handled by top officials in the deputy attorney general's office and Justice's criminal division.''

So while former administration officials grant press interviews and write opinion articles denying wrongdoing; while the White House and Justice Department hold closed briefings for the media to disavow the reasoning of this previously relied upon memoranda and to characterize what happened; Senators of the United States are denied basic information and access to the facts. The significance of such unilateralism and arrogance shown to the Congress and to its oversight committees cannot continue.

I have long said that somewhere in the upper reaches of this administration a process was set in motion that rolled forward until it produced this scandal. To put this scandal behind us, first we need to understand what happened. We cannot get to the bottom of this until there is a clear picture of what happened at the top. It is the responsibility of the Senate, including the Judiciary Committee, to investigate the facts, from genesis to final approval to implementation and abuse. The documents must be subject to public scrutiny, and we will continue to demand their release.

There is ample evidence that American officials, both military and CIA, have used extremely harsh interrogation techniques overseas, and that many prisoners have died in our custody. Administration officials admit that 37 foreign prisoners have died in captivity, and several of these cases are under investigation, some as homicides. On June 17, David Passaro, a CIA contractor, was indicted for assault for beating an Afghan detainee with a large flashlight. The prisoner, who had surrendered at the gates of a U.S. military base in Afghanistan, died in custody on June 21, 2003, just days before I received a letter from the Bush administration saying that our Government was in full compliance with the Torture Convention.

Some individuals who committed abusive acts are being punished, as they must be. But what of those who gave the orders, set the tone or looked the other way? What of the White House and Pentagon lawyers who tried to justify the use of torture in their legal arguments? The White House has now disavowed the analysis contained in the August 1, 2002, memo signed by Jay Bybee, then head of the Office of Legal Counsel. That memo, which was sent to the White House Counsel, argued that for acts to rise to the level of torture, they must go on for months or even years, or be so severe as to generate the type of pain that would result from organ failure or even death. The White House and DOJ now call that memo ''irrelevant'' and ''unnecessary'' and say that DOJ will spend weeks rewriting its analysis.

As we all know, on June 22, 2004, the White House released a few hundreds of pages of documents—a self-serving and highly selective subset of materials. The documents that were released raised more questions than they answered. Now, more than two weeks later, none of those issues have been resolved.

For example, the White House released a January 2002 memo signed by President Bush calling for the humane treatment of detainees. Did the President sign any orders or directives after January 2002? Did he sign any with regard to prisoners in Iraq?

Why did Secretary Rumsfeld issue and later rescind tough interrogation techniques? And how did these interrogation techniques come to be used in Iraq, where the administration maintains that it has followed the Geneva Conventions?

Where is the remaining 95 percent of material requested by members of the Senate Judiciary Committee? Why is the White House withholding relevant documents dated after April 2003?

I was gratified that the Senate on June 23 passed an amendment that I offered to the Defense authorization bill that will clarify U.S. policy with regard to the treatment of prisoners and increase transparency. But the stonewalling continues: The Pentagon opposes this amendment. I am hopeful that we will prevail in keeping this provision in the bill. Five Republican Senators supported the amendment against an attempt to table it. I thank each of them. I also want to commend the Senate for adopting, also as part of the Defense authorization bill, the Durbin amendment against torture, and I want to acknowledge an important step taken in the House on the same day. The House Appropriations Committee added language to the 2005 Justice Department spending bill that would prohibit any department official or contractor from providing legal advice that could support or justify use of torture.

As it completed its term, the Supreme Court issued its decisions in highly significant cases involving the legal status of so-called enemy combatants. The Court reaffirmed the judiciary's role as a check and a balance, as the Constitution intends, on power grabs by the executive branch. The Court ruled that the Bush administration's assertion that the President can hold suspects incommunicado, indefinitely and without charge, is as arrogant as are its legal arguments that the President can authorize torture. No President is above the law or the Constitution. The Court properly rejected the administration's plea to 'just trust us' and repudiated its assertion of unchecked power.

This Senate and in particular the Judiciary Committee continues to fall short in its oversight responsibilities. President Bush has said he wants the whole truth, but he and his administration instead have circled the wagons to forestall adequate oversight. The President must order all relevant agencies to release the memos from which these policies were devised. There needs to be a thorough, independent investigation of the actions of those involved, from the people who committed abuses, to the officials who set these policies in motion. Only when these actions are taken will we begin to heal the damage that has been done.

We need to get to the bottom of this scandal if we are to play our proper role in improving security for all Americans, both here at home and around the world.

THREAT TO ONLINE PRIVACY

Mr. LEAHY. Mr. President, I want to address a recent court decision that has exposed America's e-mails to snooping and invasive practices. The 2-to-1 decision by the First Circuit Court of Appeals in a case called United States v. Councilman has dealt a serious blow to online privacy. The majority—both, Republican-appointed judges—effectively concluded that it was permissible for an Internet Service Provider to comb through its customers' emails for corporate gain. If allowed to stand, this decision threatens to eviscerate Congress's careful efforts to ensure that privacy is protected in the modern information age.

The indictment in Councilman charged the defendant ISP with violating the Federal Wiretap Act by systematically intercepting, copying, and then reading its customers' incoming emails to learn about its competitors and gain a commercial advantage. This is precisely the type of behavior that Congress wanted to prohibit when it updated the Wiretap Act in 1986, as part of the Electronic Communications Privacy Act (ECPA), to prohibit unauthorized interceptions of electronic communications. Congress's goal was to ensure that Americans enjoyed the same amount of privacy in their online communications as they did in the offline world. Just as eavesdroppers were not allowed to tap phones or plant ''bugs'' in order to listen in on our private conversations, we wanted to ensure that unauthorized eyes were not peering indiscriminately into our electronic communications.

ECPA was a careful, bipartisan and long-planned effort to protect electronic communications in two forms—from real-time monitoring or interception as they were being delivered, and from searches when they were stored in record systems. We recognized these as different functions and set rules for each based on the relevant privacy expectations and threats to privacy implicated by the different forms of surveillance.

The Councilman decision turned this distinction on its head. Functionally, the ISP in this case was intercepting emails as they were being delivered, yet the majority ruled that the relevant rules were those pertaining to stored communications, which do not apply to ISPs. The majority rejected the Government's argument that an

intercept occurs—and the Wiretap Act applies—when an email is acquired contemporaneously with its transmission, regardless of whether the transmission may have been in electronic storage for milliseconds at the time of the acquisition. As the dissenting judge found, the Government's interpretation of the Wiretap Act is consistent with Congressional intent and with the realities of electronic communication systems. I agree, and urge the Justice Department to continue to press this position in the courts. The Department has been a powerful proponent of privacy rights in this case, and I commend its efforts.

I also will be taking a close look at possible changes to the law to ensure that there is no room to skirt the wiretap provisions and engage in the type of privacy violation at issue in the Councilman case. We have an obligation to ensure that our laws keep up with technology, and it may be that advances in communications warrant change. It is imperative that we continue to safeguard privacy adequately in our modern information age.

In a world where Americans are already inundated with targeted mass marketing and mailings, the Councilman decision opens the door to even more invasive activity. With this kind of precedent, ISPs need not offer free services in exchange for reduced online privacy. They could simply snoop in secret, and their unsuspecting customers would never know.

The Councilman decision also opens the door to Government over-reaching. For practical reasons, surveillance devices are often installed at the point of millisecond-long temporary storage prior to an e-mail's arrival at its final destination. To date, law enforcement agencies have treated this as what it is—an interception—and have sought appropriate wiretap approval. But this decision allows law enforcement agents to potentially skip the rigors of the wiretap laws, and perhaps could unleash unrestrained use of search programs like Carnivore. This outcome belies the realities of electronic communications in today's society, undercuts Congress' intent, and is inconsistent with the current approach to such communications in law enforcement practice.

The Councilman decision creates an instant and enormous gap in privacy protection for email communications, and we need to address it swiftly and responsibly. I urge my colleagues to make this a top priority as we finish up the session. I ask unanimous consent to have printed in the RECORD four recent editorials and articles on this issue.

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

[From the Washington Post, July 2, 2004]

DERAIL E-MAIL SNOOPING

Imagine that your friendly local mail carrier, before delivering a letter for you, decides to steam it open and read its contents. An outrageous and illegal infringement on your privacy, obviously. But a Federal appeals court in Boston has just permitted an Internet service provider to engage in exactly this kind of snooping when the message is sent in cyberspace rather than by snail mail. This ruling is an unnecessarily cramped parsing of a law that Congress meant to guard, not eviscerate, the privacy of communications. The Justice Department, whose prosecution of the ISP executive was thrown out by the appeals court, should seek a review of the ruling. If that doesn't work—if the Federal wiretapping law has been outpaced by the technology it was supposed to regulate—Congress should quickly step in to fix the glitch.

The wiretapping law makes it a crime to intentionally intercept ''any wire, oral, or electronic communication.'' This language dates to 1986, when e-mail was at an embryonic stage but Congress, in an effort to account for and anticipate that and other technological changes, enacted the Electronic Communications Privacy Act.

The appeals court, however, ruled that opening and reading e-mails isn't covered by the wiretapping law because the messages weren't actually intercepted, as the law defines that term, but were, rather, in ''electronic storage'' and therefore covered by another, looser law. That finding stems from the peculiar nature of e-mail transmission, in which messages are briefly stored as they're transmitted from computer to computer. As the court itself acknowledged, that would leave little privacy for e-mail: ''It may well be that the protections of the Wiretap Act have been eviscerated as technology advances.''

In practcal terms, the implications of the ruling are perhaps more troubling for the restraints it lifts on law enforcement than for the theoretical leeway it gives service providers to copy and read e-mails. The facts of the case were unusual: A small online company that sold out-of-print books and also provided free e-mail service wanted to peek at Amazon.com's sales strategy and copied all of Amazon's messages to the smaller company's customers. Mainstream ISPs have policies that eschew such spying, and the customer backlash that would ensure if they engaged in similar practices would probably deter them from doing so. But the ruling highlights the need for stringent privacy policies in which customers give clear—and informed—consent.

Of more concern, the case could make it far easier for law enforcement agents to engage in real-time monitoring of e-mail and similar traffic, like instant messaging, without complying with the strict rules applied to wiretaps. Under this reading of the law, agents would still need to show probable cause to obtain search warrants from a judge. But they wouldn't have to hew to the more exacting requirements of the wiretap law.

E-mail has become too ubiquitous, too central a facet of modern life, for this ruling to stand.

[From the New York Times, July 2, 2004]

INTERCEPTING E-MAIL

When you click on ''send'' to deliver that e-mail note to your lover, mother or boss, you realize that you are not communicating directly with that person. As you well know, you have stored the e-mail on the computer of your Internet service provider, which, as you also know, may read, copy and use the note for its own purposes before sending it on.

What, you didn't know all this? Sounds ludicrous? We would have thought so, too, but a Federal appeals court recently ruled that companies providing e-mail services could read clients' e-mail notes and use them as they wish. Part of its rationale was that none of this would shock you because you have never expected much online privacy.

Count us among the shocked. The decision, on a 2-to-1 vote by a panel of the United States Court of Appeals for the First Circuit in Massachusetts, sets up a frightening precedent, one that must be reversed by the courts, if not the Congress. It's true that people are aware of some limits on online privacy, particularly in the workplace. But the notion that a company like America Online, essentially a common carrier, has the right to read private e-mail is ludicrous.

All major I.S.P.s, including AOL, say they have no interest in doing that and have privacy policies against it. The case before the First Circuit involved a small online bookseller, no longer in business, that also provided e-mail service. To learn about the competition, the company copied and reviewed all e-mail sent from Amazon.com to its e-mail users. One of its executives was indicted on an illegal-wiretapping charge.

Both the trial and appeals courts ruled that the Federal wiretap law, which makes it a crime to intercept any ''wire, oral or electronic communication,'' did not apply because there had been no actual interception. Technically speaking, the judges held, the bookseller had simply copied e-mail notes stored on its servers, and different laws apply to the protection of stored communications.

These laws were drafted before e-mail emerged as a form of mass communication, so there is some ambiguity in how to apply them. But as the dissenting judge on the appellate panel noted, his two colleagues interpreted the wiretap statute far too narrowly. What's more, their analysis was predicated on the bizarre notion that our e-mail notes are not in transit once we send them, but in storage with an intermediary. The same logic would suggest that the postal service can read your letters while they are in ''storage.''

Americans' right to privacy will be seriously eroded if e-mail is not protected by wiretap laws. The implications of this erosion extend beyond the commercial realm. The government will also find it easier to read your e-mail if it does not have to get a wiretap order to do so. Congress ought to update the law to make it clear that e-mail is entitled to the same protection as a phone call.

COURT CREATES SNOOPERS' HEAVEN

(By Kim Zetter)

It was a little court case, but its impact on e-mail users could be huge.

Last week a Federal appeals court in Massachusetts ruled that an e-mail provider did not break the law when he copied and read e-mail messages sent to customers through his server.

Upholding a lower-court decision that the provider did not violate the Wiretap Act, the 1st U.S. Circuit Court of Appeals set a precedent for e-mail service providers to legally read e-mail that passes through a network.

The court ruled (PDF) that because the provider copied and read the mail after it was in the company's computer system, the provider did not intercept the mail in transit and, therefore, did not violate the Wiretap Act.

It's a decision that could have far-reaching effects on the privacy of digital communications, including stored voicemail messages.

In 1998, Bradford C. Councilman was the vice president of Interloc, a company selling rare and out-of-print books that offered book-dealer customers e-mail accounts

through its Web site. Unknown to those customers, Councilman had engineers write and install code on the company network that would copy any e-mail sent to customers from Amazon.com, a competitor in the rare-books field.

Although Councilman did not prevent customers from receiving their e-mail, he read thousands of copied messages to discover what books customers were seeking and gain a commercial advantage over Amazon. Interloc was later bought by Alibris, which was unaware that Councilman had installed the code on the system.

Councilman wasn't caught because customers complained about his actions; a tip about another, unrelated issue led authorities to discover what he had done.

But just what had Councilman done that was so bad?

Everyone knows that e-mail is an insecure form of communication. Like a postcard, unencrypted correspondence sent over the Internet is open to snooping by anyone.

Additionally, companies have the right to read their employees' e-mail, since the companies own the computer systems through which the correspondence passes, and employees send the mail on company time. And ISPs scan e-mail for viruses and spam all the time, before delivering the mail to the provider's customers.

But there is an expectation that service providers will access communications only with permission from customers, or when they need to do so to maintain their network. In fact, the Wiretap Act states that a provider shall not ''intercept, disclose, or use'' communication passing through its network ''except for mechanical or service quality control checks.''

In April, Google launched an e-mail program called Gmail that gives customers 1 GB of e-mail storage in exchange for letting Google's computers scan the content of incoming e-mails to seed them with related text ads. Gmail customers agree to let a computer read their e-mail.

In contrast, Councilman personally read customers' messages to undermine his competitors' business. He did no without customers' permission and with the knowledge that if his customers found out, his company would likely lose their business.

And yet the court found him innocent of violating the specific law under which authorities charged him.

The court ruled that because the mail was already on Councilman's computer network when he accessed it, he didn't intercept it in transit and therefore was not guilty under the Wiretap Act. The court said the mail was in storage at that point and, therefore, was governed under the Stored Communications Act.

In a similar case in 1991, the U.S. Secret Service seized three computers belonging to a company called Steve Jackson Games. The company, in addition to producing fantasy books and games, hosted an online bulletin board for gamers to communicate with one another. An employee of the company was under suspicion for activities conducted outside work, but the Secret Service confiscated his employer's computers as well. The Secret Service accessed, read and deleted 162 e-mail messages that were stored on the computers used for the bulletin board.

In a suit filed by the game company against the Secret Service, a federal district court found that while the Secret Service agents did not intercept the e-mail, and thus violate the Wiretap Act, they did violate the Stored Communications Act.

Pete Kennedy, the lawyer from the Texas-based firm that litigated the case, called the decision ''a solid first step toward recognizing that computer communications should be as well-protected as telephone communications.''

The Stored Communications Act, along with the Wiretap Act, is part of the Electronic Communications Privacy Act, which protects electronic, oral and wire communications.

But because Councilman was charged under the Wiretap Act and not the Stored Communications Act, the court had to rule in his favor. But even if prosecutors had wanted to charge him under the Stored Communications Act, they could not have done so, since service providers are exempted under the Act.

What this means is that before the Councilman case, ISPs that read their customers' mail without permission could only have been prosecuted under the Wiretap Act. But now the Councilman case eliminates that possibility as well.

The problem with interpreting e-mail on an ISP's server as stored communication is that it opens the possibility for e-mail even outside the ISP to be viewed as stored e-mail.

At many points during its path from sender to recipient, e-mail passes through a number of computer systems and routers that temporarily store it in RAM while the system determines the next point to send it on the delivery route. Under the court's definition, an ISP could access, copy and read the mail at any of these points. Anyone who is not exempt under the Stored Communications Act, however, could still be charged under that law, though penalties for violating this law are less severe than penalties for violating the Wiretap Act.

Last week's ruling means that e-mail has fewer protections than phone conversations and postal mail. Granting e-mail providers the ability to read e-mail is equivalent to granting postal workers the right to open and read any mail while it's at a post office for sorting, but not while it's in transit between post offices or being hand-delivered to a recipient's home or business.

The ruling also has repercussions for voicemail messages, as long as certain provisions in the Patriot Act remain law.

Before the Patriot Act, the legal definition of wire communication included voicemail messages. This meant that authorities had to obtain a wiretap order to access voicemail messages or face charges of illegal interception under the Wiretap Act. Under the Patriot Act, however, the definition of wire communication *changed*. Voicemail messages are now considered stored communication, like e-mail. As a result, law enforcement authorities need only a search warrant to access voicemail messages, a much easier process than obtaining a wiretap order.

The provision in the Patriot Act that changed this is set to sunset in December 2005, but if the current administration has its way, the law will be renewed.

The changes in the Patriot Act, combined with the decision in the Councilman case, also mean that a phone company could now access voicemail messages without customers' permission and not be charged with intercepting the messages under the Wiretap Act. They also would not be charged under the Stored Communications Act, since they are exempt from this statute.

If all of this is hard to follow, it's just as confusing to the people who make their living interpreting the law.

''This is one of the most complex and convoluted areas of the law that you will run across,'' said Lee Tien, senior staff attorney for the Electronic Frontier Foundation. ''The statutes themselves are not models of clarity. Even for the judges it's complicated, and then, on top of the statutes, you add the changing technology.''

In the end, in the absence of laws to preserve privacy, the best solution for e-mail users to protect their privacy is to use encryption. But until encryption for voicemail messages becomes common, you'll have to settle for talking in tongues.

[From the New York Times, July 6, 2004]

YOU'VE GOT MAIL (AND COURT SAYS OTHERS CAN READ IT)

(By SAUL HANSELL)

When everything is working right, an e-mail message appears to zip instantenously from the sender to the recipient's inbox. But in reality, most messages make several momentary stops as they are processed by various computers en route to their destination.

Those short stops may make no difference to the users, but they make an enormous difference to the privacy that e-mail is accorded under federal law.

Last week a Federal appeals court in Boston ruled that federal wiretap laws do not apply to e-mail messages if they are stored, even for a millisecond, on the computers of the Internet providers that process them—meaning that it can be legal for the government or others to read such messages without a court order.

The ruling was a surprise to many people, because in 1986 Congress specifically amended the wiretap laws to incorporate new technologies like e-mail. Some argue that the ruling's implications could affect emerging applications like Internet-based phone calls and Gmail Google's new e-mail service, which shows advertising based on the content of a subscriber's e-mail messages.

''The court has eviscerated the protections that Congress established back in the 1980's,'' said Marc Rotenberg, the executive director of the Electronic Privacy Information Center, a civil liberties group.

But other experts argue that the Boston case will have little practical effect. The outcry, said Stuart Baker, a privacy lawyer with Steptoe & Johnson in Washington, is ''much ado about nothing.''

Mr. Baker pointed out that even under the broadest interpretation of the law, Congress made it easier for prosecutors and lawyers in civil cases to read other people's e-mail messages than to listen to their phone calls. The wiretap law—which requires prosecutors to prove their need for a wiretap and forbids civil litigants from ever using them—applies to e-mail messages only when they are in transit.

But in a 1986 law, Congress created a second category, called stored communication, for messages that had been delivered to recipients' inboxes but not yet read. That law, the Stored Communications Act, grants significant protection to e-mail messages, but does not go as far as the wiretap law: it lets prosecutors have access to stored messages with a search warrant, while imposing stricter requirements on parties in civil suits.

Interestingly, messages that have been read but remain on the Internet provider's computer system have very little protection. Prosecutors can typically gain access to an opened e-mail message with a simple subpoena rather than a search warrant. Similarly, lawyers in civil cases, including divorces, can subpoena opened e-mail messages.

The case in Boston involved an online bookseller, now called Alibris. In 1998, the company offered e-mail accounts to book dealers and, hoping to gain market advantage, secretly copied messages they received from Amazon.com. In 1999, Alibris and one employee pleaded guilty to criminal wiretapping charges.

But a supervisor, Bradford C. Councilman, fought the charges, saying he did not know

about the scheme. He also moved to have the case dismissed on the ground that the wiretapping law did not apply. He argued that because the messages had been on the hard drive of Alibris's computer while they were being processed for delivery, they counted as stored communication. The wiretap law bans a company from monitoring the communications of its customers, except in a few cases. But it does not ban a company from reading customers' stored communications.

''Congress recognized that any time you store communication, there is an inherent loss of privacy,'' said Mr. Councilman's lawyer, Andrew Good of Good & Cormier in Boston.

In 2003, a Federal district court in Boston agreed with Mr. Councilman's interpretation of the wiretap law and dismissed the case. Last week, the First Circuit Court of Appeals, in a 2-to-1 decision, affirmed that decision.

Because most major Internet providers have explicit policies against reading their customers' e-mail messages, the ruling would seem to have little effect on most people.

But this year Google is testing a service called Gmail, which electronically scans the content of the e-mail messages its customers receive and then displays related ads. Privacy groups have argued that the service is intrusive, and some have claimed it violates wiretap laws. The Councilman decision, if it stands, could undercut that argument.

Federal prosecutors, who often argue that wiretap restrictions do not apply in government investigations, were in the somewhat surprising position of arguing that those same laws should apply to Mr. Councilman's conduct. A spokesman for the United States attorney's office in Boston said the department had not decided whether to appeal.

Mr. Baker said that another Federal appeals court ruling, in San Francisco, is already making it hard for prosecutors to retrieve e-mail that has been read and remains on an Internet provider's system.

In that case, Theofel v. Farey-Jones, a small Internet provider responded to a subpoena by giving a lawyer copies of 339 e-mail messages received by two of its customers.

The customers claimed the subpoena was so broad it violated the wiretap and stored communication laws. A district court agreed the subpoenas were too broad, but ruled they were within the law. The plaintiffs appealed, and the Justice Department filed a friend of the court brief arguing that the Stored Communications Act should not apply.

In February, the appeals court ruled that e-mail stored on the computer server of an Internet provider is indeed covered by the Stored Communications Act, even after it has been read. The court noted that the act refers both to messages before they are delivered and to backup copies kept by the Internet provider. ''An obvious purpose for storing a message on an I.S.P.'s server after delivery,'' the court wrote, ''is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user's own computer.''

Calling e-mail ''stored communication'' does not necessarily reduce privacy protections for most e-mail users. While the Councilman ruling would limit the applicability of wiretap laws to e-mail, it appears to apply to a very small number of potential cases. The Theofel decision, by contrast, by defining more e-mail as ''stored communications,'' is restricting access to e-mail in a wide range of cases in the Ninth Circuit, and could have a far greater effect on privacy of courts in the rest of the country follow that ruling.

ADDITIONAL STATEMENTS

IBM AND THE RESEARCH TRIANGLE PARK

• Mrs. DOLE. Mr. President, when IBM joined the Research Triangle Park as its first major tenant in 1965, this company helped establish the Research Triangle Park as the premier technological, biotech, and economic development powerhouse for North Carolina.

Today I thank and congratulate IBM for its decades of support and investment in the Research Triangle Park and the surrounding communities in North Carolina. As the largest employer in the Triangle Park, IBM is an excellent example of corporate citizenship that provides dependable, high-paying jobs in both the area and worldwide.

With over 13,000 jobs in the Triangle Park alone, the largest concentration of IBM jobs worldwide, IBM uses the graduates and resources from the State's extensive college and university system. IBM invests in our State by helping to keep North Carolina talent at home.

Please join me and other North Carolina leaders in congatulating IBM on its commitment to build a better company for our region and wishing IBM and the Research Triangle Park ongoing success as they broaden their partnership with the people of my home State.•

MESSAGE FROM THE HOUSE

At 3:02 p.m., a message from the House of Representatives, delivered by Mr. Hays, one of its reading clerks, announced that the House has passed the following bill, in which it requests the concurrence of the Senate:

H.R. 4754. An act making appropriations for the Department of Commerce, Justice, and State, the Judiciary, and related agencies for the fiscal year ending September 30, 2005, and for other purposes.

MEASURES REFERRED

The following bill was read the first and the second times by unanimous consent, and referred as indicated:

H.R. 4754. An act making appropriations for the Departments of Commerce, Justice, and State, the Judiciary, and related agencies for the fiscal year ending September 30, 2005, and for other purposes; to the Committee on Appropriations.

MEASURES PLACED ON THE CALENDAR

The following bills were read the second time, and placed on the calendar:

S. 2629. A bill to amend the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 to eliminate the coverage gap, to eliminate HMO subsidies, to repeal health savings accounts, and for other purposes.

S. 2630. A bill to amend title 5, United States Code to establish a national health program administered by the Office of Personnel Management to offer Federal employee health benefits plans to individuals who are not Federal employee, and for other purposes.

S. 2631. A bill to require the Federal Trade Commission to monitor and investigate gasoline prices under certain circumstances.

S. 2632. A bill to establish a first responder and terrorism preparedness grant information hotline, and for other purposes.

S. 2633. A bill to amend the Federal Power Act to provide refunds for unjust and unreasonable charges on electric energy in the State of California.

REPORTS OF COMMITTEES

The following reports of committees were submitted:

By Mr. ROBERTS, from the Select Committee on Intelligence:

Special Report entitled ''Report of the Select Committee on Intelligence on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq'' (Rept. No. 108–301). Additional views filed.

INTRODUCTION OF BILLS AND JOINT RESOLUTIONS

The following bills and joint resolutions were introduced, read the first and second times by unanimous consent, and referred to as indicated:

By Mr. LEAHY:

S. 2636. A bill to criminalize Internet scams involving fraudulently obtaining personal information, commonly known as phishing; to the Committee on the Judiciary.

By Mr. GRAHAM of South Carolina:

S. 2637. A bill to amend the National Labor Relations Act to ensure the right of employees to a secret-ballot election conducted by the National Labor Relations Board; to the Committee on Health, Education. Labor, and Pensions.

SUBMISSION OF CONCURRENT AND SENATE RESOLUTIONS

The following concurrent resolutions and Senate resolutions were read, and referred (or acted upon), as indicated:

By Mr. HARKIN (for himself, Mr. COCHRAN, Mr. ROBERTS, Mr. DASCHLE, Mr. CRAPO, Mr. FITZGERALD, Mr. CONRAD, Mr. COLEMAN, Mr. LEAHY, Mrs. LINCOLN, Mr. KOHL, Mrs. CLINTON, Mr. JOHNSON, Mr. DORGAN, Mr. LUGAR, and Mr. DAYTON):

Res. 402. A resolution expressing the sense of the Senate with respect to the 50th anniversary of the food aid programs established under the Agricultural Trade Development and Assistance Act of 1954; considered and agreed to.

By Ms. SNOWE (for herself, Mr. MCCAIN, Mr. HOLLINGS, Mr. DODD, Mr. KENNEDY, Mr. CHAFEE, Mrs. BOXER, Mrs. COLLINS, Mr. FITZGERALD, Mr. REED, Mr. CORZINE, Mr. JEFFORDS, Mr. WYDEN, Mr. BIDEN, and Mr. LIEBERMAN):

S. Con. Res. 122. A concurrent resolution expressing the sense of the Congress regarding the policy of the United States at the