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

56th Annual Meeting of the International Whaling Commission; to the Committee on Foreign Relations.

ADDITIONAL COSPONSORS

S. 1411

At the request of Mr. KERRY, the names of the Senator from Vermont (Mr. LEAHY) and the Senator from Rhode Island (Mr. REED) were added as cosponsors of S. 1411, a bill to establish a National Housing Trust Fund in the Treasury of the United States to provide for the development of decent, safe, and affordable housing for low-income families, and for other purposes.

S. 1890

At the request of Mr. ENZI, the name of the Senator from Maryland (Ms. MIKULSKI) was added as a cosponsor of S. 1890, a bill to require the mandatory expensing of stock options granted to executive officers, and for other purposes.

S. 2313

At the request of Mr. GRAHAM of Florida, the name of the Senator from Vermont (Mr. LEAHY) was added as a cosponsor of S. 2313, a bill to amend the Help America Vote Act of 2002 to require a voter-verified permanent record or hardcopy under title III of such Act, and for other purposes.

S. 2338

At the request of Mr. BOND, the mane of the Senator from Indiana (Mr. BAYH) was added as a cosponsor of S. 2338, a bill to amend the Public Health Service Act to provide for arthritis research and public health, and for other purposes.

S. 2340

At the request of Mr. BINGAMAN, the name of the Senator from Hawaii (Mr. AKAKA) was added as a cosponsor of S. 2340, a bill to reauthorize title II of the Higher Education Act of 1965.

S. 2412

At the request of Mr. BOND, the name of the Senator from Illinois (Mr. DURBIN) was added as a cosponsor of S. 2412, to expand Parents as Teachers programs and other programs of early childhood home visitation, and for other purposes.

S. 2526

At the request of Mr. BOND, the name of the Senator from Virginia (Mr. WARNER) was added as a cosponsor of S. 2526, a bill to reauthorize the Children's Hospitals Graduate Medical Education Program.

S. 2568

At the request of Mr. BIDEN, the names of the Senator from Delaware (Mr. CARPER) and the Senator from Illinois (Mr. FITZGERALD) were added as cosponsors of S. 2568, a bill to require the Secretary of the Treasury to mint coins in commemoration of the tercentenary of the birth of Benjamin Franklin, and for other purposes.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

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.

Mr. LEAHY. Mr. President, today I am introducing a bill, the Anti-Phishing Act of 2004, that targets a large and growing class of crime that is spreading across the Internet.

Phishing is a rapidly growing class of identity theft scams on the Internet that is causing both short-term losses and long-term economic damage.

In the short-term, these scams defraud individuals and financial institutions. Some estimates place the cost of phishing at over two billion dollars just over the last 12 months.

In the long run, phishing undermines the Internet itself. By making consumers uncertain about the integrity of the Internet's complex addressing system, phishing threatens to make us all less likely to use the Internet for secure transactions. If you can't trust where you are on the web, you are less likely to use it for commerce and communications.

Phishing is spelled ''P-H-I-S-H-I-N-G.'' Those well-versed in popular culture may guess that it was named after the phenomenally popular Vermont band, Phish. But phishing over the Internet was in fact named from the sport of fishing, as an analogy for its technique of luring Internet prey with convincing email bait. The ''F'' is replaced by a ''P-H'' in keeping with a computer hacker tradition.

Phishing attacks usually start with emails that are, in Internet jargon, ''spoofed.'' That is, they are made to appear to be coming from some trusted financial institution or commercial entity. The spoofed email usually asks the victim to go to a website to confirm or renew private account information. These emails offer a link that appears to take the victim to the website of the trusted institution. In fact the link takes the victim to a sham website that is visually identical to that of the trusted institution, but is in fact run by the criminal. When the victim takes the bait and sends their account information, the criminal uses it—sometimes within minutes—to transfer the victim's funds or to make purchases. Phishers are the new con artists of cyberspace.

To give an idea of how easy it is to be fooled, we have reproduced some recent phishing charts, with the help of the Anti-Phishing Working Group. These are just two examples of a problem that affects countless companies. The website on the right is an actual website of MBNA, a well-established financial institution and credit card issuer. On the left is a recently discovered phishing site that mimicked the MBNA site.

As you can see, the two websites are practically identical. Both have the MBNA logo, and both have the same graphics, in the same layout. But if you end up going to the website on the left, when you enter your account information, you are giving it to an identity thief.

As another example, the next two websites both appear to be from eBay. Again, the one on the right is from the genuine website. The one on the left is a fake website that is controlled by a phisher. As you can see, if you end up at the website on the left, it would be next to impossible to know that you are not at the real eBay website. Informed Internet users can avoid this problem if they simply use their web browser to go to the website, instead of using a link sent to them in an email, but far too many people do not do this.

This is a growing problem. Phishing is on the rise. In recent months there has been an explosion of these types of attacks. As you can see from the next chart, these attacks are growing at an alarming rate. Roughly one million Americans already have been victims of phishing attacks.

And phishing attacks are increasingly sophisticated. Early phishing attacks were by novices, but there is evidence now that some attacks are backed by organized crime. And some attacks these days include spyware, which is software that is secretly installed on the victim's computer, which waits to capture account information when the victim even goes to legitimate websites.

Phishers also have become more sophisticated in how they cast their huge volumes of email bait on the Internet waters. Security experts recently discovered that vast networks of home computers are being hijacked by hackers using viruses, and then they are rented to phishers—all without the knowledge of the owners of these home computers.

Some phishers can be prosecuted under wire fraud or identity theft statutes, but often these prosecutions take place only after someone has been defrauded. Moreover, the mere threat of phishing attacks undermines everyone's confidence in the Internet. When people cannot trust that websites are what they appear to be, they will not use the Internet for their secure transactions. So traditional wire fraud and identity theft statutes are not sufficient to respond to phishing.

The Anti-Phishing Act of 2004 protects the integrity of the Internet in two ways. First, it criminalizes the bait. It makes it illegal to knowingly send out spoofed email that links to sham websites, with the intention of committing a crime. Second, it criminalizes the sham websites that are the true scene of the crime.

It makes it illegal to knowingly create or procure a website that purports to be a legitimate online business, with the intent of collecting information for some criminal purpose.

There are important First Amendment concerns to be protected. The Anti-Phishing Act protects parodies and political speech from being prosecuted as Phishing.