

coaches returned to campus late Tuesday, they joined students and fans in an exuberant pep rally to celebrate their achievements. On Wednesday, a parade was held in their honor, culminating on the steps of City Hall. Mayor Deedee Corradini and the city council presented the team with the key to the city.

I want to congratulate the entire Ute team: The coaching staff, including Coach Majerus and his great assistant coaches Donny Daniels, Jeff Judkins, and Brock Brundhorst. And, my hat is off to the players: Michael Doleac, Drew Hansen, Andre Miller, Hanno Mottola, Alex Jensen, Jordie McTavish, David Jackson, Nate Althoff, Greg Barratt, Jon Carlisle, Trace Caton, Britton Johnsen, and Adam Sharp. Thanks for giving us so much to cheer about.

THE VERY BAD DEBT BOXSCORE

MR. HELMS. Mr. President, at the close of business yesterday, Wednesday, April 1, 1998, the federal debt stood at \$5,540,550,647,696.94 (Five trillion, five hundred forty billion, five hundred fifty million, six hundred forty-seven thousand, six hundred ninety-six dollars and ninety-four cents).

One year ago, April 1, 1997, the federal debt stood at \$5,375,122,000,000 (Five trillion, three hundred seventy-five billion, one hundred twenty-two million).

Five years ago, April 1, 1993, the federal debt stood at \$4,225,874,000,000 (Four trillion, two hundred twenty-five billion, eight hundred seventy-four million).

Ten years ago, April 1, 1988, the federal debt stood at \$2,509,151,000,000 (Two trillion, five hundred nine billion, one hundred fifty-one million).

Fifteen years ago, April 1, 1983, the federal debt stood at \$1,237,481,000,000 (One trillion, two hundred thirty-seven billion, four hundred eighty-one million) which reflects a debt increase of more than \$4 trillion—\$4,303,069,647,696.94 (Four trillion, three hundred three billion, sixty-nine million, six hundred forty-seven thousand, six hundred ninety-six dollars and ninety-four cents) during the past 15 years.

WAKE-UP CALL ON ENCRYPTION

Mr. LEAHY. Mr. President, it is time the Administration woke up to the critical need for a common sense encryption policy in this country. I have been sounding the alarm bells about this issue for several years now, and have introduced encryption legislation, with Senator BURNS and others, in the last Congress and again in this one, to balance the important privacy, economic, national security and law enforcement interests at stake. The volume of those alarm bells should be raised to emergency sirens.

Because of the sorry state of our current encryption policies and, specifically, our export controls on encryption, we are seeing increasing

numbers of high-tech jobs and expertise driven overseas. Recently, a large computer security company, Network Associates, announced that it will make strong encryption software developed in the United States available through a Swiss company. Encryption technology invented with American ingenuity, will now be manufactured and distributed in Europe, and imported back into this country. All those good, high-tech jobs associated with Network Associates' encryption product are now in Europe, not in Silicon Valley, not in Vermont, not in any American town, because of our outdated export controls on encryption.

Network Associates is not the first American company to face the dilemma of how to supply its customers, both domestic and foreign, with the strong encryption they are demanding and also comply with current export restrictions on encryption. Other companies, including Sun Microsystems, are cooperating with foreign companies to manufacture and distribute overseas strong encryption software originally developed here at home.

I have said before, and repeat here again, that driving encryption expertise overseas is a threat to our national security, driving high-tech jobs overseas is a threat to our economic security, and stifling the widespread, integrated use of strong encryption is a threat to our public safety. That is why I have called in legislation for relaxation of our export controls on encryption.

Over the past month, we have learned of two serious breaches of computer security that threaten our critical infrastructures. Both incidents were apparently caused by teenagers using their home computers to trespass into the computer systems of the Department of Defense, the telephone network, the computer system for an airport control tower, and into the computer database of a pharmacy containing private medical records. One of these adolescent explorations in cyberspace disrupted telephone service in Rutland, Massachusetts and shut down the control tower at a small airport.

The conduct of these teenagers is now the subject of criminal investigation, due in large part to the great strides we have made in updating our criminal laws to protect critical computer networks and the information on those networks. I am proud to have sponsored these computer crime laws in the last two Congresses. But targeting cybercrime with criminal laws and tough enforcement is only part of the solution. While criminal penalties may deter some computer criminals, these laws usually come into play too late, after the crime has been committed and the injury inflicted.

We should keep in mind the adage that "the best defense is a good offense." Americans and American firms must be encouraged to take preventive measures to protect their computer information and systems. A recent report

by the FBI and Computer Security Institute released shows that the number of computer crimes and information security breaches continues to rise, resulting in over \$136 million in losses in the last year alone.

The lesson of the recent computer breaches by the teenagers is that all the physical barriers we might put in place can be circumvented using the wires that run into every building to support the computers and computer networks that are the mainstay of how we do business. A well-focused cyber-attack on the computer networks that support telecommunications, transportation, water supply, banking, electrical power and other critical infrastructure systems could wreak havoc on our national economy or even jeopardize our national defense or public safety.

We have been aware of the vulnerabilities of our computer networks for almost a decade. In 1988, I chaired hearings of the Subcommittee on Technology and the Law on the risks of high-tech terrorism. It became clear to me that merely "hardening" our physical space from potential attack is not enough. We must also "harden" our critical infrastructures to ensure our security and our safety.

That is where encryption technology comes in. Encryption is one important tool in our arsenal to protect the security of our computer information and networks. Both former Senator Sam Nunn and former Deputy Attorney General Jamie Gorelick, who serve as co-chairs of the Advisory Committee to the President's Commission on Critical Infrastructure Protection, testified at a hearing last month that "encryption is essential for infrastructure protection."

Yet, even computer security experts agree that U.S. encryption policy has "acted as a deterrent to better security." As long ago as 1988, at my High-Tech Terrorism hearing, Jim Woolsey, who later became the director of the Central Intelligence Agency, testified about the need to do a better job of using encryption to protect our computer networks.

I have long advocated the use of strong encryption by individuals, government agencies and private companies to protect their valuable computer information. Indeed, a major thrust of the encryption legislation I have introduced is to encourage—and not stand in the way of—the widespread use of encryption. This would be a plus for both our law enforcement and national security agencies.

Unfortunately, we still have a long way to go to update our country's encryption policy to reflect that this technology is a significant crime and terrorism prevention tool. I am particularly concerned by the testimony of former Senator Sam Nunn last month that the "continuing federal government-private sector deadlock over encryption and export policies"

may pose an obstacle to the cooperation needed to protect our country's critical infrastructures.

At the heart of the encryption debate is the power this technology gives computer users to choose who may access their communications and stored records, to the exclusion of all others. For the same reason that encryption is a powerful privacy enhancing tool, it also poses challenges for law enforcement. Law enforcement agencies want access even when we do not choose to give it.

The FBI has made clear that law enforcement wants immediate access to the plaintext of encrypted communications and stored data, and, absent industry capitulation, will seek legislation to this effect. Indeed, while much of this debate has focused on relaxation of export controls, the FBI has upped the ante. Recognizing that the encryption genie is out of the bottle, the FBI has indicated it may seek import restrictions and domestic controls on encryption.

The FBI has told me in response to written questions that: "[I]f the current voluntary efforts are not successful... it is the responsibility of the FBI... to seek alternative approaches to alleviate the problems caused by encryption. This would include legislative remedies which effectively address law enforcement concerns regarding the import of robust encryption products, as well as encryption products manufactured for use in the U.S."

The Administration has not disavowed this position. In a recent letter to the Minority Leader, the Administration expressed a preference for a "good faith dialogue" and "cooperative solutions" over "seeking to legislate domestic controls," but has clearly not ruled out the latter approach.

Even as our law enforcement and intelligence agencies try to slow down the widespread use of strong encryption, technology continues to move forward. Ironically, foot-dragging by the Administration on export controls and threats by the FBI to call for domestic encryption controls, have only motivated computer scientists to find alternative means to protect the privacy of online communications that may, in fact, pose more of a challenge to law enforcement.

Indeed, the terms of the current encryption debate may soon become moot. The New York Times reported a few weeks ago that Ronald Rivest of MIT has developed a new method for protecting the confidentiality of electronic messages that does not use encryption. Instead, this method breaks a message into separate packets, each marked with a special authentication header, and then "hides" those packets in a stream of other packets. Eavesdroppers would not know which packets were the "wheat" part of the message and which packets were the irrelevant "chafe". As Mr. Rivest noted in his article announcing this technique, "attempts by law en-

forcement to regulate confidentiality by regulating encryption must fail, as confidentiality can be obtained effectively without encryption and even sometimes without the desire for confidentiality by the two communicants."

I know that others of my colleagues, including Senators BURNS, DASCHLE, ASHCROFT, KERREY, and MCCAIN, share my appreciation of importance of this encryption issue for our economy, our national security and our privacy. This is not a partisan issue. This is not a black-and-white issue of being either for law enforcement and national security or for Internet freedom. Characterizing the debate in these simplistic terms is neither productive nor accurate.

Delays in resolving the encryption debate hurt most the very public safety and national security interests that are posed as obstacles to resolving this issue. I look forward to working with these colleagues on sensible solutions in legislation, which will not be subject to change at the whim of agency beauracrats.

Every American, not just those in the software and high-tech industries and not just those in law enforcement agencies, has a stake in the outcome of this debate. We have a legislative stalemate right now that needs to be resolved, and I plan to work closely with my colleagues on a solution in this congressional session.

I commend Senator ASHCROFT for holding an encryption hearing last month and providing a forum to discuss the important privacy and constitutional interests at stake in the encryption debate. How we resolve this debate today will have important repercussions for the exercise of our constitutional rights tomorrow. Do you agree with me that every American, not just those in the high-tech industries and not just those in law enforcement agencies, has a stake in the outcome of this debate?

Mr. ASHCROFT. Yes, I do. The testimony presented at the hearing made clear that how we resolve the law enforcement issues at the heart of the encryption debate may affect the exercise and protections of important First, Fourth and Fifth amendment rights. While we must ensure law enforcement the appropriate amount of access we cannot do so at the expense of important constitutional liberties. As I mentioned at the hearing, the FBI has argued that a system of mandatory access to private communications—or a system in which the federal government strongly "persuades" individuals to hand over their rights to the FBI—would make it easier for law enforcement to do its job. Of course it would, but it would also make things easier on law enforcement if we simply repealed the Fourth Amendment.

Mr. LEAHY. These constitutional issues are vital ones for Congress to consider. I understand that efforts are underway for industry stakeholders to

reach some accommodation with the Administration. I encourage constructive dialogue between the Administration and industry and, in fact, have been urging a dialogue between law enforcement and industry for over a year. But Congress will continue to exercise necessary oversight to ensure that the privacy and other constitutional rights of Americans are protected.

Mr. ASHCROFT. As the Chairman of the Judiciary Subcommittee on the Constitution, Federalism and Property Rights, you can be assured that the subcommittee will stand ready to provide oversight to ensure that no constitutional right of any American is compromised. Several very important rights were addressed by the witnesses during the hearing, and the constitutional concerns of law-abiding citizens must be respected. Importantly, in the ongoing dialogue between industry and federal law enforcement we must make sure that the interests of the citizens of the U.S. are represented and their constitutional rights respected. We must ensure that everyone in the negotiations—including the administration—views the constitutional rights of law abiding citizens as non-negotiable absolutes, not as bargaining chips.

Mr. LEAHY. I have been concerned about companies, such as Sun Microsystems and Network Associates, using foreign companies to manufacture and distribute strong encryption, which was developed in the United States but may not be exported under U.S. regulations. These instances are just the latest examples that delays in resolving the encryption debate is driving overseas cryptographic expertise and high-tech jobs, to the detriment of our economy and our national security. Do you share these concerns?

Mr. ASHCROFT. Yes, I certainly share those concerns. The impact to our national security is clear and under the current Administration policy the United States is sending some of our greatest talent and products to foreign shores, enabling foreign competitors, both to industry and to our national security, to gain a strong foothold. In just the past few weeks, Network Associates, our largest independent maker of computer security software, decided to allow its Dutch subsidiary to begin selling strong encryption that does not provide a back door for law enforcement surveillance. This move by Network Associates was necessitated by our current wrong-headed export provisions. We have to re-examine these policies. Simply put, strong encryption means a strong economy. Mandatory access, by contrast, means weaker encryption and a less secure, and therefore less valuable, network. This recent example of the export of a manufacturing enterprise and the accompanying intellectual capital is only one example of a bad policy weakening our economy.

Mr. LEAHY. In my view, encryption legislation should promote the following goals:

First, legislation should ensure the right of Americans to choose how to protect the privacy and security of their communications and information;

Second, legislation should bar a government-mandated key escrow encryption system;

Third, legislation should establish both procedures and standards for access by law enforcement to decryption keys or decryption assistance for both encrypted communications and stored electronic information and only permit such access upon court order authorization, with appropriate notice and other procedural safeguards;

Fourth, legislation should establish both procedures and standards for access by foreign governments and foreign law enforcement agencies to the plaintext of encrypted communications and stored electronic information of United States persons;

Fifth, legislation should modify the current export regime for encryption to promote the global competitiveness of American companies;

Sixth, legislation should not link the use of certificate authorities with key recovery agents or, in other words, link the use of encryption for confidentiality purposes with use of encryption for authenticity and integrity purposes;

Seventh, legislation should, consistent with these goals of promoting privacy and the global competitiveness of our high-tech industries, help our law enforcement agencies and national security agencies deal with the challenges posed by the use of encryption; and

Eighth, legislation should protect the security and privacy of information provided by Americans to the government by ensuring that encryption products used by the government interoperate with commercial encryption products.

Do you agree with these goals?

Mr. ASHCROFT. Yes, I agree with these goals and will look to these same items as a reference point for the drafting, introducing and passage of encryption reform legislation.

Mr. LEAHY. Would the Senator agree to work with me on encryption legislation that achieves these goals and that we could bring to the floor this Congress?

Mr. ASHCROFT. Yes. I believe it is critical for us to address this issue and soon. I also believe that we should work together to produce a piece of legislation that demonstrates our position on encryption policy.

EQUAL PAY DAY

Mr. LEAHY. Mr. President, tomorrow, April 3, 1998, is Equal Pay Day. This is the day by which women will have had to work all of 1997 and the first three months of 1998 to make what a man made in 1997 alone. We are not talking about jobs requiring different skills or abilities. We are talking about equal pay for equal work. This is not a glass ceiling, this is a glass wall. Women cannot break the

glass ceiling until the wall comes down and they are given the equal pay that they deserve.

Early in the next century, women—for the first time ever—will outnumber men in the United States workplace. In 1965, women held 35 percent of all jobs. That has grown to more than 45 percent today. And in a few years, women will make up a majority of the workforce.

Fortunately, there are more business and career opportunities for women today than there were thirty years ago. Unlike 1965, federal, state, and private sector programs now offer women many opportunities to choose their own futures. Working women also have opportunities to gain the knowledge and skills to achieve their own economic security.

But despite these gains, working women still face a unique challenge—achieving pay equity. The average woman earns 74 cents for every dollar that the average man earns. According to a study by the National Academy of Sciences, one-half of the pay gap is due to discrimination. This is unacceptable.

This discrimination is evident even in traditionally female professions such as nursing. For example, Marcelle, my wife, is a registered nurse. Female registered nurses make on average \$7,600 a year less than men. It is unacceptable when female nurses make only 80 percent of the wages of their male counterparts for the same work.

My home state of Vermont is a leader in providing pay equity. According to the Institute for Women's Policy Research, Vermont ranks third in providing equal pay. Even with this ranking, the average woman in Vermont still is making less than 76 cents for every dollar that the average man makes in Vermont. We must work in the Senate and in the workplace to close this gap.

I am pleased to join Senator DASCHLE in reintroducing the Paycheck Fairness Act. This legislation will help to address the problem of pay inequality by redressing past discrimination and increasing enforcement against future abuses.

Senator HARKIN is also a true leader on pay equity. I am an original cosponsor of his bill, the Fair Pay Act, which prohibits pay discrimination based on sex, race or national origin. These two pieces of legislation will help to provide women with what they deserve: equal pay for equal work.

I understand that these bills will not solve all of the problems of pay inequity, but they will close legal loopholes that allow employers to routinely underpay women. By closing these loopholes, we will help women achieve better economic security and provide them with more opportunities.

Women are being advanced in the workplace and the glass ceiling is slowly cracking. Last year, President Clinton appointed Madeline Albright as the first female Secretary of State, and I am proud that Vermont is also a leader

in advancing women in the workplace. The University of Vermont has a female president, Dr. Judith Ramaley, and Martha Rainville was recently elected Adjutant General of the Vermont National Guard—the first woman in the nation to hold this position. While women are advancing in the workplace, we need to ensure that they are receiving fair pay for their work.

I want to commend Senator DASCHLE and Senator HARKIN on their initiative in introducing the Paycheck Fairness Act and the Fair Pay Act. I also want to recognize and commend the hundreds of organizations around the country that will recognize tomorrow as Equal Pay Day.

POSITIVE SYSTEMS

Mr. BURNS. Mr. President, I stand today to recognize one of Montana's next generation jewels—Positive Systems in Whitefish, Montana. As a result of the dedication and commitment to their industry, Positive Systems has been recognized by the 1998 Governor's Excellence in Exporting Award Certificate of Appreciation.

Incorporated in 1991, Positive Systems provides a technical service in a rather unique and young industry. Dale Johnson, Cody Benkelman and Ron Behrendt designed a digital aerial photography service that will benefit many sectors of our economy. Positive Systems is the only business using such methods in the rapidly growing aerial mapping industry. These three men from different backgrounds combined their skills to launch this new enterprise.

Positive Systems has mapped landscapes throughout the world working for everyone from farmers to NASA. The four cameras mounted in a small aircraft take pictures in the visible spectrum as well as in the near infrared. Although the human eye is capable of sensing just a portion of the entire light spectrum, the cameras can see much more. The camera lenses pick up the nearest infrared which has several remarkable attributes including the fact that it interacts with chlorophyll, reflecting very well off of healthy plants.

By designating a color to the near infrared the cameras can detect the amount of light bouncing off of a given plant—the more reflective the plant, the healthier it is. In an age of high-tech, precision agriculture, every advantage helps. An acre of farmland, for instance, can support upward of 11,000 heads of lettuce; so to lose even a few acres on a corporate farm can mean a huge financial impact.

Understanding the whole system is a primary focus at NASA, where the Earth sciences program is providing government funds for private sector research into global change over time. In addition, Positive System teams with