 330 Or. 517 (2000). Such activities are legitimate and essential crime-fighting tools. The Professional Standards for Government Attorneys Act ensures that these tools will be available to combat terrorism.

Finally, section 501 addresses the most pressing contemporary question of government attorney ethics—namely, the question of which rule should govern government attorneys' communications with represented persons. It asks the Judicial Conference of the United States to submit to the Supreme Court a proposed uniform national rule to govern this area of professional conduct, and to study the need for additional national rules to govern other areas in which the proliferation of local rules may interfere with effective Federal law enforcement. The Rules Enabling Act process is the ideal one for developing such rules, both because the Federal judiciary traditionally is responsible for overseeing the conduct of lawyers in Federal court proceedings, and because this process would best provide the Supreme Court an opportunity fully to consider and objectively to weigh all relevant considerations.

The problems posed to Federal law enforcement investigations and prosecutions by the McDade law are real and urgent. The Professional Standards for Government Attorneys Act provides a reasonable and measured alternative: It preserves the traditional role of the State courts in regulating the conduct of attorneys licensed to practice before them, while ensuring that Federal prosecutors and law enforcement agents will be able to use traditional Federal investigative techniques. We need to pass this corrective legislation before more cases are compromised.

Terrorist attacks against mass transportation systems. Another provision of the USA Act that was not included in the Administration's initial proposal is section 801, which targets acts of terrorism and other violence against mass transportation systems. Just last week, a Greyhound bus crashed in Tennessee after a deranged passenger slit the driver's throat and then grabbed the steering wheel, force the bus into the oncoming traffic. Six people were killed in the crash. Because there are currently no federal law addressing terrorism of mass transportation systems, however, there may be no federal jurisdiction over such as case, even if it were committed by suspected terrorists. Clearly, there is an urgent need for strong criminal legislation to deter attacks against mass transportation systems. Section 801 will fill this gap.

Cybercrime. The Computer Fraud and Abuse Act, 18 U.S.C. §1030, is the primary federal criminal statue prohibiting computer frauds and hacking. I worked with Senator HATCH in the last Congress to make improvements to this law in the Internet Security Act, which passed the Senate as part of another bill. Our work is included in section 815 of the USA Act. This section would amend the statute to clarify the appropriate scope of federal jurisdiction. First, the bill adds a definition of "loss" to cover any reasonable cost to the victim in responding to a computer hacker. Calculation of loss is important both in determining whether the $5,000 jurisdictional hurdle in the statute is met, and, at sentencing, in calculating the appropriate guideline range and restitution amount.

Second, the bill amends the definitions of "protected computer" to include qualified computers even when they are physically located outside of the United States. This clarification will preserve the ability of the United States to assist in internal hacking cases.

Finally, this section eliminates the current directive to the Sentencing Commission requiring that all violations, including misdemeanor violations, of certain provisions of the Computer Fraud and Abuse Act be punished with a term of imprisonment of at least six months.

Biological weapons. Borrowing from a bill introduced in the last Congress By Senator BIDEN, the USA Act contains a provision in section 802 to strengthen our federal laws relating to the threat of biological weapons. Current law prohibits the possession, development, or acquisition of biological agents or toxins "for use as a weapon." This section amends the definition of "for use as a weapon" to include all situations in which it can be proven that the defendant had any purpose other than a peaceful purpose. This will enhance the government's ability to prosecute suspected terrorists in possession of biological agents or toxins, and conform the scope of the criminal offense in 18 U.S.C. §175 more closely to the related forfeiture provision in 18 U.S.C. §176. This section also contains a new statute, 18 U.S.C. §175b, which generally makes it an offense for certain restricted persons, including non-resident aliens from countries that support international terrorism, to possess a listed biological agent or toxin.

Of greater consequence, section 802 defines another additional offense, punishable by up to 10 years in prison, of possessing a biological agent, toxin, or delivery system "of a type or in a

quantity that, under the circumstances," is not reasonably justified by a peaceful purpose. As originally proposed by the Administration, this provision specifically stated that knowledge of whether the type or quantity of the agent or toxin was reasonably justified was not an element of the offense. Thus, although the burden of proof is always on the government, every person who possesses a biological agent, toxin, or delivery system was at some level of risk. I am pleased that the Administration agreed to drop this portion of the provision.

Nevertheless, I remain troubled by the subjectivity of the substantive standard for violation of this new criminal prohibition, and question whether it provides sufficient notice under the Constitution. I also share the concerns of the American Society for Microbiology and the Association of American Universities that this provision will have a chilling effect upon legitimate scientific inquiry that offsets any benefit in protecting against terrorism. While we have tried to prevent against this by creating an explicit exclusion for "bona fide research," this provision may yet prove unworkable, unconstitutional, or both. I urge the Justice Department and the research community to work together on substitute language that would provide prosecutors with a more workable tool.

Secret Service jurisdiction. Two sections of the USA Act were added at the request of the United States Secret Service, with the support of the Administration. I was pleased to accommodate the Secret Service by including these provisions in the bill to expand Electronic Crimes Task Force and to clarify the authority of the Secret Service to investigator computer crimes.

The Secret Service is committed to the development of new tools to combat the growing areas of financial crime, computer fraud, and cyberterrorism. Recognizing a need for law enforcement, private industry and academia to pool their resources, skills and revision to combat criminal elements in cyberspace, the Secret Service created the New York Electronic Crimes Task Force (NYECTF). This highly successful model is comprised of over 250 individual members, including 50 different Federal, State and local enforcement agencies, 100 private companies, and 9 universities. Since its inception in 1995, the NYECTF has successfully investigated a range of financial and electronic crimes, including credit card fraud, identify theft, bank fraud, computer systems intrusions, and e-mail threats against protectees of the Secret Service. Section 105 of the USA Act authorizes the Secret Service to develop similar task forces in cities and regions across the country where critical infrastructure may be vulnerable to attacks from terrorists or other cyber-criminals.

Section 507 of the USA Act gives the Secret Service concurrent jurisdiction to investigate offenses under 18 U.S.C. §1030, relating to fraud and related activity in connection with computers. Prior to the 1996 amendments to the Computer Fraud and Abuse Act, the Secret Service was authorized to investigate any an all violations of section 1030, pursuant to an agreement between the Secretary of Treasury and the Attorney General. The 1996 amendments, however, concentrated Secret Service jurisdiction on certain specified subsections of section 1030. The current amendment would return full jurisdiction to the Secret Service and would allow the Justice and Treasury Departments to decide on the appropriate work-sharing balance between the two. This will enable the Secret Service to investigate a wide range of potential White House network intrusions, as well as intrusions into remote sites (outside of the White House) that could impact the safety and security of its protectees, and to continue its mission to protect the nation's critical infrastructure and financial payment systems.

Counter-terrorism Fund. The USA Act also authorizes, for the first time, a counter-terrorism fund in the Treasury of the United States to reimburse Justice Department for any costs incurred in connection with the fight against terrorism.

Specifically, this counter-terrorism fund will: (1) reestablish an office or facility that has been damaged as the result of any domestic or international terrorism incident; (2) provide support to counter, investigate, or prosecute domestic or international terrorism, including paying rewards in connection with these activities; (3) conduct terrorism threat assessments of Federal agencies; and (4) for costs incurred in connection with detaining individuals in foreign countries who are accused of acts of terrorism in violation of United States law.

I first authored this counter-terrorism fund in the S. 1319, the 21st Century Department of Justice Appropriations Authorization Act, which Senator HATCH and I introduced in August.

Enhanced surveillance procedures. The USA Act provides enhanced surveillance procedures for the investigation of terrorism and other crimes. The challenge before us has been to strike a reasonable balance to protect both security and the liberties of our people. In some respects, the changes made are appropriate and important ones to update surveillance and investigative procedures in light of new technology and experience with current law. Yet, in other respects, I have deep concerns that we may be increasing surveillance powers and the sharing of criminal justice information without adequate checks on how information may be handled and without adequate accountability in the form of judicial review.

The bill contains a number of sensible proposals that should not be controversial.

Wiretap predicates. For example, sections 201 and 202 of the USA Act would add to the list of crimes that may be used as predicates for wiretaps certain offenses which are specifically tailored to the terrorist threat. In addition to crimes that relate directly to terrorism, the list would include crimes of computer fraud and abuse which are committed by terrorists to support and advance their illegal objectives.

FISA roving wiretraps. The bill, in section 206, would authorize the use of roving wiretaps in the course of a foreign intelligence investigation and brings FISA into line with criminal procedures that allow surveillance to follow a person, rather than requiring a separate court order identifying each telephone company or other communication common carrier whose assistance is needed. This is a matter on which the Attorney General and I reached early agreement. This is the kind of change that has a compelling justification, because it recognizes the ease with which targets of investigations can evade surveillance by changing phones. In fact, the original roving wiretap authority for use in criminal investigations was enacted as part of the Electronic Communications Privacy Act (ECPA) in 1986. I was proud to be the primary Senate sponsor of that earlier law.

Paralleling the statutory rules applicable to criminal investigations, the formulation I originally proposed made clear that this roving wiretap authority must be requested in the application before the FISA court was authorized to order such roving surveillance authority. Indeed, the Administration agrees that the FISA court may not grant such authority sua sponte. Nevertheless, we have accepted the Administration's formulation of the new roving wiretap authority, which requires the FISA court to make a finding that the actions of the person whose communications are to be intercepted could have the effect of thwarting the identification of a specified facility or place. While no amendment is made to the statutory directions for what must be included in the application for a FISA electronic surveillance order, these applications should include the necessary information to support the FISA court's finding that roving wiretap authority is warranted.

Search warrants. The USA Act, in section 219, authorizes nationwide service of search warrants in terrorism investigations. This will allow the judge who is most familiar with the developments in a fast-breaking and complex terrorism investigation to make determinations of probable cause, no matter where the property to be searched is located. This will not only save time by avoiding having to bring up-to-speed another judge in another jurisdiction where the property is located, but also serves privacy and Fourth Amendment interests in ensuring that the most knowledgeable judge makes the determination of probable cause. The bill, in section 209, also authorizes voice mail messages to be seized on the authority

of a probable cause search warrant rather than through the more burdensome and time-consuming process of a wiretap.

Electronic records. The bill updates the laws pertaining to electronic records in three primary ways. First, in section 210, the bill authorizes the nationwide service of subpoenas for subscriber information and expands the list of items subject to subpoena to include the means and source of payment for the service.

Second, in section 211, the bill equalizes the standard for law enforcement access to cable subscriber records on the same basis as other electronic records. The Cable Communications Policy Act, passed in 1984 to regulate various aspects of the cable television industry, did not take into account the changes in technology that have occurred over the last fifteen years. Cable television companies now often provide Internet access and telephone service in addition to television programming. This amendment clarifies that a cable company must comply with the laws governing the interception and disclosure of wire and electronic communications just like any other telephone company or Internet service provider. The amendments would retain current standards that govern the release of customer records for television programming.

Finally, the bill, in section 212, permits, but does not require, an electronic communications service to disclose the contents of and subscriber information about communications in emergencies involving the immediate danger of death or serious physical injury. Under current law, if an ISP's customer receives an e-mail death threat from another customer of the same ISP, and the victim provides a copy of the communication to the ISP, the ISP is limited in what actions it may take. On one hand, the ISP may disclose the contents of the forwarded communication to law enforcement (or to any other third party as it sees fit). See 18 U.S.C. §2702(b)(3). On the other hand, current law does not expressly authorize the ISP to voluntarily provide law enforcement with the identity, home address, and other subscriber information of the user making the threat. See 18 U.S.C. §2703(c)(1)(B),(C) (permitting disclosure to government entities only in response to legal process). In those cases where the risk of death or injury is imminent, the law should not require providers to sit idly by. This voluntary disclosure, however, in no way creates an affirmative obligation to review customer communications in search of such imminent dangers.

Also, under existing law, a provider (even one providing services to the public) may disclose the contents of a customer's communications—to law enforcement or anyone else—in order to protect its rights or property. See 18 U.S.C. §2702(b)(5). However, the current statute does not expressly permit a provider voluntarily to disclose non-content records (such as a subscriber's login records) to law enforcement for purposes of self-protection. See 18 U.S.C. §2703(c)(1)(B). Yet the right to disclose the content of communications necessarily implies the less intrusive ability to disclose non-content records. Cf. United States v. Auler, 539 F.2d 642, 646 n.9 (7th Cir. 1976) (phone company's authority to monitor and disclose conversations to protect against fraud necessarily implies right to commit lesser invasion of using, and disclosing fruits of, pen register device) (citing United States v. Freeman, 524 F.2d 337, 341 (7th Cir. 1975)). Moreover, as a practical matter providers must have the right to disclose the facts surrounding attacks on their systems. When a telephone carrier is defrauded by a subscriber, or when an ISP's authorized user launches a network intrusion against his own ISP, the provider must have the legal ability to report the complete details of the crime to law enforcement. The bill clarifies that service providers have the statutory authority to make such disclosures.

Pen registers. There is consensus that the existing legal procedures for pen register and trap-and-trace authority are antiquated and need to be updated. I have been proposing ways to update the pen register and trap and trace statutes for several years, but not necessarily in the same ways as the Administration initially proposed. In fact, in 1998, I introduced with then-Senator Ashcroft, the E-PRIVACY Act, S. 2067, which proposed changes in the pen register laws. In 1999, I introduced the E-RIGHTS Act, S. 934, also with proposals to update the pen register laws.

Again, in the last Congress, I introduced the Internet Security Act, S. 2430, on April 13, 2000, that proposed (1) changing the pen register and trap and trace device law to give nationwide effect to pen register and trap and trace orders obtained by Government attorneys and obviate the need to obtain identical orders in multiple federal jurisdictions; (2) clarifying that such devices can be used for computer transmissions to obtain electronic addresses, not just on telephone lines; and (3) as a guard against abuse, providing for meaningful judicial review of government attorney applications for pen registers and trap and trace devices.

As the outline of my earlier legislation suggests, I have long supported modernizing the pen register and trap and trace device laws by modifying the statutory language to cover the use of these orders on computer transmissions; to remove the jurisdictional limits on service of these orders; and to update the judicial review procedure, which, unlike any other area in criminal procedure, bars the exercise of judicial discretion in reviewing the justification for the order. The USA Act, in section 216, updates the pen register and trap and trace laws only in two out of three respects I believe are important, and without allowing meaningful judicial review. Yet, we were able to improve the Administration's initial proposal, which suffered from the same problem as the provision that was hastily taken up and passed by the Senate, by voice vote, on September, 13, 2001, as an amendment to the Commerce Justice State Appropriations Act.

Nationwide service. The existing legal procedures for pen register and trap-and-trace authority require service of individual orders for installation of pen register or trap and trace device on the service providers that carried the targeted communications. Deregulation of the telecommunications industry has had the consequence that one communication may be carried by multiple providers. For example, a telephone call may be carried by a competitive local exchange carrier, which passes it at a switch to a local Bell Operating Company, which passes it to a long distance carrier, which hands it to an incumbent local exchange carrier elsewhere in the U.S., which in turn may finally hand it to a cellular carrier. If these carriers do not pass source information with each call, identifying that source may require compelling information from a host of providers located throughout the country.

Under present law, a court may only authorize the installation of a pen register or trap device "within the jurisdiction of the court." As a result, when one provider indicates that the source of a communication is a carrier in another district, a second order may be necessary. The Department of Justice has advised, for example, that in 1996, a hacker (who later turned out to be launching his attacks from a foreign country) extensively penetrated computers belonging to the Department of Defense. This hacker was dialing into a computer at Harvard University and used this computer as an intermediate staging point in an effort to conceal his location and identity. Investigators obtained a trap and trace order instructing the phone company, Nynex, to trace these calls, but Nynex could only report that the communications were coming to it from a long-distance carrier, MCI. Investigators then applied for a court order to obtain the connection information from MCI, but since the hacker was no longer actually using the connection, MCI could not identify its source. Only if the investigators could have served MCI with a trap and trace order while the hacker was actively on-line could they have successfully traced back and located him.

In another example provided by the Department of Justice, investigators encountered similar difficulties in attempting to track Kevin Mitnick, a criminal who continued to hack into computers attached to the Internet despite the fact that he was on supervised release for a prior computer crime conviction. The FBI attempted to trace

these electronic communications while they were in progress. In order to evade arrest, however, Mitnick moved around the country and used cloned cellular phones and other evasive techniques. His hacking attacks would often pass through one of two cellular carriers, a local phone company, and then two Internet service providers. In this situation, where investigators and service providers had to act quickly to trace Mitnick in the act of hacking, only many repeated attempts—accompanied by an order to each service provider—finally produced success. Fortunately, Mitnick was such a persistent hacker that he gave law enforcement many chances to complete the trace.

This duplicative process of obtaining a separate order for each link in the communications chain can be quite time-consuming, and it serves no useful purpose since the original court has already authorized the trace. Moreover, a second or third order addressed to a particular carrier that carried part of a prior communication may prove useless during the next attack: in computer intrusion cases, for example, the target may use an entirely different path (i.e., utilize a different set of intermediate providers) for his or her subsequent activity.

The bill would modify the pen register and trap and trace statutes to allow for nationwide service of a single order for installation of these devices, without the necessity of returning to court for each new carrier. I support this change.

Second, the language of the existing statute is hopelessly out of date and speaks of a pen register or trap and trace "device" being "attached" to a telephone "line." However, the rapid computerization of the telephone system has changed the tracing process. No longer are such functions normally accomplished by physical hardware components attached to telephone lines. Instead, these functions are typically performed by computerized collection and retention of call routing information passing through a communications system.

The statute's definition of a "pen register" as a "device" that is "attached" to a particular "telephone line" is particularly obsolete when applied to the wireless portion of a cellular phone call, which has no line to which anything can be attached. While courts have authorized pen register orders for wireless phones based on the notion of obtaining access to a "virtual line," updating the law to keep pace with current technology is a better course.

Moreover, the statute is ill-equipped to facilitate the tracing of communications that take place over the Internet. For example, the pen register definition refers to telephone "numbers" rather than the broader concept of a user's communications account. Although pen register and trap orders have been obtained for activity on computer networks, Internet service providers have challenged the application of the statute to electronic communications, frustrating legitimate investigations. I have long supported updating the statute by removing words such as "numbers . . . dialed" that do not apply to the way that pen/trap devices are used and to clarify the statute's proper application to tracing communications in an electronic environment, but in a manner that is technology neutral and does not capture the content of communications. That being said, I have been concerned about the FBI and Justice Department's insistence over the past few years that the pen/trap devices statutes be updated with broad, undefined terms that continue to flame concerns that these laws will be used to intercept private communications content.

The Administration's initial pen/trap device proposal added the terms "routing" and "addressing" to the definitions describing the information that was authorized for interception on the low relevance standard under these laws. The Administration and the Department of Justice flatly rejected my suggestion that these terms be defined to respond to concerns that the new terms might encompass matter considered content, which may be captured only upon a showing of probable cause, not the mere relevancy of the pen/trap statute. Instead, the Administration agreed that the definition should expressly exclude the use of pen/trap devices to intercept "content," which is broadly defined in 18 U.S.C. 2510(8).

While this is an improvement, the FBI and Justice Department are shortsighted in their refusal to define these terms. We should be clear about the consequence of not providing definitions for these new terms in the pen/trap device statutes. These terms will be defined, if not by the Congress, then by the courts in the context of criminal cases where pen/trap devices have been used and challenged by defendants. If a court determines that a pen register has captured "content," which the FBI admits such devices do, in violation of the Fourth Amendment, suppression may be ordered, not only of the pen register evidence but any other evidence derived from it. We are leaving the courts with little or no guidance of what is covered by "addressing" or "routing."

The USA Act also requires the government to use reasonably available technology that limits the interceptions under the pen/trap device laws "so as not to include the contents of any wire or electronic communications." This limitation on the technology used by the government to execute pen/trap orders is important since, as the FBI advised me June, 2000, pen register devices "do capture all electronic impulses transmitted by the facility on which they are attached, including such impulses transmitted after a phone call is connected to the called party." The impulses made after the call is connected could reflect the electronic banking transactions a caller makes, or the electronic ordering from a catalogue that a customer makes over the telephone, or the electronic ordering of a prescription drug.

This transactional data intercepted after the call is connected is "content." As the Justice Department explained in May, 1998 in a letter to House Judiciary Committee Chairman Henry Hyde, "the retrieval of the electronic impulses that a caller necessarily generated in attempting to direct the phone call" does not constitute a "search" requiring probable cause since "no part of the substantive information transmitted after the caller had reached the called party" is obtained. But the Justice Department made clear that "all of the information transmitted after a phone call is connected to the called party . . . is substantive in nature. These electronic impulses are the 'contents' of the call: They are not used to direct or process the call, but instead convey certain messages to the recipient."

When I added the direction on use of reasonably available technology (codified as 18 U.S.C. 3121(c)) to the pen register statute as part of the Communications Assistance for Law Enforcement Act (CALEA) in 1994, I recognized that these devices collected content and that such collection was unconstitutional on the mere relevance standard. Nevertheless, the FBI advised me in June, 2000, that pen register devices for telephone services "continue to operate as they have for decades" and that "there had been no change . . . that would better restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." Perhaps, if there were meaningful judicial review and accountability, the FBI would take the statutory direction more seriously and actually implement it.

Judicial review. Due in significant part to the fact that pen/trap devices in use today collect "content," I have sought in legislation introduced over the past few years to update and modify the judicial review procedure for pen register and trap and trace devices. Existing law requires an attorney for the government to certify that the information likely to be obtained by the installation of a pen register or trap and trace device will be relevant to an ongoing criminal investigation. The court is required to issue an order upon seeing the prosecutor's certification. The court is not authorized to look behind the certification to evaluate the judgment of the prosecutor.

I have urged that government attorneys be required to include facts about their investigations in their applications for pen/trap orders and allow courts to grant such orders only where the facts support the relevancy of the information likely to be obtained by the orders. This is not a change in the applicable standard, which would remain the very low relevancy standard.

Instead, this change would simply allow the court to evaluate the facts presented by a prosecutor, and, if it finds that the facts support the government's assertion that the information to be collected will be relevant, issue the order. Although this change will place an additional burden on law enforcement, it will allow the courts a greater ability to assure that government attorneys are using such orders properly.

Some have called this change a "rollback" in the statute, as if the concept of allowing meaningful judicial review was an extreme position. To the contrary, this is a change that the Clinton Administration supported in legislation transmitted to the Congress last year. This is a change that the House Judiciary Committee also supported last year. In the Electronic Communications Privacy Act, H.R. 5018, that Committee proposed that before a pen/trap device "could be ordered installed, the government must first demonstrate to an independent judge that 'specific and articulable facts reasonably indicate that a crime has been, is being, or will be committed, and information likely to be obtained by such installation and use . . . is relevant to an investigation of that crime." (Report 106-932, 106th Cong. 2d Sess., Oct. 4, 2000, p. 13). Unfortunately, the Bush Administration has taken a contrary position and has rejected this change in the judicial review process.

Computer trespasser. Currently, an owner or operator of a computer that is accessed by a hacker as a means for the hacker to reach a third computer, cannot simply consent to law enforcement monitoring of the computer. Instead, because the owner or operator is not technically a party to the communication, law enforcement needs wiretap authorization under Title III to conduct such monitoring. I have long been interested in closing this loophole. Indeed, when I asked about this problem, the FBI explained to me in June, 2000, that:

> This anomaly in the law creates an untenable situation whereby providers are sometimes forced to sit idly by as they witness hackers enter and, in some situations, destroy or damage their systems and networks while law enforcement begins the detailed process of seeking court authorization to assist them. In the real world, the situation is akin to a homeowner being forced to helplessly watch a burglar or vandal while police seek a search warrant to enter the dwelling.

I therefore introduced as part of the Internet Security Act, S. 2430, in 2000, an exception to the wiretap statute that would explicitly permit such monitoring without a wiretap if prior consent is obtained from the person whose computer is being hacked through and used to send "harmful interference to a lawfully operating computer system."

The Administration initially proposed a different formulation of the exception that would have allowed an owner/operator of any computer connected to the Internet to consent to FBI wiretapping of any user who violated a workplace computer use policy or online service term of service and was thereby an "unauthorized" user. The Administration's proposal was not limited to computer hacking offenses under 18 U.S.C. 1030 or to conduct that caused harm to a computer or computer system. The Administration rejected these refinements to their proposed wiretap exception, but did agree, in section 217 of the USA Act, to limit the authority for wiretapping with the consent of the owner/operator to communications of unauthorized users without an existing subscriber or other contractual relationship with the owner/operator.

Sharing criminal justice information. The USA Act will make significant changes in the sharing of confidential criminal justice information with various Federal agencies. For those of us who have been concerned about the leaks from the FBI that can irreparably damage reputations of innocent people and frustrate investigations by alerting suspects to flee or destroy material evidence, the Administration's insistence on the broadest authority to disseminate such information, without any judicial check, is disturbing. Nonetheless, I believe we have improved the Administration's initial proposal in responsible ways. Only time will tell whether the improvements we were able to reach agreement on are sufficient.

At the outset, we should be clear that current law allows the sharing of confidential criminal justice information, but with close court supervision. Federal Rule of Criminal Procedure 6(e) provides that matters occurring before a grand jury may be disclosed only to an attorney for the government, such other government personnel as are necessary to assist the attorney and another grand jury. Further disclosure is also allowed as specifically authorized by a court.

Similarly, section 2517 of title 18, United States Code provides that wiretap evidence may be disclosed in testimony during official proceedings and to investigative or law enforcement officers to the extent appropriate to the proper performance of their official duties. In addition, the wiretap law allows disclosure of wiretap evidence "relating to offenses other than specified in the order" when authorized or approved by a judge. Indeed, just last year, the Justice Department assured us that "law enforcement agencies have authority under current law to share title III information regarding terrorism with intelligence agencies when the information is of overriding importance to the national security." (Letter from Robert Raben, Assistant Attorney General, September 28, 2000).

For this reason, and others, the Justice Department at the time opposed an amendment proposed by Senators KYL and FEINSTEIN to S. 2507, the "Intelligence Authorization Act for FY 2001 that would have allowed the sharing of foreign intelligence and counterintelligence information collected from wiretaps with the intelligence community. I deferred to the Justice Department on this issue and sought changes in the proposed amendment to address the Department's concern that this provision was not only unnecessary but also "could have significant implications for prosecutions and the discovery process in litigation", "raises significant issues regarding the sharing with intelligence agencies of information collected about United States persons" and jeopardized "the need to protect equities relating to ongoing criminal investigations." In the end, the amendment was revised to address the Justice Department's concerns and passed the Senate as a free-standing bill, S. 3205, the Counterterrorism Act of 2000. The House took no action on this legislation.

Disclosure of wiretap information. The Administration initially proposed adding a sweeping provision to the wiretap statute that broadened the definition of an "investigative or law enforcement officer" who may receive disclosures of information obtained through wiretaps to include federal law enforcement, intelligence, national security, national defense, protective and immigration personnel and the President and Vice President. This proposal troubled me because information intercepted by a wiretap has enormous potential to infringe upon the privacy rights of innocent people, including people who are not even suspected of a crime and merely happen to speak on the telephone with the targets of an investigation. For this reason, the authority to disclose information obtained through a wiretap has always been carefully circumscribed in law.

While I recognize that appropriate officials in the executive branch of government should have access to wiretap information that is important to combating terrorism or protecting the national security, I proposed allowing such disclosures where specifically authorized by a court order. Further, with respect to information relating to terrorism, I proposed allowing the disclosure without a court order as long as the judge who authorized the wiretap was notified as soon as practicable after the fact. This would have provided a check against abuses of the disclosure authority by providing for review by a neutral judicial official. At the same time, there was a little likelihood that a judge would deny any requests for disclosure in cases where it was warranted.

On Sunday, September 30, the Administration agreed to my proposal, but within two days, it backed away from its agreement. I remain concerned that the resulting provision will allow the unprecedented, widespread disclosure of this highly sensitive information without any notification to or review by the court that authorizes and supervises the wiretap. This is clearly an area where our Committee will have to exercise close oversight to

make sure that the newly-minted disclosure authority is not being abused.

The Administration offered three reasons for reneging on the original deal. First, they claimed that the involvement of the court would inhibit Federal investigators and attorneys from disclosing information needed by intelligence and national security officials. Second, they said the courts might not have adequate security and therefore should not be told that information was disclosed for intelligence or national security purposes. And third, they said the President's constitutional powers under Article II give him authority to get whatever foreign intelligence he needs to exercise his national security responsibilities.

I believe these concerns are unfounded. Federal investigators and attorneys will recognize the need to disclose information relevant to terrorism investigations. Courts can be trusted to keep secrets and recognize the needs of the President.

Current law requires that such information be used only for law enforcement purpose. This provides an assurance that highly intrusive invasions of privacy are confined to the purpose for which they have been approved by a court, based on probable cause, as required by the Fourth Amendment. Current law calls for minimization procedures to ensure that the surveillance does not gather information about private and personal conduct and conversations that are not relevant to the criminal investigation.

When the Administration reneged on the agreement regarding court supervision, we turned to other safeguards and were more successful in changing other questionable features of the Administration's bill. The Administration accepted my proposal to strike the term "national security" from the description of wiretap information that may be shared throughout the executive branch and replace it with "foreign intelligence" information. This change is important in clarifying what information may be disclosed because the term "foreign intelligence" is specifically defined by statute whereas "national security" is not.

Moreoever, the rubric of "national security" has been used to justify some particularly unsavory activities by the government in the past. We must have at least some assurance that we are not embarked on a course that will lead to a repetition of these abuses because the statute will now more clearly define what type of information is subject to disclosure. In addition, Federal officials who receive the information may use it only as necessary to the conduct of their official duties. Therefore, any disclosure or use outside the conduct of their official duties remains subject to all limitations applicable to their retention and dissemination of information of the type of information received. This includes the Privacy Act, the criminal penalties for unauthorized disclosure of electronic surveillance information under chapter 119 of title 18, and the contempt penalties for unauthorized disclosure of grand jury information. In addition, the Attorney General must establish procedures for the handling of information that identifies a United States person, such as the restrictions on retention and dissemination of foreign intelligence and counterintelligence information pertaining to United States persons currently in effect under Executive Order 12333.

While these safeguards do not fully substitute for court supervision, they can provide some assurance against misuse of the private, personal, and business information about Americans, that is acquired in the course of criminal investigations and that may flow more widely in the intelligence, defense, and national security worlds.

Disclosure of grand jury information. The wiretap statute was not the only provision in which the Administration sought broader authority to disclose highly sensitive investigative information. It also proposed broadening Rule 6(e) of the Federal Rules of Criminal Procedure to allow the disclosure of information relating to terrorism and national security obtained from grand jury proceedings to a broad range of officials in the executive branch of government. As with wiretaps, few would disagree that information learned in a criminal investigation that is necessary to combating terrorism or protecting the national security ought to be shared with the appropriate intelligence and national security officials. The question is how best to regulate and limit such disclosures so as not to compromise the important policies of secrecy and confidentiality that have long applied to grand jury proceedings.

I proposed that we require judicial review of requests to disclose terrorism and foreign intelligence information to officials in the executive branch beyond those already authorized to receive such disclosures. Once again, the Administration agreed to my proposal on Sunday, September 30, but reneged within two days. As a result, the bill does not provide for any judicial supervision of the new authorization for dissemination of grand jury information throughout the executive branch. The bill does contain the safeguards that I have discussed with respect to law enforcement wiretap information. However, as with the new wiretap disclosure authority, I am troubled by this issue and plan to exercise the close oversight of the Judiciary Committee to make sure it is not being abused.

Foreign intelligence information sharing. The Administration also sought a provision that would allow the sharing of foreign intelligence information throughout the executive branch of the government notwithstanding any current legal prohibition that may prevent or limit its disclosure. I have resisted this proposal more strongly than anything else that still remains in the bill. What concerns me is that it is not clear what existing prohibitions this provision would affect beyond the grand jury secrecy rule and the wiretap statute, which are already covered by other provisions in the bill. Even the Administration, which wrote this provision, has not been able to provide a fully satisfactory explanation of its scope.

If there are specific laws that the Administration believes impede the necessary sharing of information on terrorism and foreign intelligence within the executive branch, we should address those problems through legislation that is narrowly targeted to those statutes. Tacking on a blunderbuss provision whose scope we do not fully understand can only lead to consequences that we cannot foresee. Further, I am concerned that such legislation, broadly authorizing the secret sharing of intelligence information throughout the executive branch, will fuel the unwarranted fears and dark conspiracy theories of Americans who do not trust their government. This was another provision of which the Administration reneged on its agreement with me; it agreed to drop it on September 30, but resurrected it within two days, insisting that it remain in the bill. I have been able to mitigate its potential for abuse somewhat by adding the same safeguards that apply to disclosure of law enforcement wiretap and grand jury information.

"Sneak and peek" search warrants. Another issue that has caused me serious concern relates to the Administration's proposal for so-called "sneak and peek" search warrants. The House Judiciary Committee dropped this proposal entirely from its version of the legislation. Normally, when law enforcement officers execute a search warrant, they must leave a copy of the warrant and a receipt for all property seized at the premises searched. Thus, even if the search occurs when the owner of the premises is not present, the owner will receive notice that the premises have been lawfully searched pursuant to a warrant rather than, for example, burglarized.

Two circuit courts of appeal, the Second and the Ninth Circuits, have recognized a limited exception to this requirement. When specifically authorized by the issuing judge or magistrate, the officers may delay providing notice of the search to avoid compromising an ongoing investigation or for some other good reason. However, this authority has been carefully circumscribed.

First, the Second and Ninth Circuit cases have dealt only with situations where the officers search a premises without seizing any tangible property. As the Second Circuit explained, such searches are "less intrusive than a conventional search with physical seizure because the latter deprives the owner not only of privacy but also of the use of his property." United States v. Villegas, 899 F.2d 1324, 899 F.2d 1324, 1337 (2d Cir. 1990).

Second, the cases have required that the officers seeking the warrant must show good reason for the delay. Finally, while the courts have allowed notice of the search may be delayed, it must be provided within a reasonable period thereafter, which should generally be no more than seven days. The reasons for these careful limitations were spelled out succinctly by Judge Sneed of the Ninth Circuit: "The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment, demands that surreptitious entries be closely circumscribed." United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986).

The Administration's original proposal would have ignored some of the key limitations created by the caselaw for sneak and peek search warrants. First, it would have broadly authorized officers not only to conduct surreptitious searches, but also to secretly seize any type of property without any additional showing of necessity. This type of warrant, which has never been addressed by a published decision of a federal appellate court, has been referred to in a law review article written by an FBI agent as a "sneak and steal" warrant. See K. Corr, "Sneaky But Lawful: The Use of Sneak and Peek Search Warrants," 43 U. Kan. L. Rev. 1103, 1113 (1995). Second, the proposal would simply have adopted the procedural requirements of 18 U.S.C. § 2705 for providing delayed notice of a wiretap. Among other things, this would have extended the permissible period of delay to a maximum of 90 days, instead of the presumptive seven-day period provided by the caselaw on sneak and peek warrants.

I was able to make significant improvements in the Administration's original proposal that will help to ensure that the government's authority to obtain sneak and peek warrants is not abused. First, the provision that is now in section 213 of the bill prohibits the government from seizing any tangible property or any wire or electronic communication or stored electronic information unless it makes a showing of reasonable necessity for the seizure. Thus, in contrast to the Administration's original proposal, the presumption is that the warrant will authorize only a search unless the government can make a specific showing of additional need for a seizure. Second, the provision now requires that notice be given within a reasonable time of the execution of the warrant rather than giving a blanket authorization for up to a 90-day delay. What constitutes a reasonable time, of course, will depend upon the circumstances of the particular case. But I would expect courts to be guided by the teachings of the Second and the Ninth Circuits that, in the ordinary case, a reasonable time is no more than seven days.

FISA. Several changes in the Foreign Intelligence Surveillance Act (FISA) are designed to clarify technical aspects of the statutory framework and take account of experience in practical implementation. These changes are not controversial, and they will facilitate the collection of intelligence for counterterrorism and counterintelligence purposes. Other changes are more significant and required careful evaluation and revision of the Administration's proposals.

Duration of surveillance. The USA Act, in section 297, changes the duration of electronic surveillance under FISA in cases of an agent of a foreign power, other than a United States persons, who acts in the United States as an officer or employee of a foreign power or as a member of an international terrorist group. Current law limits court orders in these cases to 90 days, the same duration as for United States persons. Experience indicates, however, that after the initial period has confirmed probable cause that the foreign national meets the statutory standard, court orders are renewed repeatedly and the 90-day renewal becomes an unnecessary procedural for investigators taxed with far more pressing duties.

The Administration proposed that the period of electronic surveillance be changed from 90 days to one year in these cases. This proposal did not ensure adequate review after the initial stage to ensure that the probable cause determination remained justified over time. Therefore, the bill changes the initial period of the surveillance 90 to 120 days and changes the period for extensions from 90 days to one year. The initial 120-day period provides for a review of the results of the surveillance or search directed at an individual before one-year extensions are requested. These changes do not affect surveillance of a United States person.

The bill also changes the period for execution of an order for physical search under FISA from 45 to 90 days. This change applies to United States persons as well as foreign nationals. Experience since physical search authority was added to FISA in 1994 indicates that 45 days is frequently not long enough to plan and carry out a covert physical search. There is no change in the restrictions which provide that United States persons may not be the targets of search or surveillance under FISA unless a judge finds probable cause to believe that they are agents of foreign powers who engage in specified international terrorist, sabotage, or clandestine intelligence activities that may involve a violation of the criminal statutes of the United States.

FISA judges. The bill, in section 208, seeks to ensure that the special court established under FISA has sufficient judges to handle the workload. While changing the duration of orders and extensions will reduce the number of cases in some categories, the bill retains the court's role in pen register and trap and trace cases and expands the court's responsibility for issuing orders for records and other tangible items needed for counterintelligence and counter terrorism investigations. Upon reviewing the court's requirements, the Administration requested an increase in the number of federal district judges designated for the court from seven to 11 of whom no less than 3 shall reside within 20 miles of the District of Columbia. The latter provision ensures that more than one judge is available to handle cases on short notice and reduces the need to invoke the alternative of Attorney General approval under the emergency authorities in FISA.

Agent of a foreign power standard. Other changes in FISA and related national security laws are more controversial. In several areas, the bill reflects a serious effort to accommodate the requests for expanded surveillance authority with the need for safeguards against misuse, especially the gathering of intelligence about the lawful political or commercial activities of Americans. One of the most difficult issues was whether to eliminate the existing statutory "agent of a foreign power" standards for surveillance and investigative techniques that raise important privacy concerns, but not at the level that the supreme Court has held to require a court order and a probable cause finding under the Fourth Amendment. These include pen register and trap and trace devices, access to business records and other tangible items held by third parties, and access to records that have statutory privacy protection. The latter include telephone, bank, and credit records.

The "agent of a foreign power" standard in existing law was designed to ensure that the FBI and other intelligence agencies do not use these surveillance and investigative methods to investigate the lawful activities of Americans in the name of an undefined authority to collect foreign intelligence or counterintelligence information. The law has required a showing of reasonable suspicion, less than probable cause, to believe that a United States person is an "agent of a foreign power" engaged in international terrorism or clandestine intelligence activities.

However, the "agent of a foreign power" standard is more stringent than the standard under comparable criminal law enforcement procedures which require only a showing of relevance to a criminal investigation. The FBI's experience under existing laws since they were enacted at various time over the past 15 years has been that, in practice, the requirement to show reasonable suspicion that a person is an "agent of a foreign power" has been almost as burdensome as the requirement to show probable cause required by the Fourth Amendment for more intrusive techniques. The FBI has made a clear case that a relevance standard is appropriate for counterintelligence and counterterrorism investigations, as well as for criminal investigations.

The challenge, then, was to define those investigations. The alternative proposed by the Administration was to cover any investigation to obtain foreign intelligence information. This was extremely broad, because the definition includes any information with respect to a foreign power that relates to, and if concerning a United States person is necessary to, the national defense or the security of the United States or the conduct of the foreign affairs of the United States. This goes far beyond FBI counterintelligence and counterterrorism requirements. Instead, the bill requires that use of the surveillance technique or access to the records concerning a United States person be relevant to an investigation to protect against international terrorism or clandestine intelligence activities.

In addition, an investigation of a United States person may not be based solely on activities protected by the First Amendment. This framework applies to pen registers and trap and trace under section 215, access to records and other items under section 215, and the national security authorities for access to telephone, bank, and credit records under section 506. Lawful political dissent and protest by American citizens against the government may not be the basis for FBI counterintelligence and counterterrorism investigations under these provisions.

A separate issue for pen registers and trap and trace under FISA is whether the court should have the discretion to make the decision on relevance. The Administration has insisted on a certification process. I discussed this issue as it comes up in the criminal procedures for pen registers and trap and trace under title 18, and my concerns apply to the FISA procedures as well.

The purpose of FISA. The most controversial change in FISA requested by the Administration was the proposal to allow surveillance and search when "a purpose" is to obtain foreign intelligence information. Current law requires that the secret procedures and different probable cause standards under FISA be used only if a high-level executive official certifies that "the purpose" is to obtain foreign intelligence formation. The Administration's aim was to allow FISA surveillance and search for law enforcement purposes, so long as there was at least some element of a foreign intelligence purpose. This proposal raised constitutional concerns, which were addressed in a legal opinion provided by the Justice Department, which I insert in the record at the end of my statement.

The Justice Department opinion did not defend the constitutionality of the original proposal. Instead, it addressed a suggestion made by Senator Feinstein to the Attorney General at the Judiciary Committee hearing to change "the purpose" to "a significant purpose." No matter what statutory change is made even the Department concedes that the court's may impose a constitutional requirement of "primary purpose" based on the appellate court decisions upholding FISA against constitutional challenges over the past 20 years.

Section 218 of the bill adopts "significant purpose," and it will be up to the courts to determine how far law enforcement agencies may use FISA for criminal investigation and prosecution beyond the scope of the statutory definition of "foreign intelligence information."

In addition, I proposed and the Administration agreed to an additional provision in Section 505 that clarifies the boundaries for consultation and coordination between officials who conduct FISA search and surveillance and Federal law enforcement officials including prosecutors. Such consultation and coordination is authorized for the enforcement of laws that protect against international terrorism, clandestine intelligence activities of foreign agents, and other grave foreign threats to the nation. Protection against these foreign-based threats by any lawful means is within the scope of the definition of "foreign intelligence information," and the use of FISA to gather evidence for the enforcement of these laws was contemplated in the enactment of FISA. The Justice Department's opinion cites relevant legislative history from the Senate Intelligence Committee's report in 1978, and there is comparable language in the House report.

Immigration. The Administration initially proposed that the Attorney General be authorized to detain any alien indefinitely upon certification of suspicion to links to terrorist activities or organizations. Under close questioning by both Senator KENNEDY and Senator SPECTER at the Committee hearing on September 25, the Attorney General said that his proposal was intended only to allow the government to hold an alien suspected of terrorist activity while deportation proceedings were ongoing. In response to a question by Senator SPECTER, the Attorney General said: "Our intention is to be able to detain individuals who are the subject of deportation proceedings on other grounds, to detain them as if they were the subject of deportation proceedings on terrorism." The Justice Department, however, continued to insist on broader authority, including the power to detain even if the alien was found not to be deportable.

I remain concerned about the provision, in section 412, but I believe that it has been improved from the original proposal offered by the Administration. First, the Justice Department must now charge an alien with an immigration or criminal violation within seven days of taking custody, and the Attorney General's certification of an alien under this section is subject to judicial review. Second, if an alien is found not to be removable, he must be released from custody. Third, the Attorney General can only delegate the power to certify an alien to the Deputy Attorney General, ensuring greater accountability and preventing the certification decision from being made by low-level officials. Despite these improvements, I would have preferred that this provision not be included, and I would urge the Attorney General and his successors to employ great discretion in using this new power.

In addition, the Administration initially proposed a sweeping definition of terrorist activity and new powers for the Secretary of State to designate an organization as a terrorist organization for purposes of immigration law. We were able to work with the Administration to refine this definition to limit its application to individuals who had innocent contacts with non-designated organizations. We also limited the retroactive effect of these new definitions. If an alien solicited funds or membership, or provided material support for an organization that was not designated at that time by the Secretary of State, the alien will have the opportunity to show that he did not know and should have known that his acts would further the organization's terrorist activity. This is substantially better than the administration's proposal, which by its terms, would have empowered the INS to deport someone who raised money for the African National Congress in the 1980s.

Throughout our negotiations on these issues, Senator KENNEDY provided steadfast leadership. Although neither of us are pleased with the final product, it is far better than it would have been without his active involvement.

Trade Sanctions. I was disappointed that the Administration's initial proposal authorizing the President to impose unilateral food and medical sanctions would have undermined a law we passed last year with overwhelming bipartisan support.

Under that law, the President already has full authority to impose unilateral food and medicine sanctions during this crisis because of two exceptions built into the law that apply to our current situation. Nevertheless, the Administration sought to undo this law and obtain virtually unlimited authority in the future to impose food and medicine embargoes, without making any effort for a multi-lateral approach in cooperation with other nations. Absent such a multi-lateral approach, other nations would be free to step in immediately and take over business from American firms and farmers that they are unilaterally barred from pursuing.

Over 30 farm and export groups, including the American Farm Bureau Federation, the Grocery Manufacturers of America, the National Farmers Union, and the U.S. Dairy Export Council, wrote to me and explained that the Administration proposal would "not achieve its intended policy goal."

I worked with Senator ENZI, and other Senators, on substitute language

to give the Administration the tools it needs in this crisis. This substitute has been carefully crafted to avoid needlessly hurting American farmers in the future, yet it will assure that the U.S. can engage in effective multilateral sanctions.

This bipartisan agreement limits the authority in the bill to existing laws and executive orders, which give the President full authority regarding this conflict, and grants authority for the President to restrict exports of agricultural products, medicine or medical devices. I continue to agree with then-Senator Ashcroft who argued in 1999 that unilateral U.S. food and medicine sanctions simply do not work when he introduced the "Food and Medicine for the World Act."

As recently as October 2000, then-Senator Ashcroft pointed out how broad, unilateral embargoes of food or medicine are often counterproductive. Many Republican and Democratic Senators made it clear just last year that the U.S. should work with other countries on food and medical sanctions so that the sanctions will be effective in hurting our enemies, instead of just hurting the U.S. I am glad that with Senator ENZI's help, we were able to make changes in the trade sanctions provision to both protect our farmers and help the President during this crisis.

Money Laundering. Title III of the USA Act consists of a bipartisan bill that was reported out of the Banking Committee on October 4, 2001. I commend the Chairman and Ranking Member of that Committee, Senators SARBANES and GRAMM, for working together to produce a balanced and effective package of measures to combat international money laundering and the financing of terrorism.

I am pleased that the Chairman and Ranking Member of the Banking Committee agreed to our inclusion in the managers' amendment of a small change to a provision of title III, section 319, relating to forfeiture of funds in United States interbank accounts. As reported by the Banking Committee, this provision included language suggesting that in a criminal case, the government may have authority to seek a pretrial restraining order of substitute assets. In fact, as all but one of the circuit courts to consider the issue have held, the government has no such authority. The managers' amendment strikes the offending language from section 319.

Another provision added as part of the Banking Committee title—section 351—is far more troubling. Section 351 creates a new Bank Secrecy Act offense involving the bulk smuggling of more than $10,000 in currency in any conveyance, article of luggage or merchandise or container, either into or out of the United States. The obvious purpose of this section is to circumvent the Supreme Court's decision in United States v. Bajakajian, 118 S. Ct. 2029 (1998), which held that a "punitive" forfeiture violates the Excessive Fines Clause of the Eighth Amendment if it is grossly disproportional to the gravity of the offense it is designed to punish.

In fact, the crime created in section 351—willfully evading a currency reporting requirement by "concealing" and transporting more than $10,000 across a U.S. border—is no different than the crime at issue in Bajakajian—willfully evading a currency reporting requirement by transporting more than $10,000 across a U.S. border. A forfeiture that is "grossly disproportional" with respect to the latter will inevitably be found "grossly disproportional" with respect to the former. The new element of "concealment" does little or nothing to bolster the government's claim to forfeiture of the unreported currency, since this element is already implicit in the current crime of evasion: It is hardly likely that a person who is in the process of willfully evading the currency reporting requirement will be waiving his currency around for all the world to see.

Conclusion. I have done my best under the circumstances and want to thank especially Senator KENNEDY for his leadership on the Immigration parts of the bill. My efforts have not been completely successful and there are a number of provisions on which the Administration has insisted with which I disagree. Frankly, the agreement of September 30, 2001 would have led to a better balanced bill. I could not stop the Administration from reneging on the agreement any more than I could have sped the process to reconstitute this bill in the aftermath of those breaches. In these times we need to work together to face the challenges of international terrorism. I have sought to do so in good faith.

Mr. President, I reserve the remainder of my time and yield the floor.

The PRESIDING OFFICER. Who yields time?

The Senator from Utah.

Mr. HATCH. Mr. President, I enjoyed the remarks of my distinguished colleague from Vermont. I compliment him for the work he has done on this bill and for the hard work, over the last 3 weeks, that he and his staff have put into this bill, as well as other members of the Judiciary Committee as a whole, and, of course, people on my side as well.

Mr. President, I do not intend to take very long. I know our colleagues are tired, and I know they would like to go home. I also know that we have a distinguished colleague in the Chamber who has some amendments on which we may have to vote.

Four weeks ago we were a relatively tranquil nation, but on September 11, in what amounted to a dastardly attack, an unprovoked attack of war, the World Trade Center was destroyed, along with almost 6,000 people, or maybe more. Our Pentagon was struck by a volitionary act of terrorism.

As a result of the acts of heroes, one of the planes was downed in Pennsylvania, killing all aboard, including those heroes who made sure that that plane did not strike either the Capitol or the White House. I want to pay special tribute to those people who were so heroic as to give up their own lives to protect the lives of so many others.

There have been so many acts of heroism and self-sacrifice—the firefighters who gave their lives, the firefighters who worked day and night, the volunteers who have gone in there, the mayor of New York City, the Governor, and so many others who deserve mention.

This bill, hopefully, will help to at least rectify and redeem some of the problems, problems that have existed ever since September 11.

We did not seek this war; it was thrust upon us. It was an unprovoked attack by people who claim that they represent a religious point of view when, in fact, what they represent is a complete distortion of the religion of Islam.

Islamic people do not believe in murder, murdering innocent civilians. The Koran does not teach that. They do not believe in suicide. The Koran does not teach that.

This is not a war against Islam; this is a war against terrorism and people who have so little regard for human life that they would do something against innocent civilians that was unthinkable before September 11.

Therefore, we live in a dangerous and difficult world today. It is a different world. And we are going to have to wake up and do the things we have to do to protect our citizenry and, of course, to protect the rest of the world to the extent this great Nation can, with the help of other nations, a number of which have become supportive of our efforts. We are very grateful to them.

But a lot of people do not realize we have terror cells in this country—that has been in the media even—and there are people in this country who are dedicated to the overthrow of America. There are people who are dedicated to terrorism right here within our Nation. And some of these people who have participated in this matter may very well be people who were rightfully in our Nation—or at least we thought were rightfully in our Nation.

The responsibility of redeeming and rectifying this situation is the responsibility of the Congress, the Justice Department, the FBI, the INS, and the Border Patrol. It is our job to provide the tools, and for them to first identify and then eradicate terrorist activity within our borders. And our President has taken the extraordinary step of saying we are going to go after terrorists worldwide and those who harbor them.

I agree with the President. I think it is time to do it. It is time to hit them where it hurts. It is time to let them know we are not going to put up with this type of activity.

A few weeks ago, the Justice Department sent up its legislative proposal. It

was a good legislative proposal. They had a lot of ideas in there that literally we have been trying to get through for years. When we passed the 1996 antiterrorism, effective death penalty act, a number of us tried to get some of these provisions in at that time, but we were unsuccessful for a variety of reasons, some very sincere.

The fact is, a lot of the provisions we have in the bill are not brand new; a lot of them have been requested for years. And had they been in play, who knows but we might have been able to interdict these terrorists and have stopped what happened and have stopped the loss of civil liberties for approximately 6,000 or more people.

In the past several weeks, after the Justice Department sent up its bill, Senator LEAHY and I, Justice Department officials, White House officials, staff members from both of our staffs, and staff members from other members of the committee have worked day and night to come up with this particular bill.

I congratulate my partner and my colleague, Senator LEAHY, for his hard work on this bill, and his staffers' for the work they have done on this bill, and, of course, my own staffers, and, of course, those others I have named.

This has been a very difficult bill to put forward because there are all kinds of cross-pressures, all kinds of ideas, all kinds of different thoughts, all kinds of differing philosophies. We believe, with all kinds of deliberation and work, we have been able to put together a bill that really makes sense, that will give the Justice Department the tools it needs to be able to work and stamp out terrorist activity within our country. At least we want to give them the very best tools we possibly can.

We have tried to accommodate the concerns of Senators on both sides of the aisle. We have worked very hard to do so. We cannot accommodate everybody's concerns. As Senator LEAHY has said, this is not a perfect bill. Nothing ever seems to be perfect around here. But this is as good a bill as can be put together, in a bipartisan way, in this area in the history of the Senate. I really feel good about it, that we have done this type of a job.

As I say, a lot of these provisions have been requested by the Justice Department and both Democrat and Republican White Houses for years. We took into consideration civil liberties throughout our discussions on this bill. I think we got it just right. We are protective of civil liberties while at the same time giving the tools to the law enforcement agencies to be able to do their jobs in this country.

I might mention that this bill encourages information sharing, that would be absolutely prohibited under current law, among various agencies of Government, information sharing that should have been allowed a long time ago, at least in my view.

It updates the laws with regard to electronic surveillance and brings those laws into the digital age, and brings them into an effective way so that we can, in a modernized way, protect our society, at least to the extent we can, from these types of terrorist activities.

Of course, little things, such as pen registers, trap-and-trace authority—we have been able to resolve these problems after years of problems.

I would like to make a few comments regarding the process for this legislation. Although we have considered this in a more expedited manner than other legislation, my colleagues can be assured that this bill has received thorough consideration. First, the fact is that the bulk of these proposals have been requested by the Department of Justice for years, and have languished in Congress for years because we have been unable to muster the collective political will to enact them into law.

No one can say whether these tools could have prevented the attacks of September 11. But, as the Attorney General has said, it is certain that without these tools, we did not stop the vicious acts of last month. I say to my colleagues, Mr. President, that if these tools could help us now to track down the perpetrators—if they will help us in our continued pursuit of terrorist activities within our national borders then we should not hesitate any further to pass these reforms into law. As long as these reforms are consistent with our—Constitution and they are—it is difficult to see why anyone would oppose their passage.

Furthermore, I would like to clearly dispel the myth that the reforms in this legislation somehow abridge the Constitutional freedoms enjoyed by law-abiding American citizens. Some press reports have portrayed this issue as a choice between individual liberties on the one hand, and on the other hand, enhanced powers for our law enforcement institutions. This is a false dichotomy. We should all take comfort that the reforms in this bill are primarily directed at allowing law enforcement agents to work smarter and more efficiently—in no case do they curtail the precious civil liberties protected by our Constitution. I want to assure my colleagues that we worked very hard over the past several weeks to ensure that this legislation upholds all of the constitutional freedoms our citizens cherish. It does.

Mr. President, I will submit for the RECORD my extended remarks describing this legislation, but I would like to take a minute to explain briefly a few of the most important provisions of this critical legislation.

First, the legislation encourages information-sharing between various arms of the federal government. I believe most of our citizens would be shocked to learn that, even if certain government agents had prior knowledge of the September 11 attacks, under many circumstances they would have been prohibited by law from sharing that information with the appropriate intelligence or national security authorities.

This legislation makes sure that, in the future, such information flows freely within the Federal government, so that it will be received by those responsible for protecting against terrorist attacks.

By making these reforms, we are rejecting the outdated Cold War paradigm that has prevented cooperation between our intelligence community and our law enforcement agents. Current law does not adequately allow for such cooperation, artificially hampering our government's ability to identify and prevent acts of terrorism against our citizens.

In this new war, terrorists are a hybrid between domestic criminals and international agents. We must lower the barriers that discourage our law enforcement and intelligence agencies from working together to stop these terrorists. These hybrid criminals call for new, hybrid tools.

Second, this bill updates the laws relating to electronic surveillance. Electronic surveillance, conducted under the supervision of a federal judge, is one of the most powerful tools at the disposal of our law enforcement community. It is simply a disgrace that we have not acted to modernize the laws currently on the books which govern such surveillance, laws that were enacted before the fax machine came into common usage, and well before the advent of cellular telephones, e-mail, and instant messaging. The Department of Justice has asked us for years to update these laws to reflect the new technologies, but there has always been a call to go slow, to seek more information, to order further studies.

This is no hypothetical problem. We now know that e-mail, cellular telephones, and the Internet have been principal tools used by the terrorists to coordinate their atrocious activities. We need to pursue all solid investigatory leads that exist right now that our law enforcement agents would be unable to pursue because they must continue to work within these outdated laws. It is high time that we update our laws so that our law enforcement agencies can deal with the world as it is, rather than the world as it existed 20 years ago.

A good example of way we our handicapping our law enforcement agencies relates to devices called "pen registers." Pen registers may be employed by the FBI, after obtaining a court order, to determine what telephone numbers are being dialed from a particular telephone. These devices are essential investigatory tools, which allow law enforcement agents to determine who is speaking to whom, within a criminal conspiracy.

The Supreme Court has held, in Smith v. Maryland, that the information obtained by pen register devices is not information that is subject to any constitutional protection. Unlike the content of your telephone conversation

once your call is connected, the numbers you dial into your telephone are not private. Because you have no reasonable expectation that such numbers will be kept private, they are not protected under the Constitution. The Smith holding was cited with approval by the Supreme Court just earlier this year.

The legislation under consideration today would make clear what the Federal courts have already ruled—that Federal judges may grant pen register authority to the FBI to cover, not just telephones, but other more modern modes of communication such as e-mail or instant messaging. Let me make clear that the bill does not allow law enforcement to receive the content of the communication, but they can receive the addressing information to identify the computer or computers a suspect is using to further his criminal activity.

Importantly, reform of the pen register law does not allow—as has sometimes been misreported in the press—for law enforcement agents to view the content of any e-mail messages—not even the subject line of e-mails. In addition, this legislation we are considering today makes it explicit that content can not be collected through such pen register orders.

This legislation also allows judges to enter pen register orders with nationwide scope. Nationwide jurisdiction for pen register orders makes common sense. It helps law enforcement agents efficiently identify communications facilities throughout the country, which greatly enhances the ability of law enforcement to identify quickly other members of a criminal organization, such as a terrorist cell.

Moreover, this legislation provides our intelligence community with the same authority to use pen register devices, under the auspices of the Foreign Intelligence Surveillance Act, that our law enforcement agents have when investigating criminal offenses. It simply makes sense to provide law enforcement with the same tools to catch terrorists that they already possess in connection with other criminal investigations, such as drug crimes or illegal gambling.

In addition to the pen register statute, this legislation updates other aspects of our wiretapping statutes. It is amazing that law enforcement agents do not currently have authority to seek wiretapping authority from a Federal judge when investigating a terrorist offense. This legislation fixes that problem.

Moving on, I note that much has been made of the complex immigration provisions of this bill. I know Senators SPECTER, KOHL and KENNEDY had questions about earlier provisions, particularly the detention provision for suspected alien terrorists.

I want to assure my colleagues that we have worked hard to address your concerns, and the concerns of the public. As with the other immigration provisions of this bill, we have made painstaking efforts to achieve this workable compromise.

Let me address some of the specific concerns. In response to the concern that the INS might detain a suspected terrorist indefinitely, the Senator KENNEDY, Senator KYL, and I worked out a compromise that limits the provision. It provides that the alien must be charged with an immigration or criminal violation within seven days after the commencement of detention or be released. In addition, contrary to what has been alleged, the certification itself is subject to judicial review. The Attorney General's power to detain a suspected terrorist under this bill is, then, not unfettered.

Moreover, Senator LEAHY and I have also worked diligently to craft necessary language that provides for the deportation of those aliens who are representatives of organizations that endorse terrorist activity, those who use a position of prominence to endorse terrorist activity or persuade others to support terrorist activity, or those who provide material support to terrorist organizations. If we are to fight terrorism, we can not allow those who support terrorists to remain in our country. Also, I should note that we have worked hard to provide the State Department and the INS the tools they need to ensure that no applicant for admission who is a terrorist is able to secure entry into the United States through legal channels.

Finally, the bill gives law enforcement agencies powerful tools to attack the financial infrastructure of terrorism giving our Government the ability to choke off the financing that these dangerous terrorist organizations need to survive. It criminalizes the practice of harboring terrorists, and puts teeth in the laws against providing material support to terrorists and terrorist organizations. It gives the President expanded authority to freeze the assets of terrorists and terrorist organizations, and provides for the eventual seizure of such assets. These tools are vital to our ability to effectively wage the war against terrorism, and ultimately to win it.

There have been few, if any, times in our nation's great history where an event has brought home to so many of our citizens, so quickly, and in such a graphic fashion, a sense of our vulnerability to unexpected attack.

I believe we all took some comfort when President Bush promised us that our law enforcement institutions would have the tools necessary to protect us from the danger that we are only just beginning to perceive.

The Attorney General has told us what tools he needs. We have taken the time to review the problems with our current laws, and to reflect on their solutions. The time to act is now. Let us please move forward expeditiously, and give those who are in the business of protecting us the tools that they need to do the job.

Mr. President, I think most people understand this is an important bill. All of us understand it needs to be done. All of us understand that these are tools our law enforcement people deserve and need to have. And, frankly, it is a bill that I think can make a real difference with regard to the interdiction of future acts of terrorism in our society.

Nobody can guarantee, when you have people willing to commit suicide in the perpetration of these awful acts, at all times that we can absolutely protect our Nation. But this bill will provide the tools whereby we might be able—and in most cases should be able—to resolve even those types of problems.

So with that, I am happy to yield the floor.

The PRESIDING OFFICER (Mr. DURBIN). Who yields time?

The Senator from Maryland.

Mr. SARBANES. Mr. President, I yield myself 10 minutes.

The PRESIDING OFFICER. The Senator from Maryland is recognized for 10 minutes.

Mr. SARBANES. Mr. President, I rise in very strong support of S. 1510, the Uniting and Strengthening America Act of 2001, and in particular, Title III of S. 1510, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001.

Title III was reported out of the Committee on Banking, Housing, and Urban Affairs, which I am privileged to chair, a week ago today by a unanimous vote of 21 to 0.

President Bush said on September 24: "We have launched a strike on the financial foundation of the global terror network."

Title III of our comprehensive anti-terrorism package supplies the armament for that strike. Osama bin Laden may have boasted that "al-Qaeda [includes] modern, educated youth who are aware of the cracks inside the western financial system, as they are aware of the lines in their hands." With Title III, we are sealing up those cracks.

Title III contains, among other things, authority to take targeted action against countries, institutions, transactions, or types of accounts the Secretary of the Treasury finds to be of "primary money-laundering concern." It also contains requirements for due diligence standards directed at corresponding accounts opened at U.S. banks by foreign offshore banks and banks in jurisdictions that have been found to fall significantly below international anti-money laundering standards.

It contains a bar on the maintenance of U.S. correspondent accounts for offshore shell banks—those banks that have no physical presence or employees anywhere, and that are not part of a regulated and recognized banking company. There is also a requirement that all financial institutions establish anti-money laundering programs.

Title III also contains several provisions that should enhance the ability

of the Government to share more specific information with banks, and the ability of banks to share information with one another relating to potential terrorist or money-laundering activities, and a large number of important technical improvements in anti-money laundering statutes, as well as, mandates to the Department of the Treasury to act or formulate recommendations to improve our anti-money laundering programs.

The problem of money laundering is not a new one. There have been significant efforts for some time in Congress to cut the financial lifelines on which criminal operations depend. Senator JOHN KERRY'S exhaustive investigation nearly a decade ago into the collapse of a shady institution called BCCI, which he found was established with "the specific purpose of evading regulation or control by governments," led him to introduce anti-money laundering legislation. A bill similar to his was approved last year by the Banking Committee of the House of Representatives on a 31 to 1 vote.

Recent investigations by Senator CARL LEVIN'S Permanent Subcommittee on Investigations produced two excellent reports on the ways criminals use financial institutions to launder funds and how we can counter these activities. Senator LEVIN'S reports demonstrated dramatically how correspondent banking facilities and private banking services impede financial transparency and hide foreign client identity and activity, thereby contributing to international money laundering.

Senator CHARLES GRASSLEY has also advocated for stronger money laundering legislation, and sponsored the Money Laundering and Financial Crimes Strategy Act of 1998, which mandates the development of an annual national money laundering strategy.

Two weeks ago we held our own hearings in the Banking Committee. We heard from a number of expert witnesses and from Under Secretary of the Treasury Gurule; Assistant Attorney General Chertoff; and Ambassador Stuart Eizenstat, the former Deputy Secretary of the Treasury.

On October 4, the Banking Committee marked-up and reported out our own bill. The committee print was built, in a sense, on the foundation given to us by Senators KERRY, LEVIN, GRASSLEY, and by others in this institution.

Before describing the provisions of Title III in greater detail, I want to thank all members of the Banking Committee for their contributions to this legislation. As I indicated, it came out of the committee on a vote of 21 to 0. The Ranking Member, Senator GRAMM, provided crucial support. He raised certain issues which were addressed in the course of the mark-up involving, among other things, important due process protections. Senators STABENOW and JOHNSON were instrumental in producing a compromise to resolve a dispute over one of the package's most important provisions. Senator ENZI contributed his experience as an accountant in refining another critical provision.

Senator SCHUMER, who has been involved in past efforts to address money laundering activities, played an important role, as did Senators ALLARD, BAYH, CORZINE, and CRAPO, who offered amendments and contributed important improvements to various parts of the subtitle.

I am deeply grateful to all of the members of the committee for their strong, positive, and constructive contributions and for their willingness to work day and night. It is my understanding that the committee staff went three consecutive nights without any sleep in order to prepare this legislation. This is carefully considered legislation because it reflects and builds upon efforts which have been made over a number of years.

Earlier today, our colleagues on the Financial Services Committee in the House of Representatives marked-up a bill, many of the provisions of which are identical or virtually identical to those contained in Title III of the package now before us.

Public support across the country for anti-money laundering legislation is extremely strong. Jim Hoagland put it plainly in the Washington Post:

> This crisis offers Washington an opportunity to force American and international banks to clean up concealment and laundering practices they now tolerate or encourage and which terrorism can exploit.

Terrorist attacks require major investments of time, planning, training, practice, and financial resources to pay the bills. Money laundering is the transmission belt that gives terrorists the resources to carry out their campaigns of carnage. We intend, with Title III of this legislation, to end that transmission belt and its ability to bring resources to the networks that enable terrorists to carry out their campaigns of violence.

Title III addresses all aspects of our defenses against money laundering. Those defenses generally fall into three parts. The first is the Bank Secrecy Act, "BSA", passed in 1970. It requires financial institutions to keep standardized transaction records and report large currency transactions and suspicious transactions and mandates reporting of the movement of more than $10,000 in currency into or out of the country. The statute is called the "bank secrecy act," because it bars bank secrecy in America, by preventing financial institutions from maintaining opaque records, or discarding their records altogether. Secrecy is the hiding place for crime, and Congress has barred our institutions from allowing those hiding places. The financial institutions covered by that act include banks, broker-dealers, casinos, and non-bank transmitters of funds, currency exchangers, and check cashers—all financial services businesses through which our citizens—and criminals hiding as legitimate citizens—can move funds into and through our economy. Unfortunately, reporting regulations covering some of these institutions have not yet been promulgated.

The second part of our money laundering defenses are the criminal statutes first enacted in 1986 that make it a crime to launder money and allow criminal and civil forfeiture of the proceeds of crime. The third part is the statutory framework that allows information to be communicated to and between law enforcement officials. Our goal must be to assure—to the greatest extent consistent with reasonable privacy protections—that the necessary information can be used by the right persons in "real time" to cut off terrorism and crime.

Title III modernizes provisions in all three areas to meet today's threats in a global economy. Its provisions are divided into five subtitles, dealing, respectively, with "international counter-money laundering measures"—sections 311-328—"Bank Secrecy Act improvements"—sections 331-342—bulk cash smuggling—section 351 and anti-corruption measures—sections 361-363.

There are 39 provisions in Title III. At this time, I want to summarize some of the bill's most important provisions.

Section 311 gives the Secretary of the Treasury, in consultation with other senior government officials, authority to impose one or more of five new "special measures" against foreign jurisdictions, entities, transactions or accounts that the Secretary, after consultation with other senior federal officials, determines to pose a "primary money laundering concern" to the United States. The special measures all involve special recordkeeping and reporting measures—to eliminate the curtains behind which launderers hide. In extreme cases the Secretary is permitted to bar certain kinds of interbank accounts from especially problematic jurisdictions. The statute specifies the considerations the Secretary must take into account in using the new authority and contains provisions to supplement the Administrative Procedure Act to assure that any remedies—except certain short-term measures—are subject to full comment from all affected persons.

This new provision gives the Secretary real authority to act to close overseas loopholes through which U.S. financial institutions are abused. At present the Secretary has no weapons except Treasury Advisories—which don't impose specific requirements—or full economic sanctions that suspend financial and trade relations with offending targets. President Bush's invocation of the International Economic Emergency Powers Act (IEEPA) several weeks ago was obviously appropriate. But there are many other situations in which we will not want to

block all transactions, but in which we will want to do more than simply advise financial institutions about under-regulated foreign financial institutions or holes in foreign counter-money laundering efforts. Former Deputy Secretary Eizenstat testified before the Committee that adding this tool to the Secretary's arsenal was essential.

Section 312 focuses on another aspect of the fight against money laundering, the financial institutions that are on the front lines making the initial decisions about what foreign banks to allow inside the United States. It requires U.S. financial institutions to exercise appropriate due diligence when dealing with private banking accounts and interbank correspondent relationships with foreign banks. With respect to foreign banks, the section requires U.S. financial institutions to apply appropriate due diligence to all correspondent accounts with foreign banks, and enhanced due diligence for accounts sought by offshore banks or banks in jurisdictions found to have substandard money laundering controls or which the Secretary determines to be of primary money laundering concern under the new authority given him by section 311.

The section also specifies certain minimum standards for the enhanced due diligence that U.S. financial institutions are required to apply to accounts opened for two categories of foreign banks with high money laundering risks—offshore banks and banks in jurisdictions with weak anti-money laundering and banking controls. These minimum standards were developed from, and are based upon, the factual record and analysis contained in the Levin staff report on correspondent banking and money laundering.

Section 312 is essential to Title III. It addresses, with appropriate flexibility, mechanisms whose very importance for the conduct of commercial banking makes them special targets of money launderers, as illustrated in Senator LEVIN's extensive reports and hearings. A related provision, in section 319, requires foreign banks that maintain correspondent accounts in the United States to appoint agents for service of process within the United States and authorizes the Attorney General and the Secretary of the Treasury to issue a summons or subpoena to any such foreign bank seeking records, wherever located, relating to such a correspondent account. U.S. banks must sever correspondent arrangements with foreign banks that do not either comply with or contest any such summons or subpoena, and if the Attorney General or the Secretary of the Treasury asks them to sever the arrangements.

These provisions send a simple message to foreign banks doing business through U.S. correspondent accounts: be prepared, if you want to use our banking facilities, to operate in accordance with U.S. law.

Section 313 also builds on the factual record before the Banking Committee to bar from the United States financial system pure "brass-plate" shell banks created outside the U.S. that have no physical presence anywhere and are not affiliated with recognized banking institutions. These shell banks carry the highest money laundering risks in the banking world because they are inherently unavailable for effective oversight—there is no office where a bank regulator or law enforcement official can go to observe bank operations, review documents or freeze funds.

Section 327 permits the Secretary to deal with abuse of another recognized commercial banking mechanism—concentration accounts that are used to commingle related funds in one place temporarily pending disbursement or the transfer of funds into individual client accounts. Concentration accounts have been used to launder funds, and the bill permits the Secretary to issue rules to bar the use of concentration accounts to move client funds anonymously, without documentation linking particular funds to their true owners.

Section 332 requires financial institutions to establish minimum anti-money laundering programs that include appropriate internal policies, management, employee training, and audit features. This is not a "one size fits all" requirement; in fact its very generality recognizes that different types of programs will be appropriate for different types and sizes of institutions.

A number of improvements are made to the suspicious activity reporting rules. First, technical changes strengthen the safe harbor from civil liability for institutions that report suspicious activity to the Treasury. The provisions not only add to the protection for reporting institutions; they also address individual privacy concerns by making it clear that government officers may not disclose suspicious transaction reports information except in the conduct of their official duties. The Act also requires the issuance of suspicious transaction reporting rules applicable to brokers and dealers in securities within 270 days of the date of enactment.

Sections 341 and 342 of the Title deal with underground banking systems such as the Hawala, which is suspected of being a channel used to finance the al Qaeda network. Section 341 makes it clear that underground money transmitters are subject to the same record-keeping rules—and the same penalties for violating those rules—as above-ground, recognized, money transmitters. It also directs the Secretary of the Treasury to report to Congress, within one year, on the need for additional legislation or regulatory controls relating to underground banking systems. Section 342 authorizes the Secretary of the Treasury to instruct the United States Executive Director of each of the international financial institutions to use such Director's "voice and vote" to support loans and other use of resources to benefit nations that the President determines to be contributing to efforts to combat international terrorism, and to require the auditing of each international financial institution to ensure that funds are not paid to persons engaged in or supporting terrorism.

Section 351 creates a new Bank Secrecy Act offense involving the bulk smuggling of more than $10,000 in currency in any conveyance, article of luggage or merchandise or container, either into or out of the United States, and related forfeiture provisions. This provision has been sought for several years by both the Departments of Justice and Treasury.

Other provisions of the bill address relevant provisions of the Criminal Code. These provisions were worked out with the Judiciary Committee and are included in Title III because of their close relationship to the provisions of Title 31 added or modified by Title III.

The most important is section 315, which expands the list of specified unlawful activities under 18 U.S.C. 1956 and 1957 to include foreign corruption offenses, certain U.S. export control violations, offenses subject to U.S. extradition obligations under multilateral treaties, and misuse of funds of international financial institutions.

Section 316 establishes procedures to protect the rights of persons whose property may be subject to confiscation in the exercise of the government's anti-terrorism authority.

Section 319 treats amounts deposited by foreign banks in interbank accounts with U.S. banks as having been deposited in the United States for purposes of the forfeiture rules, but grants the Attorney General authority, in the interest of fairness and consistent with the United States' national interest, to suspend a forfeiture proceeding based on that presumption. This closes an important forfeiture loophole.

Section 321 allows the United States to exclude any alien that the Attorney General knows or has reason to believe is or has engaged in or abetted certain money laundering offenses.

A third important set of provisions modernize information sharing rules to reflect the reality of the fight against money laundering and terrorism.

Section 314 requires the Secretary of the Treasury to issue regulations to encourage cooperation among financial institutions, financial regulators and law enforcement officials and to permit the sharing of information by law enforcement and regulatory authorities with such institutions regarding persons reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities. The section also allows banks to share information involving possible money laundering or terrorist activity among themselves—with notice to the Secretary of the Treasury.

Section 335 permits, but does not require, a bank to include information,

in a response to a request for an employment reference by a second bank, about the possible involvement of a former institution-affiliated party in potentially unlawful activity, and creates a safe harbor from civil liability for the bank that includes such information in response to an employment reference request, except in the case of malicious intent. Given its different focus, it is not my intention to similarly limit a bank's safe harbor from civil liability for the filing of suspicious activity reports under the Bank Secrecy Act.

Section 340 contains amendments to various provisions of the Bank Secrecy Act, the Right to Financial Privacy Act, and the Fair Credit Reporting Act, to permit information subject to those statutes to be used in the conduct of United States intelligence or counterintelligence activities to protect against international terrorism.

The modernization of our money laundering laws represented by Subtitle III is long overdue. It is not the work of one week or one weekend, but represents years of careful study and a bipartisan effort to produce a piece of prudent legislation. The care taken in producing the legislation extends to several provisions calling for reporting on the legislation's effect and a provision for a three-year review of the legislation's effectiveness.

Title III responds, as I've indicated, to the statement of Assistant Attorney General Chertoff, the head of the Department of Justice's Criminal Division, at the Banking Committee's September 26 hearing that "[w]e are fighting with outdated weapons in the money laundering arena today." Without this legislation, the cracks in the system of which bin Laden boasted will remain open. We should not, indeed we can not, allow that to happen, any more than we can delay dealing with the financial aspects of the terrorist threat.

Title III is a balanced effort to address a complex area of national concern. I strongly urge my colleagues to follow the unanimous recommendation of the Banking Committee and support this important component of the anti-terrorism package.

I ask unanimous consent that a section-by-section summary of Title III be included in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

TITLE III—INTERNATIONAL MONEY LAUNDERING ABATEMENT AND ANTI-TERRORIST FINANCING ACT OF 2001—SECTION-BY-SECTION SUMMARY

Sec. 301. Short title and table of contents.

Sec. 302. Findings and purposes.

Sec. 303. Provides that the provisions added and amendments made by Title III will terminate after September 30, 2004, if the Congress enacts a joint resolution to that effect, and that such joint resolution will be given expedited consideration in each Houses of Congress.

SUBTITLE A. INTERNATIONAL COUNTER-MONEY LAUNDERING AND RELATED MEASURES

Sec. 311. Gives the Secretary of the Treasury, in consultation with other senior government officials, authority (in the Secretary's discretion) to impose one or more of five new "special measures" against foreign jurisdictions, entities, transactions and accounts that the Secretary, after consultation with other senior federal officials, determines to pose a "primary money laundering concern" to the United States. The special measures include: (1) requiring additional recordkeeping or reporting for particular transactions, (2) requiring the identification of the foreign beneficial owners of certain accounts at a U.S. financial institution, (3) requiring the identification of customers of a foreign bank who use an interbank payable-through account opened by that foreign bank at a U.S. bank, (4) requiring the identification of customers of a foreign bank who use an interbank correspondent account opened by that foreign bank at a U.S. bank, and (5) after consultation with the Secretary of State, the Attorney General, and the Chairman of the Federal Reserve Board, restricting or prohibiting the opening or maintaining of certain interbank correspondent or payable-through accounts. Measures 1–4 may not be imposed, other than by regulation, for a period in excess of 120 days; measure 5 may only be imposed by regulation. Also requires the Secretary of the Treasury, in consultation with the appropriate Federal banking agencies, to submit to Congress, within 180 days of the date of enactment, recommendations for the most effective way to require foreign nationals opening a U.S. bank account to provide identification comparable to that required when U.S. citizens open a bank account.

Sec. 312. Requires a U.S. financial institution that maintains a correspondent account or private banking account for a non-United States person to establish appropriate and, if necessary, enhanced due diligence procedures to detect and report instances of money laundering. Creates a minimum anti-money laundering due diligence standards for U.S. financial institutions that enter into correspondent banking relationships with banks that operate under offshore banking licenses or under banking licenses issued by countries that (a) have been found non-cooperative with international counter money laundering principles, or (b) have been the subject of special measures authorized by Sec. 311. Creates minimum anti-money laundering due diligence standards for maintenance of private banking accounts by U.S. financial institutions.

Sec. 313. Bars depository institutions and broker-dealers operating in the United States from establishing, maintaining, administering, or managing correspondent accounts for foreign shell banks, other than shell bank vehicles affiliated with recognized and regulated depository institutions.

Sec. 314. Requires the Secretary of the Treasury to issue regulations to encourage cooperation among financial institutions, financial regulators and law enforcement officials and to permit the sharing of information by law enforcement and regulatory authorities with such institutions regarding persons reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities. Allows (with notice to the Secretary of the Treasury) the sharing of information among banks involving possible terrorist or money laundering activity.

Sec. 315. Expands the list of specified unlawful activities under 18 U.S.C. 1956 and 1957 to include foreign corruption offenses, certain U.S. export control violations, and misuse of funds of the IMF.

Sec. 316. Establishes procedures to protect the rights of persons whose property may be subject to confiscation in the exercise of the government's anti-terrorism authority.

Sec. 317. Gives United States courts "long-arm" jurisdiction over foreign persons committing money laundering offenses in the United States, over foreign banks opening United States bank accounts, and over foreign persons seizing assets ordered forfeited by a U.S. court.

Sec. 318. Expands the definition of financial institution for purposes of 18 U.S.C. 1956 and 1957 to include banks operating outside the United States.

Sec. 319. Treats amounts deposited by foreign banks in interbank accounts with U.S. banks as having been deposited in the United States for purposes of the forfeiture rules, but grants the Attorney General authority, in the interest of justice and consistent with the United States' national interest, to suspend a forfeiture proceeding based on that presumption. Requires U.S. financial institutions to reply to a request for information from a U.S. regulator relating to anti-money laundering compliance within 120 hours of receipt of such a request. Requires foreign banks that maintain correspondent accounts in the United States to appoint agents for service of process within the United States and authorizes the Attorney General and the Secretary of the Treasury to issue a summons or subpoena to any such foreign bank seeking records, wherever located, relating to such a correspondent account. Requires U.S. banks to sever correspondent arrangements with foreign banks that do not either comply with or contest any such summons or subpoena. Authorizes United States courts to order a convicted criminal to return property located abroad and to order a civil forfeiture defendant to return property located abroad pending trial on the merits. Authorizes United States prosecutors to use a court-appointed Federal receiver to find a criminal defendant's assets, wherever located.

Sec. 320. Permits the United States to institute forfeiture proceedings against the proceeds of foreign criminal offenses found in the United States.

Sec. 321. Allows the United States to exclude any alien that the Attorney General knows or has reason to believe is or has engaged in or abetted certain money laundering offenses.

Sec. 322. Extends the prohibition against the maintenance of a forfeiture proceedings on behalf of a fugitive to include a proceeding by a corporation whose majority shareholder is a fugitive and a proceeding in which the corporation's claim is instituted by a fugitive.

Sec. 323. Permits the government to seek a restraining order to preserve the availability of property subject to a foreign forfeiture or confiscation judgment.

Sec. 324. Increases from $100,000 to $1,000,000 the maximum civil and criminal penalties for a violation of provisions added to the Bank Secrecy Act by sections 311 and 312 of the Act.

Sec. 325. Directs the Secretary of the Treasury, in consultation with the Attorney General, the Federal banking agencies, the SEC, the CFTC and other appropriate agencies to evaluate operation of the provisions of Subtitle A of Title III of the Act and recommend to Congress any relevant legislative action, within 30 months of the date of enactment.

Sec. 326. Directs the Secretary of the Treasury to report annually to the Senate Banking Committee and House Financial Services Committee on measures taken pursuant to Subtitle A of Title III of the Act.

Sec. 327. Authorizes the Secretary of the Treasury to issue regulations concerning the

maintenance of concentration accounts by U.S. depository institutions to prevent an institution's customers from anonymously directing funds into or through such accounts.

Sec. 328. Provides criminal penalties for officials who violate their trust in connection with the administration of Title III.

SUBTITLE B. CURRENCY TRANSACTION REPORTING AMENDMENTS AND RELATED IMPROVEMENTS

Sec. 331. Clarifies the terms of the safe harbor from civil liability for financial institutions filing suspicious activity reports pursuant to 31 U.S.C. 5318(g).

Sec. 332. Requires financial institutions to establish anti-money laundering programs and grants the Secretary of the Treasury authority to set minimum standards for such programs.

Sec. 333. Clarifies that penalties for violation of the Bank Secrecy Act and its implementing regulations also apply to violation of Geographic Targeting Orders issued under 31 U.S.C. 3526, and to certain recordkeeping requirements relating to funds transfers. Otherwise clarifies and updates certain provisions of 31 U.S.C. 5326 relating to Geographic Targeting Orders.

Sec. 334. Adds "money laundering related to terrorist funding" to the list of subjects to be dealt with in the annual National Money Laundering Strategy prepared by the Secretary of the Treasury pursuant to the "Money Laundering and Financial Crimes Strategy Act of 1998."

Sec. 335. Permits (but does not require) a bank to include information, in a response to a request for an employment reference by a second bank, about the possible involvement of a former institution-affiliated party in potentially unlawful activity, and creates a safe harbor from civil liability for the bank that includes such information in response to an employment reference request, except in the case of malicious intent.

Sec. 336. requires the Bank Secrecy Act Advisory Group to include a privacy advocate among its membership and to operate under certain of the "sunshine" provisions of the Federal Advisory Committee Act.

Sec. 337. Directs the Secretary of the Treasury and the Federal bank regulatory agencies to submit reports to Congress, one year after the date of enactment, containing recommendations on possible legislation to conform the penalties imposed on depository institutions for violations of the Bank Secrecy Act with penalties imposed on such institutions under section 8 of the Federal Deposit Insurance Act.

Sec. 338. Directs the Secretary of the Treasury, after consultation with the Securities and Exchange Commission and the Federal Reserve Board, to promulgate regulations, within 270 days of the date of enactment, requiring broker-dealers to file suspicious activity reports. Also requires the Secretary of the Treasury, the SEC, Federal Reserve Board, and the CFTC to submit jointly to Congress, within one year of the date of enactment, recommendations for effective application of the provisions of 31 U.S.C. 5311-30 to both registered and unregistered investment companies.

Sec. 339. Directs the Secretary of the Treasury to submit a report to Congress, six months after the date of enactment, on the role of the Internal Revenue Service in the administration of the Bank Secrecy Act, with emphasis on whether IRS Bank Secrecy Act information processing responsibility (for reports filed by all financial institutions) or Bank Secrecy Act audit and examination responsibility (for certain non-bank financial institutions) should be retained or transferred.

Sec. 340. Contains amendments to various provisions of the Bank Secrecy Act, the Right to Financial Privacy Act, and the Fair Credit Reporting Act, to permit information to be used in the conduct of United States intelligence or counterintelligence activities to protect against international terrorism.

Sec. 341. Clarifies that the Bank Secrecy Act treats certain underground banking systems as financial institutions, and that the funds transfer recordkeeping rules applicable to licensed money transmitters also apply to such underground systems. Directs the Secretary of the Treasury to report to Congress, within one year of the date of enactment, on the need for additional legislation or regulatory controls relating to underground banking systems.

Sec. 342. Authorizes the Secretary of the Treasury to instruct the United States Executive Director of each of the international financial institutions (for example, the IMF and the World Bank) to use such Director's "voice and vote" to support loans and other use of resources to benefit nations that the President determines to be contributing to United States efforts to combat international terrorism, and to require the auditing of each international financial institution to ensure that funds are not paid to persons engaged in or supporting terrorism.

SUBTITLE C. CURRENCY CRIMES

Sec. 351. Creates a new Bank Secrecy Act offense involving the bulk smuggling of more than $10,000 in currency in any conveyance, article of luggage or merchandise or container, either into or out of the United States, and related forfeiture provisions.

SUBTITLE D. ANTI-CORRUPTION MEASURES

Sec. 361. Expresses the sense of Congress that the United States should take all steps necessary to identify the proceeds of foreign government corruption that have been deposited in United States financial institutions and return such proceeds to the citizens of the country to whom such assets belong.

Sec. 362. Expresses the sense of Congress that the United States must continue actively and publicly to support the objectives of the 29-country Financial Action Task Force Against Money Laundering.

Sec. 363. Expresses the sense of Congress that the United States, in its deliberations and negotiations with other countries, should promote international efforts to identify and prevent the transmittal of funds to and from terrorist organizations.

SUBTITLE E. MISCELLANEOUS

Sec. 371. Expands the SEC's emergency order authority.

Sec. 372. Creates uniform protection standards for Federal Reserve facilities.

Mr. LEAHY. Mr. President, I thank the distinguished chairman of the Banking Committee, the senior Senator from Maryland, Mr. SARBANES. He did unbelievable work in this committee to pass out a money-laundering bill—a very complex and difficult subject. He did it unanimously, I believe, in a committee that probably has as diverse a membership—that is an understatement—as one might find. I compliment him and thank him for his kind words.

I reserve the remainder of my time. I see the chairman of the Senate Intelligence Committee here, who wishes to give his opening statement.

The PRESIDING OFFICER. The Senator from Nevada is recognized.

Mr. REID. Mr. President, I conferred with Senator DASCHLE a few minutes ago. It is his desire—so there is no misunderstanding of the Members—that a number of opening statements be given: The Senator from Florida, the chairman of the Intelligence Committee, and we understand Senator STABENOW wishes to speak, and there may be a couple of other opening statements.

As soon as that is done, we are going to turn to Senator FEINGOLD to offer the first of his amendments. After that, there will be a vote on the first Feingold amendment.

Mr. LEAHY. Mr. President, I yield 10 minutes to the senior Senator from Florida.

The PRESIDING OFFICER. The Senator from Florida is recognized for 10 minutes.

Mr. GRAHAM. Mr. President, I wish to commend Senators DASCHLE and LOTT for their leadership in bringing this critical piece of legislation to the Senate just 1 month after the horrific events of September 11. Senators LEAHY and HATCH also deserve credit for moving quickly to shape the judiciary components of this bill and choreograph other provisions, including those affecting the intelligence agencies.

My remarks will focus on title IX of this legislation, which is entitled "Improved Intelligence," as well as the other provisions in the bill that directly affect the mission of the agencies of the intelligence community.

Title IX is derived from S. 1448, legislation which was developed within the intelligence community, entitled "Intelligence to Prevent Terrorism Act of 2001."

Since long before September 11, I have been working with members of the committee, particularly Senators FEINSTEIN and KYL, on comprehensive counterterrorism legislation. Most of the provisions of our bill, with some changes requested by the administration, have now become title IX of S. 1510.

The provisions in title IX, as well as other provisions in the bill, are designed to accomplish a daunting but not impossible task. That task is to change the cultures within the Federal law enforcement and intelligence agencies—primarily the FBI and the CIA—so they work seamlessly together for the good of the American people.

Both the FBI and the CIA are very good. They are the standards of the world in their own missions. But those missions are very different. The Federal Bureau of Investigation is goal oriented. A criminal case has a beginning, a middle, and an end. In a case that has developed the guilty party, the end is a conviction for the crime committed. The information collected during a criminal case is very closely held. It is held closely because its purpose is to result in the successful prosecution of an event that occurred in the past—not to inform thinking about what may happen now or in the future.

The Central Intelligence Agency, on the other hand, as well as its other companions in the intelligence community, has a global approach, literally

and figuratively. The CIA is restricted to activities outside the United States of America. The CIA collects information on a worldwide basis, and it processes that information, analyzes that information, and it places it in the hands of its customers. Its customers are other Federal agencies and senior policymakers, including the President of the United States. The purpose of that information is to allow those senior policymakers to make more informed decisions.

Given the threats we now face, the cultures growing out of these different missions must be melded. We cannot fight terrorism by putting yellow tape around a bomb site, calling it a crime scene, collecting evidence, and proceeding to trial frequently years later. We must put the evidence collected after such an event to work for us in real time so we can predict and prevent the next attack. If there is a single goal of the intelligence components of this antiterrorism bill, it is to change the focus from responding to acts that have already occurred to preventing the acts which threaten the lives of American citizens in this country and abroad.

It is critical that all information lawfully available to the Federal Government be used efficiently and effectively to fight terrorism. We cannot continue to use critical information only in a criminal trial. Any information collected must be available to intelligence officials to inform their operational initiatives so as to prevent the next attack.

Along these lines, several provisions of S. 1510 are designed to change the way information is handled within the Federal Government. For example, section 203 permits law enforcement to share information collected in grand jury proceedings and from title III criminal wiretaps with intelligence agencies. Current law, as it has been interpreted, prevents that sharing, except in very limited circumstances.

Section 905 then complements section 203 in that it requires law enforcement officers, FBI agents, and the Justice Department prosecutors to provide foreign intelligence derived in the course of a criminal investigation, including grand juries, criminal wiretaps, FBI interviews, and the like, to the Central Intelligence Agency and to other intelligence agencies.

A "permissive" approach is not good enough under current circumstances. Too many lives have been lost, too many lives are at risk. Law enforcement sharing of information with the intelligence agencies must be mandatory.

Section 908 further complements this legislation by providing the training of law enforcement officers at the Federal, State, and local agencies so they will be better equipped to recognize foreign intelligence information when they see it, and to get it to the right place on a timely basis.

Let me give a couple of hypothetical but eerily-close-to-reality examples. It is likely that there are, tonight, grand juries meeting at various places in the United States to deal with issues related to the events of September 11. Witnesses may be providing information—information about training camps in Afghanistan, ground warfare techniques used by al-Qaida and the Taliban, the types and quantity of weapons available. This type of information will be critical for the military—critical for the military now, not 2 years from now when these cases might go to trial.

Another example is in the area of wiretaps. Let me just take two wiretaps. One has been issued under the Foreign Intelligence Surveillance Act because there was a finding by a Federal judge that there was credible evidence that the telephone was being used by an agent of a foreign power.

In the course of listening to the wiretap, this conversation comes across: I am planning to fly from a specifically designated site in Central America to a city in Texas. I am going to take my flight a week from Monday. My intention is, once I arrive over that city, to distribute chemical or biological materials that will terrorize the people of that city by creating havoc due to the illnesses that will be provoked.

But how are you going to pay for this? You don't have the money to buy a plane, chemicals, or get the expertise necessary to do that?

I am going to do that because I am going to rob a bank next Monday in order to get the money that I need to pay for this operation. The bank is going to be located at the corner of First and Main, and I am going to do it 3 hours after the bank closes next Monday.

The person listening to that conversation with a foreign intelligence wiretap is under a legal obligation to make known to the appropriate law enforcement officials that there is about to be a bank robbery at a specific location on a specific date and time in a certain Texas city.

Conversely, if that exact conversation had taken place under a criminal wiretap under title 3, the person listening to that conversation would be prohibited from telling the foreign intelligence agencies that there was about to be a terrorist attack on a date certain against a specific Texas city originating at a specific site in Central America.

Try to convince the American people that makes sense. It clearly does not in today's reality. This legislation is going to make the same requirement of mandatory sharing when the information is gathered under a criminal wiretap that involves foreign intelligence information, as is the case today when information gathered under a Foreign Intelligence Surveillance Act wiretap must be made available to appropriate law enforcement officials.

Another provision of title 9 addresses the role of the Director of Central Intelligence in the process of collecting foreign intelligence under the Foreign Intelligence Surveillance Act. It recognizes the need to target limited resources, including personnel and translators against the highest priority targets.

I ask if I can have an additional 5 minutes.

The PRESIDING OFFICER. The Senator from Vermont.

Mr. LEAHY. I have about 11 minutes left that has not been committed which I thought I might use to answer some questions. I give the Senator 2 of my 11 minutes.

Mr. GRAHAM. I appreciate the Senator's limitations.

Mr. LEAHY. We just had one Senator ask me for 30 minutes. I am looking at my 11. How can I give him 30? But I will give you 2 of the 11.

Mr. GRAHAM. Mr. President, I thank the Senator from Vermont.

We have a provision that the Director of Central Intelligence, the DCI, will set the overall strategic goals for the collection of foreign intelligence so that we can use our limited resources as effectively as possible.

In order to complement that, we also have a provision that will establish a national virtual translation center as a means of increasing our woefully limited linguistic capabilities to translate the material which we are gathering.

We will also provide for additional capability with human intelligence. We have become very reliant on technology—eavesdropping, satellite imagery, to the exclusion of the use of human beings. If we want to gain information about the bin Ladens of the world, we cannot just take a picture of bin Laden.

Today it is increasingly difficult to eavesdrop on bin Laden. What we need to do is get a human being who is able to get close enough to bin Laden to learn his intentions and capabilities. This gets to the difficult issue of what kind of assets, human beings, we hire to work for us to gather such information?

We would all like to employ the purist of people, all choir boys to do this type of work. Unfortunately, they are not the type of people who are likely to be able to get close to the bin Ladens of the world. Thus, we have a provision in this legislation in the nature of a sense of Congress which we hope will send a strong message to the intelligence community that we are encouraging them to overcome some previous messages from Congress and to proceed to recruit the persons who they find to be necessary to gain access to terrorists so that we can have the best opportunity of protecting ourselves.

With the adoption of this legislation, we have not reached the end of our task or responsibilities to protect the American people. We are taking a substantial step in that direction.

To reiterate, another provision of title 9 addresses the role of the Director of Central Intelligence in the process of collecting foreign intelligence

under the Foreign Intelligence Surveillance Act. It recognizes the need to target limited resources—e.g. translators—against the highest priority targets.

In order to ensure that scarce resources are effectively used, the DCI—in his role as head of the Intelligence community, not as CIA Director—will set overall strategic goals for FISA collection.

He will work with the Attorney General to ensure that FISA information is distributed to the intelligence operators and analysts who need it government-wide.

Of course, the operational targeting and collection using wiretaps will be conducted by the FBI, as it has in the past; the DCI will perform no role in those decisions.

One of the scarce resources that has plagued the Intelligence Community, as well as law enforcement, is translation capability.

Section 907 of this bill requires the FBI and CIA to work together to create a "National Virtual Translation Center."

Such a center would seek to remedy the chronic problem of developing critical language abilities, and matching those resources to intelligence collected by the wide range of techniques available.

It is not enough to be able to listen to the conversations of terrorists and their supporters.

Those conversations must be translated, often from difficult languages such as Urdu, and analyzed, all in a timely fashion.

Our intelligence services collect vast amounts of data every day. It is possible that we may find that a critical clue to the September 11 attacks may have been available, but untranslated, days, weeks, or even months before the hijackings.

We must address this problem before another specific threat is overlooked.

Finally, I would like to mention a problem that has received a great deal of attention in recent weeks. There has been criticism of the intelligence agencies for placing too great a reliance on technical intelligence collection—laws dropping, satelite photograph—in recent years at the expense of human sources, or spies.

A corollary of this criticism is that CIA officers are to risk-averse and that they do not aggressively recruit sources overseas that may have access to terrorist groups because the sources may have engaged in human rights violations or violent crimes.

As to the first problem, the Intelligence authorization bill for fiscal year 2002, which may come to the floor next week, provides greater resources for human source recruitment—and it is part of a 5-year plan to beef up this method of collection.

With respect to the second problem, we in the Congress simply must accept some of the responsibility for creating a risk-averse reaction at CIA, if needed there is one.

The internal CIA regulations addressing the so-called "dirty asset" problem grew out of the criticisms by Congress in the mid-1990s about the recruitment of sources in Guatemala with sordid pasts.

We address this issue in S. 1510, section 903, by sending a strong message to CIA Headquarters and CIA officers overseas that recruitment of any person who has access to terrorists or terrorist groups should be of the highest priority.

There is no place in times like these for timidity in seeking every method available to learn the capabilities, plans, and intentions of terrorists.

Congress needs to send a strong message that we value such efforts to recruit sources on terrorism, even those with pasts we would not applaud.

Section 903 sends that message.

I urge passage of S. 1510.

I again commend the Members of the Senate who have played such an effective role.

I also thank the staff: Al Cumming, Bob Filippone, Vicki Divoll, Steven Cash, Bill Duhnke, Paula DeSutter, Jim Hensler, and Jim Barnett.

They have been working for the past many months to bring us to the point of this legislation being available for adoption by the Senate tonight and for the safety of the American people.

The PRESIDING OFFICER. The time of the Senator has expired. The Senator from Vermont.

Mr. LEAHY. I ask the distinguished Senator from Utah—I see the distinguished senior Senator from Pennsylvania is here—perhaps after the senior Senator from Utah, and then after the senior Senator from Pennsylvania speaks, whether it might be possible to go to the Senator from Wisconsin for the purpose of bringing up his amendments, and we can then debate and vote on them. Will that be agreeable to everybody?

Mr. HATCH. It is agreeable.

Mr. LEAHY. I ask unanimous consent that after the Senator from Utah, and the Senator from Pennsylvania, we go to the Senator from Wisconsin for the purpose of bringing up his amendments.

The PRESIDING OFFICER. Without objection, it is so ordered.

The Senator from Utah.

Mr. HATCH. Mr. President, in my opening remarks, I was remiss in not mentioning the tremendous work of the distinguished chairman and vice chairman of the Intelligence Committee. They have done a tremendous amount of work on the intelligence aspect of this bill. As a member of the Intelligence Committee, I express my high regard for the both of them and the work they have done.

I also express my regard for my friend from Maryland, Senator SARBANES, who came to the Senate with me, for the work he has done on the money-laundering section of this bill. He and Senator GRAMM and the Banking Committee have done yeoman's service on this, and I hope we are able to have that as part of the final bill.

I would be remiss if I did not acknowledge the great work that has been done—also, Senator KYL and so many others. I felt I needed to say that. I thank the Chair.

The PRESIDING OFFICER. Who yields time?

Mr. SPECTER. Mr. President, parliamentary inquiry, that I have 30 minutes under the unanimous consent request?

The PRESIDING OFFICER. The Senator is correct.

Mr. SPECTER. I yield myself 15 minutes.

The PRESIDING OFFICER. The Senator from Pennsylvania.

Mr. SPECTER. Mr. President, I have sought recognition and asked for this reservation of time to express my concerns about the record which the Senate is creating so that whatever legislation we pass will pass constitutional muster.

The Supreme Court of the United States has handed down a series of decisions in the past decade which question the constitutionality and, in fact, invalidate acts of Congress because there has been an insufficient record compiled. So I make these statements and review the record so far with a view to urging my colleagues to create a record in this Chamber, in conference, or wherever that opportunity may present itself.

In 1989, in the case of Sable v. FCC, the Supreme Court of the United States struck down an act of Congress saying, "no Congressman or Senator purported to present a considered judgment." I thought it was a remarkable statement by the Supreme Court since Congressman Tom Bliley in the House of Representatives had established a very comprehensive record.

The Supreme Court in 1997, in a case captioned Reno v. ACLU, again invalidated an act of Congress noting, "the lack of legislative attention to the statute at issue in Sable suggests another parallel with this case."

It was surprising to me that the Supreme Court of the United States would invalidate an act of Congress on the ground that no Senator or Congressman had purported to present a considered judgment, when that is the view of the Supreme Court which is contrary to Congress.

Under our doctrine of separation of powers, it seemed to me an act of Congress should stand unless there is some specific provision in the Constitution which warrants invalidating it or for vagueness under the due process clause of the fifth amendment.

The Supreme Court of the United States, in January of last year, did it again in a case captioned Kimel v. Florida Board of Regents, a case which involved the Age Discrimination in Employment Act. There the Court said, "our examination of the act's legislative record confirms that Congress' 1974 extension of the Act to the States

was an unwarranted response to a perhaps inconsequential problem." Again, a remarkable holding that the Congress had an unwarranted response and that it was an inconsequential problem, totally contradicting the judgment of the Congress of the United States.

Then the Court went on in the Kimel case to say, "Congress had no reason to believe that broad prophylactic legislation was necessary in this field."

Those are only a few of the cases where the Supreme Court of the United States has invalidated acts of Congress. There is no doubt there is a need for legislation to expand the powers of law enforcement to enable us to act against terrorists. My own experience in 8 years on the Intelligence Committee, 2 years of which was as chairman, and my work as chairman of the Judiciary Subcommittee on Terrorism have convinced me without a doubt of the scourge of terrorism which we have seen many times but never with the intensity which we observed on September 11 of this year.

The act of Congress in expanding law enforcement has to be very carefully calibrated to protect civil liberties and be in accordance with the Constitution of the United States. Attorney General Ashcroft met with a number of us on Wednesday, September 19, just 8 days after the incident of September 11, and asked that we enact legislation by the end of the week. My response at that time was I thought it could not be done in that time frame, but I thought we could hold hearings in the remainder of that week, perhaps on Thursday the 20th, or Friday the 21st, or Saturday the 22nd, to move ahead, understanding the import of the administration's bill, and legislate to give them what they needed, consistent with civil rights.

The Judiciary Committee then held a hearing on September 25 where the Attorney General testified for about an hour and 20 minutes. At that time, as that record will show, only a few Senators were able to ask questions. In fact, the questioning ended after my turn came, and most of the Judiciary Committee did not have a chance to raise questions.

On September 26, the following day, I wrote to the chairman of the committee saying:

I write to urge that our Judiciary Committee proceed promptly with the Attorney General's terrorism package with a view to mark up the bill early next week so the full Senate can consider it and hopefully act upon it by the end of the week. I am concerned that some further act of terrorism may occur which could be attributed to our failure to act promptly.

I then found out on October 3 that the Subcommittee on the Constitution was having a hearing. By chance, I heard about it in the corridors. Although we were having a hearing with Health and Human Services Secretary Thompson on bioterrorism, I absented myself from the bioterrorism hearing and went down the hall to the Judiciary subcommittee hearing and participated there and expressed many of the reservations and concerns I am commenting about today.

On that date, I again wrote to Senator LEAHY. I ask unanimous consent that the full text of my letter to him and the full text of his reply to me of October 9 be printed in the RECORD at the conclusion of these remarks.

The PRESIDING OFFICER. Without objection, it is so ordered.

(See exhibit 1.)

Mr. SPECTER. I quote only from the first sentence of Senator LEAHY's response to me:

I thank you for your letters of September 26 and October 3 and for your participation in the September 25 hearing regarding antiterrorism legislation. On October 3, you wrote that you were concerned about the lack of hearings. I share that concern and have tried to notice prompt hearings on a number of aspects of the legislative proposals at the earliest possible time.

On this state of the record, which I hope can yet be perfected, I am concerned about our meeting the standards of the Supreme Court of the United States for a sufficient deliberative process.

When Attorney General Ashcroft appeared before the Judiciary Committee on September 25, he said the only detention he wanted on aliens was those who were subject to deportation proceedings. I then pointed out, as the record will show, that the legislation submitted by the Attorney General was much broader and did not limit detention simply or exclusively to those who were subject to deportation proceedings. So my comment was that it was necessary to analyze the bill very carefully, not do it hurriedly, and give the Attorney General of the Department of Justice what he needed, consistent with constitutional rights.

The other issue which I had an opportunity to raise in the very brief period of time I had—some 5 minutes—involved modifications to the Foreign Intelligence Surveillance Act, where the issue was to change the law from "the purpose," being the gathering of intelligence, to "a purpose." Ultimately the legislation has been modified to read "a significant purpose."

At that hearing, the Attorney General said he did not look to obtain content from electronic surveillance unless probable cause was established. But in the draft bill, which the Department of Justice had submitted at that time, that was not what the bill provided. So that on this state of the record, I think the Congress has some work to do, tonight in conference or perhaps by other means, to see to it we have a record which will withstand constitutional scrutiny.

On our Judiciary Committee, we have many Members who have expertise in this field. This bill, as the RECORD will show, was negotiated by the chairman and ranking member with the Department of Justice, with the participation of the committee only to the extent of the hearing of the full committee on September 25 and the subcommittee on October 3.

We have on our Judiciary Committee a number of Members who have had experience as prosecuting attorneys. We have a number of lawyers who are learned in law. We have other Members who have extensive experience on the Judiciary Committee and a great deal of common sense which may top some of us who have prosecutorial experience or extended experience with probable cause and search warrants or surveillance of some sort or another.

I express these concerns so whatever can be done by the Congress will be done to meet the constitutional standards.

How much of the 15 minutes have I used?

The PRESIDING OFFICER. The Senator has 3 minutes 37 seconds remaining.

Mr. SPECTER. I reserve the remainder of my time, and I yield the floor.

EXHIBIT 1

U.S. SENATE,
Washington, DC, September 26, 2001.

Hon. PATRICK J. LEAHY,
Chairman, Senate Judiciary Committee, Washington, DC.

DEAR PAT: I write to urge that our Judiciary Committee proceed promptly with the Attorney General's terrorism package with the view to mark up the bill early next week so the full Senate can consider it and hopefully act upon it by the end of next week.

I am concerned that some further act of terrorism may occur which could be attributed to our failure to act promptly.

Sincerely,

ARLEN SPECTER.

U.S. SENATE,
Washington, DC, October 3, 2001.

Hon. PATRICK J. LEAHY,
Chairman, Senate Judiciary Committee, Washington, DC.

DEAR SENATOR LEAHY: I am very much concerned about the delay in acting on the anti-terrorism legislation and also about the absence of hearings to establish a record for the legislative package.

In recent decisions, the Supreme Court of the United States has declared acts of Congress unconstitutional when there has been an insufficient record or deliberative process to justify the legislation.

On the anti-terrorism legislation, perhaps more than any other, the Court engages in balancing the needs of law enforcement with the civil rights issues so that it is necessary to have the specification of the problems to warrant broadening police power.

In my judgment, there is no substitute for the hearings, perhaps in closed session, to deal with these issues.

As you know, I have been pressing for hearings. I am now informed that Senator Hatch has convened a meeting of all Republican senators to, in effect, tell us what is in a proposed bill where Judiciary Committee members have had no input.

We could still have meaningful hearings this week and get this bill ready for prompt floor action.

Sincerely,

ARLEN SPECTER.

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC, October 9, 2001.

Hon. ARLEN SPECTER,
711 Hart Senate Office Building, Washington, DC.

DEAR ARLEN, I thank you for your letters of September 26, 2001 and October 3, 2001 and for your participation in the September 25, 2001 hearing regarding anti-terrorism legislation. On October 3, 2001, you wrote that you were concerned about the lack of hearings. I share that concern and have tried to notice prompt hearings on a number of aspects of the legislation proposals at the earliest possible time.

As you know, the Attorney General consented to appear at our September 25, 2001 hearing for only an hour and we had to prevail upon him to stay a few extra minutes so that Senator Feinstein and you could have a brief opportunity to ask the Attorney General a single question. I invited him to rejoin us the following Tuesday to complete the hearing and I continue to extend such invitations, but he has not accepted any of my follow up invitations. In addition, although Members of the Committee submitted questions in writing to the Attorney General following the September 25, 2001 hearing, they have yet to be answered. I agree with you that these are important matters that justify a more thorough record than we have been able to establish.

Last week, Senator Feingold chaired an important hearing on civil liberties concerns before the Constitution Subcommittee. This week Senators Schumer, Feinstein and Durbin each are working to organize hearings on these matters and Senators Kennedy and Biden are working on possible hearings next week.

At the same time, we have continued to work nonstop to prepare for Senate action on legislative proposals. We suffered a setback last week when after weeks of intensive negotiations the White House reneged on agreements reached on Sunday, September 30, 2001, and we had to spend much of last week renegotiating a legislative package. Finally, last Thursday S. 1510 was introduced by the Majority Leader, the Republican Leader, the Chairmen of the Judiciary, Banking and Select Intelligence Committees and by Senators Hatch and Shelby as Ranking Members. I am seeking to work closely with the Senate leadership to be prepared to proceed to that legislation at the earliest opportunity. The House is on a similar track and may well consider its version of legislation later this week, as well.

You and I both know that no legislation can guarantee against future terrorist attacks. Nonetheless, I have expedited work on anti-terrorism legislation, within which the Administration has insisted on including general criminal law measures not limited to terrorism, in order to allow the Senate to act promptly in response to the unprecedented attacks of September 11, 2001.

Sincerely,

PATRICK LEAHY,
Chairman.

Mr. LEAHY. I understand the distinguished Senator from Wisconsin is willing to have the distinguished Senator from Michigan recognized for 5 minutes. I ask unanimous consent she be allowed to proceed preceding the Senator from Wisconsin.

The PRESIDING OFFICER. Without objection, it is so ordered.

The Senator from Michigan is recognized for 5 minutes.

Ms. STABENOW. I thank our distinguished chairman and my friend from Wisconsin for allowing me to proceed before he presents his amendments.

I rise this evening to congratulate all involved in this effort. As has been said on so many occasions, it is not perfect but we have come together with a very positive, important step forward that we can all celebrate this evening on a bipartisan basis.

As the Senator from Michigan, along with my colleague, Senator LEVIN, we certainly celebrate the efforts along the northern border and the important authorizations for dollars that allow us to continue to protect and strengthen the efforts at the border. I thank my chairman of the Banking Committee, Senator SARBANES, for his efforts to put into this important bill language dealing with the critical issue of money laundering which essentially allows us to follow the money.

My colleague, Senator LEVIN, has been extremely involved in helping to lead efforts to lay out the case for this. Senator KERRY and Senator GRASSLEY have been involved in important work. I thank them.

The antiterrorism bill before the Senate takes a significant step forward in cutting the flow of terrorist money. As the President has repeatedly said, stopping the flow of money is key to stopping terrorism. That is what we are doing this evening. In particular, we are establishing important new responsibilities, both for our Government and for our financial institutions. The bill authorizes the Treasury Secretary to take special measures to stop suspected money-laundering activities. This anti-money-laundering language is significant because it requires financial institutions to set up their own due diligence to combat money laundering, particularly for private and corresponding banking situations. This is a key provision of which I was proud to be a part. I am pleased we were able to come up with language that allows that.

Another important provision I was pleased to offer in the Banking Committee, which is now part of the bill, was clear authority for the Treasury Secretary to issue regulations to crack down on abuses related to concentration accounts. These accounts are administrative accounts used by financial institutions to combine funds from multiple customers, various transactions. They do not require any identification or accountability of who is involved or how much money we are talking about.

The amendment I advocated urges the Treasury Secretary to issue regulations ensuring these concentration accounts identify by client name all of the client funds moving through the account to prevent anonymous movement of the funds that might facilitate money laundering. This is a classic case of why this is so important: Raul Salinas, brother of former Mexican President Carlos Salinas, transferred almost $100 million to Citibank administrative accounts in New York and London without any documentation indicating the ownership of these funds. The wire transfers sent the funds to Citibank and asked each transfer be brought to the attention of a specific private banker. Later, the private banker transferred the funds to private accounts controlled by Mr. Salinas. The origin of this money—$100 million—was never satisfactorily identified.

Allegations of drug money or other corporate sources persist to this day. We know, through Senator LEVIN's exhaustive documentation at his hearings, that other private banks use this practice as well. Although financial regulators have cautioned against this practice over and over again, they have not yet issued regulations to stop this loophole. That is why the language in this bill is so important.

The use of these anonymous concentration accounts breaks the audit trail associating specific funds with specific clients. Again, the goal, as the President said, is to follow the money. We have to have information if we are going to follow the money.

It should now be abundantly clear to Treasury that they have the authority to stop this practice. I hope it is also abundantly clear it is a serious problem. I am very concerned that the administration act quickly on these anonymous accounts.

I congratulate everyone involved in this effort. I think the effort regarding the anti-money-laundering language is a critical part of making sure we have an effective antiterrorism bill. I thank my colleagues for their work.

The PRESIDING OFFICER. The time of the Senator from Michigan has expired. Who yields time?

The Senator from Wisconsin.

Mr. FEINGOLD. Mr. President, I will give a brief statement before I start my amendments, and I ask unanimous consent the time be equally divided amongst the time I have on each of my four amendments.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. FEINGOLD. Mr. President, 1 month ago, we all were viciously attacked. I am pleased and grateful that both the domestic and international effort to respond to these attacks is fully underway. As we recall, almost as soon as the attacks of September 11 ended, our public discussion turned to two issues: how the United States will respond to these terrorist acts and how we can protect ourselves against future attacks.

Almost immediately, discussion of that second issue raised the question of how our efforts to prevent terrorism will affect the civil liberties enjoyed by all Americans as part of our constitutional birthright.

I was encouraged by many of the reactions that our leaders and Members of this body had, but especially encouraged by the words of our colleague, Senator GEORGE ALLEN of Virginia who represents one of the States struck by

terrorism. On the day after the attacks he said:

We must make sure that as we learn the facts, we do not allow these attacks to succeed in tempting us in any way to diminish what makes us a great nation. And what makes us a great nation is that this is a country that understands that people have God-given rights and liberties. And we cannot—in our efforts to bring justice—diminish those liberties.

I agree with Senator ALLEN. I believe that one of the most important duties of this Congress is in responding to the terrible events of September 11, in order to protect our civil liberties, which, of course, derive from our Constitution. That is why I am pleased that we did not take the Attorney General's advice to enact an anti-terrorism bill immediately without any deliberation or negotiation. I commend Senator LEAHY for all his efforts to improve this bill. It is certainly a better and more comprehensive bill than the one the administration originally proposed. I think even the administration recognizes that.

But I still believe we needed a more deliberative process on this bill, and more careful consideration of the civil liberties implication of it. I held a hearing in the Constitution Subcommittee at which many serious and substantive concerns about the bill were raised by commentators and experts from both sides of the political spectrum.

As the chairman of the subcommittee, I took many of those concerns very seriously. That is why I would not consent on Tuesday night to bringing up this bill and passing it without any amendments being considered. I am pleased that we were able to reach agreement on a process that will allow some of my concerns with this bill to be debated and voted on through the amendment process.

That is not to say that no measures to strengthen law enforcement should be enacted. They should be. We need to do it. We need to do some very serious updating of a number of these laws. This bill does many things to assist the Department of Justice in its mission to catch those who helped the terrorists and prevent future attacks. We can and we will give the FBI new and better tools. But we must also make sure that the new tools don't become instruments of abuse.

There is no doubt that if we lived in a police state, it would be easier to catch terrorists. If we lived in a country where the police were allowed to search your home at any time for any reason; if we lived in a country where the government was entitled to open your mail, eavesdrop on your phone conversations, or intercept your email communications; if we lived in a country where people could be held in jail indefinitely based on what they write or think, or based on mere suspicion that they were up to no good, the government would probably discover and arrest more terrorists, or would be terrorists, just as it would find more lawbreakers generally. But that would not be a country in which we would want to live, and it would not be a country for which we could, in good conscience, ask our young people to fight and die. In short, that country would not be America.

I think it is important to remember that the Constitution was written in 1789 by men who had recently won the Revolutionary War. They did not live in comfortable and easy times of hypothetical enemies. They wrote the Constitution and the Bill of Rights to protect individual liberties in times of war as well as in times of peace.

There have been periods in our nation's history when civil liberties have taken a back seat to what appeared at the time to be the legitimate exigencies of war. Our national consciousness still bears the stain and the scars of those events: The Alien and Sedition Acts, the suspension of habeas corpus during the Civil War, the internment of Japanese-Americans during World War II and the injustices perpetrated against German-Americans and Italian-Americans, the blacklisting of supposed communist sympathizers during the McCarthy era, and the surveillance and harassment of antiwar protesters, including Dr. Martin Luther King, Jr., during the Vietnam war. We must not allow this piece of our past to become prologue.

Preserving our freedom is the reason we are now engaged in this new war on terrorism. We will lose that war without a shot being fired if we sacrifice the liberties of the American people in the belief that by doing so we will stop the terrorists.

That is why this exercise of considering the administration's proposed legislation and fine tuning it to minimize the infringement of civil liberties is so necessary and so important. And this is a job that only the Congress can do. We cannot simply rely on the Supreme Court to protect us from laws that sacrifice our freedoms. We took an oath to support and defend the Constitution of the United States. In these difficult times that oath becomes all the more significant.

There are quite a number of things in this bill that I am concerned about, but my amendments focus on a small discreet number of items.

At this point, I would like to turn to one of the amendments.

The PRESIDING OFFICER. The Senator is recognized.

AMENDMENT NO. 1899

Mr. FEINGOLD. I send an amendment to the desk and ask for its immediate consideration.

The PRESIDING OFFICER. The clerk will report.

The assistant legislative clerk read as follows:

The Senator from Wisconsin [Mr. FEINGOLD] proposes an amendment numbered 1899.

Mr. FEINGOLD. I ask unanimous consent the reading of the amendment be dispensed with.

The PRESIDING OFFICER. Without objection, it is so ordered.

The amendment is as follows:

(Purpose: To make amendments to the provisions relating to interception of computer trespasser communications)

On page 42, line 25, insert "or other" after "contractual".

On page 43, line 2, strike "for" and insert "permitting".

On page 43, line 8, insert "transmitted to, through, or from the protected computer" after "computer trespasser".

On page 43, line 20, insert "does not last for more than 96 hours and" after "such interception".

Mr. FEINGOLD. I ask this time now be charged to the first amendment.

The PRESIDING OFFICER (Ms. STABENOW). The time will be charged.

Mr. FEINGOLD. Madam President, this amendment simply clarifies the provision in the bill dealing with computer trespass, section 217, so that it more accurately reflects the intent of the provision, as frequently expressed by the administration. Section 217 is designed, we have been told, to permit law enforcement to assist computer owners who are subject to denial of service attacks or other episodes of hacking. As currently drafted, however, this provision could allow universities, libraries, and employers to permit government surveillance of people who are permitted to use the computer facilities of those entities. Such surveillance would take place without a judicial order or probable cause to believe that a crime is being committed. Under the bill, anyone accessing a computer "without authorization" is deemed to have no privacy rights whatsoever, with no time limit, for as long as they are accessing the computer at issue. Basically, the way I read this, this provision completely eliminates fourth amendment protection for a potentially very large set of electronic communications.

The danger that this amendment tries to address is that "accessing a computer without authorization" could be interpreted to mean a minor transgression of an office or library computer use policy. Let's take an example. A working mom uses an office computer to purchase Christmas presents on the Internet. Company policy prohibits personal use of office computers. This person has potentially accessed a computer without authorization and her company could give permission to law enforcement to review all of the e-mails that she sends or receives at work, monitor all the instant messages she sends, and record every website she visits: No warrant, no probable cause, no fourth amendment rights at all. My amendment makes clear that a computer trespasser is not someone who is permitted to use a computer by the owner or operator of that computer.

This amendment also limits the length of this unreviewed surveillance to 96 hours, which is a longer time frame than that placed on other emergency wiretap authorities. Again, if

this provision is aimed solely at responding to cyber-attacks, there is no need to continue such surveillance beyond 96 hours—which is the time we put in our amendment—because that time is sufficient to allow the government to obtain a warrant to continue the surveillance. It is not as if they cannot continue it, they simply have to get a warrant after 4 days. Warrants based on probable cause are still the constitutionally preferred method for conducting surveillance in America. The need for immediate and emergency assistance during a denial of service attack or hacking episode, which I certainly think is a legitimate concern, cannot justify continued surveillance without judicial supervision.

Finally, this amendment prevents law enforcement from abusing this authority in investigations unrelated to the actual computer trespass. The current provision potentially allows law enforcement to intercept wire and electronic communications in many investigations where they may not want, or be able, to secure a court order. If the government suspects a person of committing a crime but does not have probable cause to justify monitoring of the suspect's work computer, it could pressure the owner or operator of the computer to find some transgression in the suspect's computer use, allowing the government carte blanche access to email and internet activity of the suspect. I suspect that few small business owners will be anxious to stand up to federal law enforcement requests for this information.

Now the administration was apparently willing to add language to deal with employees using office computers, but it refused to recognize that in our society many people use computers that they do not own, with permission, but without a contractual relationship. People who don't own their own home computers use computers at libraries. Students use computers at school in computer labs or student centers. Without my amendment, these innocent users could become subject to intrusive government surveillance merely because they disobeyed a rule of the owner of the computer concerning its use. I have been told that this is not the administration's intent, but they would not fix this provision. So I think it is fair to ask why. Why does the administration insist on leaving open the possibility that this provision will be abused to entirely eliminate the privacy of students' and library patrons' computer communications? Is there a hidden agenda here? I sincerely hope not, but I was very disappointed in the administration's unwillingness to address this concern. I remain willing to negotiate on this amendment, but if there is no further movement on it, I hope my colleagues will recognize that this amendment will leave the publicly expressed purpose of the computer trespass provision untouched and fix a potentially disastrous case of overbreadth.

I reserve the remainder of my time.

I ask for the yeas and nays on the amendment.

The PRESIDING OFFICER. Is there a sufficient second?

There is a sufficient second.

The yeas and nays were ordered.

Mr. FEINGOLD. Madam President, how much time do I have remaining on my side?

The PRESIDING OFFICER. Eighteen and one-half minutes on this amendment.

Mr. FEINGOLD. Madam President, I yield 5 minutes to the Senator from Washington.

The PRESIDING OFFICER. The Senator from Washington is recognized.

Ms. CANTWELL. Madam President, I rise to support my colleague, Senator FEINGOLD, and his amendment to section 217. I think the Senator has done a tremendous job in outlining the issues related to this bill and the fact that haste can sometimes make waste. Haste in some instances on very well crafted language to uphold our rights under the Constitution can be infringed upon.

Section 217 is intended to allow computer system owners and operators to fully engage Federal law enforcement where someone hacks or intrudes into their system. As Senator FEINGOLD mentioned, that could be a business owner, or it could be a library system, or it could be a university system.

Unfortunately, as drafted, there are few limits on what communications the Government could intercept without showing probable cause that a crime has been committed and without having the opportunity for judicial review of those intercepts.

The provisions do not even limit the scope of the surveillance. Once authorized, the Government could intercept all communications of a person who is allegedly a trespasser. Again, let me be clear: Without meeting the fourth amendment requirement to show probable cause.

Further, there is no time limit on the surveillance under the provision of this legislation. For those who may be reviewing this legislation for the first time, and understanding that as they go to their workplace, or as they go to their educational institution, or as they go to their library to enhance their education, they could be under surveillance for a very long and indefinite period of time without their knowledge.

Thus, once authorized by a computer system operator, the Government could intercept all communications of a person forever without a proper search warrant. Even a court order wiretap expires after 30 days.

This amendment would remedy some of the defects in this bill. It would do that by requiring that the surveillance be only of communications associated with the trespass and that the length of the surveillance be limited to 96 hours, which, by the way, is twice as long as the time limit placed on emergency wiretap authority. If the problem continues, investigators could easily obtain additional warrant time for the surveillance to continue.

This is a very important time in our country's history. It is a time in which we want to act in unity and support the administration. It is a time in which we want to act to give law enforcement the tools they need to apprehend those who have been responsible and may be responsible for future acts of terrorism. But we also must preserve the right of citizens of this country when it comes to the fourth amendment.

I encourage my colleagues to support the Feingold amendment. I yield the floor.

The PRESIDING OFFICER. Who yields time?

Mr. FEINGOLD. Madam President, first, I want to say how important it is to have on the committee the Senator with expertise in this area as well as her own background. I appreciate very much her help on this matter.

Madam President, how much time do I have remaining on my side?

The PRESIDING OFFICER. The Senator has 14½ minutes.

Mr. FEINGOLD. I am happy to yield 5 minutes to the Senator from Minnesota.

The PRESIDING OFFICER. The Senator from Minnesota.

Mr. WELLSTONE. Madam President, my colleague from Washington I think speaks within a framework of expertise that she brings to this particular amendment. I speak from the framework of a layperson who has been trying to understand this bill's pluses and minuses.

I say to Senator FEINGOLD and all colleagues, since I think there is kind of a rush to table all of the Feingold amendments, that this amendment is eminently reasonable. The Senator from Wisconsin is saying: Let's put a time limit on this. That is good. Let's have some judicial oversight. That is good as well.

There are international terrorists who have killed many Americans and want to kill more Americans. There are a lot of provisions in this bill which I think are right on the money, including northern border protection which is relevant to the Chair, relevant to the Senator from Washington, and certainly relevant to the people I represent. But I also think there is no reason, in this rush to pass the bill, that we can't make some changes. These are minor changes the Senator wants to make. This just gives this piece of legislation more balance.

I will say this: There is a lot that is good in this bill and a lot that is attractive to me as a Senator. When you add some of the additional security provisions that help all the people we are asked to represent in addition to the benefits—the financial help to all of the rescue workers and all of the innocent people's families, people have been murdered—there is much in this

bill that is commendable. The Senator from Wisconsin is just trying to give it more balance.

I say to my colleagues that I hope you will support this amendment. I want to say one other thing as well. I really believe what is good about this bill is the provisions that focus on the people whom the terrorists are basically trying to kill—Americans. What is not as good is when the reach of the bill goes too far beyond that and is too broad.

The sunset provision that passed in the House is so important, so that we can continue to monitor this legislation as we move forward.

I think this amendment that the Senator from Wisconsin has submitted is a step to give this piece of legislation a little more balance, and it will be more vigilant of people's civil liberties. I think it is the right step.

I thank the Senator for his amendment.

Mr. FEINGOLD. I thank the Senator from Minnesota for his help, especially for making this point: All this amendment is about is making sure that it is about the problem we face with the terrorism that is threatening our country and our freedoms. That is all we are trying to do—make sure it doesn't go broadly into people's rights, and into their privacy, and into their own lives.

At this point, I am simply going to reserve the remainder of my time.

The PRESIDING OFFICER. Who yields time?

Mr. HATCH. Madam President, let me talk a little bit about the provision of today's legislation that has been referred to as the "computer trespasser" exception.

This provision is a perfect example of how our laws dealing with electronic surveillance have become outdated, and nonsensical as applied to modern technology.

Imagine the following scenario. A terrorist decides to wreak havoc in a major U.S. city by shutting down an electrical power grid. He uses a computer to hack into the mainframe computer of a regional utility company, which he plans to use to bring down the power grid. Before the terrorist can accomplish his goal, the utility company recognizes that an intruder is attempting to access their computer. The company quickly calls the FBI for assistance in repelling the intruder.

Guess what? Under current law, even with the permission from the utility company, the FBI is not permitted to monitor the terrorist's activity on the utility company's computer, because current law perversely grants the terrorist privacy rights with respect to his communications on the computer he has invaded.

It is as if police could not investigate a burglary, even when invited into the house by the victim of the burglary, because the burglar had established privacy rights inside the home he has invaded.

It is anomalies such as this, in our current laws regarding electronic surveillance, that today's legislation is designed to fix.

As it stands, the computer trespasser provision is defined in such a way that the owner or operator of a computer network cannot arbitrarily declare the user of the network at trespasser, and then invite law enforcement in to monitor that user's communications.

The provision, as written, provides that a person is not considered a computer trespasser if the person has an "existing contractual" relationship for access to all or part of the computer network.

Senator FEINGOLD's amendment would broadly amend the negotiated exception, including within its scope anyone with a contractual or "other" relationship to the owner or operator of a computer network. What is meant by "other" relationship? Any hacker could make the argument that they have a relationship with a computer operator. Indeed, were I a defense counsel, I would argue that the mere fact that the hacker has accessed the computer has created some form of relationship. Clearly, the proposed amendment would broadly and unwisely give immunity from our cyber-crime laws. This amendment creates an exception to the criminal laws and puts law enforcement back in the same position they currently are—that is, powerless to investigate hacking incidents where the owner of the computer network wants the assistance of law enforcement.

Madam President, we should not tie the hands of our law enforcement to assist the owners of our computer networks. We should not help hackers and cyberterrorists to get away.

If you are a victim of a burglary, shouldn't you have the right to ask the police to investigate your house, to come to your house and investigate?

Why should the owners of the computer not have the right to ask the police to investigate a commuter-hacking incident, especially where it appears it is terrorist oriented?

This act applies, as written, only to people without authorization to be on the computer. Why should the law protect people who have invaded a computer they have no right to be on?

Let me say one last comment about this. The proponents of this amendment argue it will apply to students using a university computer. That is true, but only if such students use that university computer to hack into a place where they do not belong.

Either we have to get serious in this modern society, with these modern computers, about terrorism or we have to ignore it. I, for one, am not for ignoring it. I believe we need to have this language in here—so does the Justice Department; so does the White House and the White House Counsel's Office—in order to do what cannot be done today to protect people in our society, and to protect our powerplants, our dams, and so many important facilities in our society that are vulnerable to cyber-terrorists. This law, the way it is currently written, will help to do that.

That is all I care to say about it. But I believe we should vote down the Senator's amendment. I know it is well intentioned. I have great respect for the Senator from Wisconsin. He is one of the very diligent members of our committee, and I appreciate him very much, but on this amendment I believe we have to keep the language of the bill the way it is written in order to give our law enforcement people the tools to be able to stop terrorist hacking into computers.

The PRESIDING OFFICER. The Senator from Wisconsin.

Mr. FEINGOLD. I thank my friend for his kind words.

Madam President, in response to the points he made, first, let me respond that I accept the premise of this basic provision in terms of updating the ability to get at computer hackers. That is an update. We did not know what this was a few years ago. We did not know what risks it posed. Nobody opposes that very important part of this bill.

But what the Senator claims is that the phrase "contractual relationship" somehow makes sure that people are protected from being subject to this who really should not be subject to this; but it does it.

I can think of at least three categories of people who do not come within the category of "contractual relationship." One is in the context employment. It is nice if you have a contract, but a lot of employees do not. They do not fall within the protection of a contractual relationship.

The same goes for people who would go and use a computer at a library. They do not have a contractual relationship to protect them in this situation.

And finally, as the Senator conceded here, in his last example, that certainly students, students at all our universities across the country, are not protected by that language. And that is all we want to do, to make it clear that this amendment is related to the problem of computer hackers, not moms who might be buying Christmas presents on a computer at work, even though they are not supposed to, or students who maybe are gambling on a university computer. Of course they should not do that, but should that subject them to extraordinary, unprecedented intrusion by Government law enforcement authority? Of course not.

The Senator attempts to suggest that the provision in here having to do with our desire to have the language say "contractual" or "other" relationship would somehow allow a hacker to claim that he is protected. The notion that a hacker would be considered as somebody who has a relationship with the company under this amendment is an absurd interpretation of the amendment's intent, so that clearly is not what this amendment would do.

And finally, let me get back to the students, the example the Senator

from Utah mentioned. It is simply an unprecedented intrusion into individual rights for a university to be able to allow—because of a minor use that is not within university rules—that person to be completely subject to this kind of intrusion.

Mr. DURBIN. Will the Senator yield for a question?

Mr. FEINGOLD. Yes.

Mr. DURBIN. I have followed this debate closely. I commend the Senator for the hearing he had on the constitutional rights part of this debate. But I want to make sure I understand exactly what his amendment sets out to do.

Is my understanding correct that under the Feingold amendment there could be surveillance of a computer for 96 hours before there is any court approval, so that in the example given by the Senator from Utah, the law enforcement authorities could, in fact, monitor the communications of someone using this computer for 96 hours before ever going to a court and asking for a warrant for that search?

Mr. FEINGOLD. That is correct. And that even troubles me for the length of time that it is allowed—but it is far better than an infinite position. Law Enforcement should be required to seek a warrant as soon as possible, within reason, given the fact that what the amendment tries to get at is emergency situations involving hackers. As soon as possible, they should have to meet the standards that are normally met.

But, yes, the amendment does permit that, in my view, rather extraordinary period of time before the requirement would have to be made.

Mr. DURBIN. And that period of time, I ask the Senator from Wisconsin, is roughly twice the amount currently given under emergency wiretap authority; is that correct?

Mr. FEINGOLD. That is correct.

Mr. DURBIN. One last question. I want to try to understand. I ask the Senator do you not say, in your amendment, that a trespasser does not include someone who is permitted to use a computer by the owner or operator of the computer?

Mr. FEINGOLD. Correct.

Mr. DURBIN. And the difference, of course, is whether it is a contractual relationship or just a permission to use; you are including permission to use as well as contractual relationship?

Mr. FEINGOLD. That is correct.

Mr. DURBIN. The examples you have given are of people going to a library, who may not have a contractual relationship with the library but use the computer, who would be subjected to this warrantless search of their computer communications for an indefinite period of time.

Mr. FEINGOLD. That is right, exactly. This is exactly the problem. All we asked of the committee and of the administration yesterday was to make it clear that they did not want to reach these people. That is what we have been told. The purpose of this is to get at the threat of computer hackers.

The Senator from Illinois has just illustrated, with those examples—and he is, of course, correct—that this could be interpreted and could be understood to include situations that not only have nothing to do with the problem but represent a very serious departure from the individual rights people should have in our country.

Mr. DURBIN. I thank the Senator from Wisconsin.

Mr. FEINGOLD. I thank the Senator from Illinois and reserve the remainder of my time.

Mr. LEAHY. Madam President, I have been concerned about the scope of the amendment carving an exception to the wiretap statute for so-called "computer trespassers." This covers anyone who accesses a computer "without authorization" and could allow government eavesdropping, without a court order or other safeguards in the wiretap statute, or Internet users who violate workplace computer use rules or online service rules.

I was unable to reach agreement with the administration on limiting the scope of this amendment, and the Feingold amendment makes further refinements. It is unfortunate that the administration did not accept this amendment.

The PRESIDING OFFICER. Who yields time?

Mr. HATCH. Madam President, how much time remains?

The PRESIDING OFFICER. The Senator from Wisconsin has 4 minutes 47 seconds; the managers have 9 minutes 14 seconds.

Mr. HATCH. I am prepared to yield back whatever time we have, if it is all right with the distinguished Senator from Vermont, with the understanding that we are just trying to stop unauthorized hacking that could be done by terrorists and others who are criminals that currently cannot be stopped. I am prepared to yield back the time, if the distinguished Senator from Vermont is.

The PRESIDING OFFICER. The Senator from Pennsylvania.

Mr. SPECTER. Madam President, I ask the chairman of the committee, after listening to the presentation by the Senator from Wisconsin, what is the chairman's view of the incursion on law enforcement by the limitation of 96 hours?

Mr. LEAHY. The incursion of law enforcement by the 96 hours?

Mr. SPECTER. The principal thrust of what the Senator from Wisconsin seeks to do is to broaden the definition of a contractual relationship to someone who may otherwise have permission. What I am trying to do is to understand the administration's position, the law enforcement position as to how law enforcement is adversely impacted by what the Senator from Wisconsin seeks to do.

My concern, as expressed earlier, is that, especially in the face of the challenge by the amendment, this is a complicated bill.

The reality is, it is hard to know all of it without the normal hearing process. Now we have a specific challenge. What I would like to know is, how does it inhibit law enforcement? What about the broader definition gives problems to law enforcement? And then, what is the difficulty in having 96 hours, which is 4 days, to see what is going on to find some basis for seeking a warrant with probable cause?

Mr. LEAHY. Frankly, I don't have a problem with the Feingold amendment as it is written. I do have a problem, however, with keeping a bill together. The initial administration request had no limitations whatsoever. It was so wide open we were concerned that someone who might be using a computer at work to add up their accounts for the month would be trapped by this because the company said you couldn't use the computer to add up your checking account, for example, to use a far-fetched example, because they would be accessing the computer without authorization and the Government could just step in and go forward.

The administration moved partly our way. We actually ended up with a compromise on this. I suspect what they would say to the Senator from Pennsylvania is that these attacks last more than 96 hours and that they would be unable to go after them if they were limited to the 96 hours.

We saw this recently 2 or 3 weeks ago where we had a continuous roving attack on a number of Government computers. As I recall—I didn't pay that much attention at the time—they were attacking them one week and when we came back the following week, they were still attacking them. So you had more than 96 hours.

Frankly, it is a case where we have reached a compromise. The distinguished ranking member, speaking on behalf of the administration, said this is not acceptable to them. Had this been part of the original package, I wouldn't have found it acceptable.

Mr. HATCH. Will the Senator yield?

Mr. SPECTER. Yes.

Mr. HATCH. Basically, what the administration is after here is that if a burglar is coming into your home and the police come to investigate, they don't have to report to a judge within 96 hours. The police have to act on these terrorist matters. If they find that a terrorist has infiltrated a computer controlling an electrical grid system, they want to get right on the ball and do something about it. That is what they are trying to do with this provision.

There are no fourth amendment rights implicated because you have people who have hacked into a computer that they don't have any right to be in.

We want to give law enforcement the power to stop that. This provision upsets that power and basically puts us back where we are when we can't do

anything in a modern digital age to stop terrorists from stopping power grids and damaging dams and a whole raft of other things.

Mr. SPECTER. Madam President, if the Senator from Utah will yield for a question?

Mr. HATCH. Surely.

Mr. SPECTER. The Senator from Wisconsin makes the point that people may have standing to use a computer even without a contractual relationship. He uses the example of a student. Does the Senator from Utah believe or does the administration represent that there are no relationships other than contractual which give a person the legitimate standing to use the computer?

Mr. HATCH. Under this provision, you do not have a right to hack into another private computer, whether you are a university student or anybody else. It only applies, the law we have written, to unauthorized access. It does not apply to authorized access. But unauthorized access, yes, it applies to that. If we don't put it in there, we will be leaving a glaring error that currently exists in our laws that prohibit us from solving some of these problems. It would be a terrible thing to not correct at this particular time, knowing what we know about how these terrorists are operating right now.

Mr. SPECTER. So is the Senator from Utah saying that if you have permission, that is a form of a contractual relationship?

Mr. HATCH. I am saying that if you have permission, you are not covered by this provision as written. In other words, you would not be considered a hacker.

Mr. SPECTER. On its face you would seem to, unless there is a contractual relationship?

Mr. HATCH. It comes down to authorized or unauthorized access. If it is authorized, it is not covered under the computer trespasser provision.

Mr. SPECTER. I thank the Senator.

The PRESIDING OFFICER. The Senator from Wisconsin.

Mr. FEINGOLD. Madam President, did the Senator yield back his remaining time?

Mr. HATCH. Yes, we are prepared to yield.

Mr. LEAHY. We are prepared if the Senator from Wisconsin is.

Mr. FEINGOLD. I want to clarify a couple points, then I will be prepared to yield the remaining time.

These were helpful exchanges on a couple of points. First of all, it became very clear from Senator SPECTER's excellent questioning that, of course, there is no guarantee, under the way this language is set up, under the words "contractual relationship," that the provision would not apply to students or to people who would use a computer at a library. I can't understand why, if that is the intent of the administration, the intent of the legislation, why they don't just agree to language that would say so. That is all we asked for yesterday. It could have resolved the problem. For some reason, they won't agree to it.

Second, is this notion that a hacker could somehow get in under our language. There is no way that a hacker has a relationship with the computer owner that permits the use of the computer. The hacker is, obviously, the antithesis, the opposite of an individual with a relationship that permits use of the computer.

Finally, I am amazed at this notion that this amendment, even under our version of it, would allow only 96 hours for surveillance when under the example of the Senator from Utah, an ongoing hacker attack is occurring.

Is it the Senator's contention that at the end of 96 hours, the FBI would not have probable cause to get a warrant, when all it has been dealing with for 4 days is this hacking of the computer? Of course, it would. It would be the easiest thing in the world.

Section 217 is a very dramatic exception to the usual rule as derived under our system, and expressed in the fourth amendment. Normally, you have to come up with probable cause and a warrant. There are exceptions because we have difficult problems sometimes. But 96 hours? At the end of that time, with clear evidence of a hacking attempt, a warrant could easily be obtained. Obviously, our amendment takes care of the need for emergency authorization. In fact, I think it is too generous. I am trying to put some kind of a time limit on this so we can have some semblance of the normal rules that protect our citizens.

If the other side yields their time, I will yield my remaining time as well.

The PRESIDING OFFICER. The majority leader is recognized.

Mr. DASCHLE. Madam President, I have listened to this debate with great interest, and I appreciate very much the arguments made by the Senator from Wisconsin. As the Senator from Vermont and, I believe, the Senator from Pennsylvania, have noted, there are circumstances where I can easily see that we could be sympathetic to his amendment. He makes an argument.

My difficulty tonight is not substantive as much as it is procedural. There is no question, all 100 of us could go through this bill with a fine-tooth comb and pinpoint those things which we could improve. There is no doubt about that. I have looked at this bill, and there are a lot of things, were I to write it alone, upon which I could improve. I know the chairman of the committee believes that too.

I think we also have to recognize that this is the product of a lot of work in concert with our Republican colleagues, in concert with the administration, in concert with civil liberties groups, and in concert with law enforcement. We have come up with what I would view as a delicate but, yes, successful compromise.

Now, if we had opened the bill to amendment, I have no doubt there are many colleagues who would offer amendments with which I would vehemently disagree—in fact, so much so that I might want to filibuster the bill. I would probably lose. I think there is a realistic expectation that on a lot of these issues, my side would lose. I think you could make the same case for the other side. So, we made the best judgment we could, taking into account the very delicate balance between civil liberties and law enforcement that we had to achieve in bringing a bill of this complexity to the floor.

I have to say, I think our chair and ranking member and all of those involved did a terrific job under the most difficult of circumstances. What we did was to say: Let's take this product and work with it; let's review it; if we have to make some changes, let's consider them; but let's recognize that if we were to take this bill open-ended, there would be no end to the amendments—that is the result that would most likely occur in such a circumstance.

While I may be sympathetic to some amendments offered tonight, had it been an open debate, there would have been a lot of amendments for which I would not have been sympathetic.

Given those circumstances, my argument is not substantive, it is procedural. We have a job to do. The clock is ticking. The work needs to get done. We have to make our best judgment about what is possible, and that process goes on.

I hope my colleagues will join me tonight in tabling this amendment and tabling every other amendment that is offered, should he choose to offer them tonight. Let's move on and finish this bill. Let's work with the House and come up with the best product between the Houses. Then, let's let law enforcement do its job, and let's use our power of oversight to ensure that civil liberties are protected.

I make a motion to table.

Mr. LEAHY. Will the Senator withhold that motion to table for a moment?

Mr. DASCHLE. Yes.

Mr. LEAHY. Madam President, I have served with over 250 Senators here, and I have been proud to serve with all of them. I know of no Senator who has a stronger commitment to our individual rights and personal liberties than the senior Senator from South Dakota, our majority leader. But I also know that were it not for his commitment and efforts, we would not be here with a far better bill than the one originally proposed by the administration. It has been because of his willingness to back us up as we try to improve that bill, to remove unconstitutional aspects of it, because of his willingness, we were able to get here.

As the Senator from South Dakota, the dearest friend I have in this body, has said, he could find parts he would do differently, and he knows there are parts I would do differently—even on this one. I have high regard for the