

of contents for chapter 83 of that title, are repealed.

SEC. 5. EFFECTIVE DATE.

This Act and the amendments made by this Act shall take effect 90 days after the date of enactment of this Act.

Ms. COLLINS. Mr. President, I am pleased that the Senate will today give final approval to legislation I introduced to curb the availability of false identification via the Internet.

Let me thank my many colleagues in both the House and Senate for their hard work in moving this measure quickly through the legislative process. In particular, I appreciate the support and assistance of Chairman HENRY HYDE of the House Judiciary Committee, as well as the work of Congressman HOWARD COBLE, Congressman HOWARD BERMAN, Congressman JOHN CONYERS, and Congressman BILL MCCOLLUM. In addition to their efforts, I want to praise the strong support of Congressman MARK GREEN, who introduced a similar bill in the House. Enactment of this bill would not have been possible without the consistent support of the chairman of the Judiciary Committee, Senator HATCH, as well as the assistance of Senators KYL, LEAHY, FEINSTEIN, and DURBIN.

The bill before the Senate today will make important improvements in our laws against the distribution and use of false identification. As I found during a lengthy investigation of the availability of false identification on the Internet, our current laws have done little to stop a growing Internet market in every imaginable type of false identification. Whether via e-mail or from a Web site with a name such as thefakeidshop.com, everything from birth certificates, to Social Security cards, to driver's licenses, are being sold or traded through the ease of cyberspace.

Testimony before the Subcommittee on Investigations demonstrated that the availability of false identification documents from the Internet is a growing problem. Special Agent David Myers, Identification Fraud Coordinator of the State of Florida's Division of Alcoholic Beverages and Tobacco, testified that two years ago only one percent of false identification documents came from the Internet. Last year, he testified, a little less than five percent came from the Internet. Now he estimates that about 30 percent of the false identification documents he seizes comes from the Internet. He predicts that by next year his unit will find at least 60 to 70 percent of the false identification documents they seize will come from the Internet.

S. 2924 will put a stop to this widespread distribution of false identification, which can be used to commit identity theft, to facilitate serious financial crimes, and to facilitate the underage purchase of alcohol and tobacco. The new law will make clear

that it is a crime to transfer false identification documents by electronic means, and that those documents can be in the form of computer files, discs, or templates.

I expect strong action by law enforcement agencies to enforce both the existing provisions of title 18, section 1028, and the expanded authority provided by this legislation. The intent of S. 2924 is simple and clear—to stop those who use the Internet to sell, distribute, or make available false identification.

I am pleased that the new law will make it a crime to place false identification, regardless of its format, on an on-line location. Thus, the posting of such tools as scanned false identification documents or templates of state driver's licenses on Web sites will, without doubt, be illegal.

Mr. President, I am pleased that the House retained the provisions that will establish a coordinating committee to concentrate resources of federal agencies on investigating and prosecuting the creation of false identification. This multi-agency effort should draw on the resources of several agencies to investigate and prosecute those who engage in the production and transfer of false identification of any type. I urge the Attorney General and the Secretary of the Treasury to involve all agencies that can assist in curbing the use of false identification.

The House also approved another important portion of the Senate bill—the elimination of a section of law that unfortunately allowed criminals to manufacture, distribute, or sell counterfeit identification documents by using easily removable disclaimers as part of an attempt to shield the illegal conduct from prosecution through a bogus claim of “novelty.” No longer will it be acceptable to provide computer templates of government-issued identification containing an easily removable layer saying that it is not a government document.

I thank my colleagues for their support of this important legislation.

COMPUTER CRIME ENFORCEMENT ACT

Mr. STEVENS. Mr. President, I ask unanimous consent the Senate proceed to the immediate consideration of H.R. 2816.

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

The legislative clerk read as follows:

A bill (H.R. 2816) to establish a grant program to permit State and local law enforcement in deterring, investigating, and prosecuting computer crimes.

There being no objection, the Senate proceeded to consider the bill.

H.R. 2816, THE COMPUTER CRIME ENFORCEMENT ACT

Mr. LEAHY. Mr. President, I am pleased that the Senate is passing the

Computer Crime Enforcement Act, which is now headed to President Clinton for his signature into law. I introduced the Senate version of this bill, S. 1314, on July 1, 1999, with Senator DEWINE and is now also co-sponsored by Senators ROBB, HATCH and ABRAHAM. This legislation also passed the Senate as part of H.R. 46, the Public Safety Officer Medal of Valor Act. I thank my colleagues for their hard work on the Computer Crime Enforcement Act, especially Representative MATT SALMON, the House sponsor.

The information age is filled with unlimited potential for good, but it also creates a variety of new challenges for law enforcement. A recent survey by the FBI and the Computer Security Institute found that 62 percent of information security professionals reported computer security breaches in the past year. These breaches in computer security resulted in financial losses of more than \$120 million from fraud, theft of information, sabotage, computer viruses, and stolen laptops. Computer crime has become a multi-billion dollar problem.

The Computer Crime Enforcement Act is intended to help states and local agencies in fighting computer crime. All 50 states have now enacted tough computer crime control laws. They establish a firm groundwork for electronic commerce, an increasingly important sector of the nation's economy.

Unfortunately, too many state and local law enforcement agencies are struggling to afford the high cost of enforcing their state computer crime statutes.

Earlier this year, I released a survey on computer crime in Vermont. My office surveyed 54 law enforcement agencies in Vermont—43 police departments and 11 State's attorney offices—on their experience investigating and prosecuting computer crimes. The survey found that more than half of these Vermont law enforcement agencies encounter computer crime, with many police departments and state's attorney offices handling 2 to 5 computer crimes per month.

Despite this documented need, far too many law enforcement agencies in Vermont cannot afford the cost of policing against computer crimes. Indeed, my survey found that 98 percent of the responding Vermont law enforcement agencies do not have funds dedicated for use in computer crime enforcement. My survey also found that few law enforcement officers in Vermont are properly trained in investigating computer crimes and analyzing cyber-evidence.

According to my survey, 83 percent of responding law enforcement agencies in Vermont do not employ officers properly trained in computer crime investigative techniques. Moreover, my survey found that 52 percent of the law enforcement agencies that handle one