New laws let feds prosecute any criminal Internet transmission routed through U.S.

By D. IAN HOPPER, Associated Press
Wednesday, Nov. 21, 2001

WASHINGTON (AP) - Under the recently approved antiterrorism law, the Justice Department can now prosecute foreign hackers even when they attack only computers in their own countries.

Critics said Wednesday the change could make the United States the world's Internet police and set a precedent that would apply American values to the worldwide network.

Prosecutions can occur if any part of a crime takes place within U.S. borders. A large part of the Internet's communications traffic goes through the United States, even in messages that travel from one foreign country to another.

The new prosecutorial powers, which have no parallel in other nations, troubled one former Justice Department computer crimes prosecutor.

"It's a massive expansion of U.S. sovereignty," said Mark Rasch, now with computer security firm, Predictive Systems.

The change was highlighted last month by the Justice Department in its field guidance to federal prosecutors.

"Individuals in foreign countries frequently route communications through the United States, even as they hack from one foreign country to another," the recommendations said. "The amendment creates the option, where appropriate, of prosecuting such criminals in the United States."

The FBI referred questions to the Justice Department. A Justice Department spokeswoman did not return calls for comment Wednesday.

Much of the Internet's message traffic travels through the United States, dependent on American hubs in Virginia and California.

Jessica Marantz of the Internet statistics firm Telegeography said more than 80 percent of Internet access points in Asia, Africa and South America are connected through U.S. cities. Therefore, an e-mail sent between two cities in China probably will travel through the United States - putting its contents under American jurisdiction.

The Justice Department pushed for the legislation as a way to fight terrorism, and American interests overseas could be protected by the change.

But the change in law creates a precedent that could be used to prosecute any computer crime, Rasch said, from basic data theft to sending pornographic pictures. Current law already allows pornography prosecutions in any jurisdiction the pictures pass through, but this has not yet been applied on an international scale to Internet transmissions.

For example, an owner of a pornography Web site in Sweden might be prosecuted for sending a racy picture to a friend in Norway if the message happened to travel through a computer in Fairfax, Va. In that case, a U.S. prosecutor could try to extradite the sender and prosecute him for breaking Virginia law, using Virginia's standards for obscenity.

"We haven't done that yet, because it's an affront to the way the Internet works," Rasch said. "But now (with the antiterror law) we're criminalizing anything that happens over the Internet because traffic passes through the United States."

"What it basically says is that we will impose our values on anything that happens

anywhere in the world provided it passes through our borders."

FBI agents complain about the difficulty of computer crime investigations that almost always venture overseas, requiring time-consuming search warrants at every step and the cooperation of foreign governments. They also are frustrated by offshore pornography and gambling Web sites, accessed by Americans, that are legal in their own countries.

Prosecutors in the Philippines last year had to dismiss charges against a college student suspected of creating the "Love Letter" virus, which caused billions of dollars in damages worldwide, because they had no applicable law. Under the U.S. antiterror statute, the suspect could have been tried in America.

"There are still a lot of countries out there without adequate (computer crime) laws," said Bruce McConnell, who is conducting a survey on international computer laws. "Extradition is slow and expensive, so I would guess it wouldn't be used except in the worst cases."

David Sobel, general counsel of the Washington-based Electronic Privacy Information Center, said the change is particularly troubling when coupled with powers to send federal agents overseas to abduct and bring back suspects for trial.

"It is a significant expansion of U.S. jurisdiction with respect to so-called cybercrimes," Sobel said. "It was enacted under the guise of counterterrorism, but it is in fact applicable to all types of crimes."

Computer crime laws are rapidly changing worldwide. Earlier this month, the 43-member Council of Europe adopted a cybercrime treaty to standardize procedures for policing on the Internet. The United States has been invited to sign the treaty but has not yet done so.