HB 401

HB401 2029

AMENDMENT #1

OFFERED IN THE HOUSE

TO: CSHB 401(L&C)

Page l, lines 3 - 15:

Delete all material and insert:

"**Section 1.** AS 11.46.482(a) is amended to read:

(a) A person commits the crime of criminal mischief in the second degree if, having no right to do so or any reasonable ground to believe the person has such a right,

(1) with intent to damage property of another, the person damages property another in an amount of $500 or more;

(2) the person tampers with an oil or gas pipeline or supporting facility or an airplane or helicopter with reckless disregard for the risk of harm to or loss of the property; [OR]

(3) the person recklessly creates a risk of damage in an amount exceeding $100,000 to property of another by the use of widely dangerous means;

(4) *[Repealed, sec. 11 ch 71 SLA 1996.]*

(5) *[Repealed, sec. 11 ch 71 SLA 1996.]*

(6) with intent to cause a substantial interruption or impairment of a service rendered to the public by another person over a computer network, the person causes substantial interruption or impairment of service to the public."

Page 2, lines 1 - 14:

Delete all material

ALASKA STATE LEGISLATURE
House of Representatives

COMMITTEE ASSIGNMENTS:

LABOR &COMMERCE COMMITTEE, CHAIRMAN
JUDICIARY COMMITTEE, MEMBER
LEGISLATIVE COUNCIL, MEMBER
SPECIAL COMMITTEE ON UTILITY RESTRUCTURING, MEMBER
SPECIAL COMMITTEE ON ECONOMIC DEVELOPMENT & TOURISM, MEMBER

e-mail: Representative_Norman_Rokeberg@legis.state.ak.us

INTERIM:
716 WEST 4TH AVENUE, SUITE 640
ANCHORAGE, AK 99501
PHONE: (907) 269-0117
FAX: (907) 269-0119

SESSION
ALASKA STATE CAPITOL
JUNEAU, AK 99801-1182
PHONE: (907) 465-4968
FAX: (907) 465-2040

Representative Norman Rokeberg

MEMORANDUM

TO: Rep. Pete Kott, Chairman
House Judiciary Committee

FROM: Rep. Norman Rokeberg

DATE: April 3, 2000

RE: CSHB 401 (L&C)
An Act relating to computer networks and to electronic mail advertisements

Thank you for scheduling CSHB 401 (L&C) for a hearing before your committee on Friday, April 7, 2000.

Attached are:

1. CSHB 401 (L&C)
2. Three indeterminate fiscal notes
3. Sponsor Statement
4. Sectional Analysis
5. "Hackers increase attacks on Web sites", Fairbanks Daily News Miner, Feb. 10, 2000
6. "Web hackers widen attacks", Anchorage Daily News, Feb. 10, 2000
7. "Clinton meets computer experts", Juneau Empire, Feb. 15, 2000
8. "Internet attacks raise concerns about risks of growth", Peninsula Clarion, Feb. 14, 2000
9. "Catching hackers won't be easy", Peninsula Clarion, Feb. 17, 2000
10. "Expert sees rising cyber-terror risk", Alaska Journal of Commerce, March 5, 2000
11. "How the government failed to stop the worlds worst Internet attack", USA Today, March 9, 2000
12. "Hackers' Web-site assaults take toll, Seattle Times, March 12, 2000
13. "Cookies' maker chews over their fate", Anchorage Daily News, March 12, 2000
14. "Technology creator warns of its threat to mankind", Anchorage Daily News, March 13, 2000
15. "Web attacks raise concerns about growth", USA Today, Feb. 13, 2000
16. "ISP Posts Blacklist of Smurf-Friendly Networks", Inter@active Week, April 20, 1998
17. "Anti-Spam Bill Introduced to Solve a National Problem", Press Release, Senator Frank Murkowski
18. Copy of S 759, Inbox Privacy Act of 1999, 106th Congress, 1st session

CS FOR HOUSE BILL NO. 401(L&C)

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-FIRST LEGISLATURE - SECOND SESSION

BY THE HOUSE LABOR AND COMMERCE COMMITTEE

Offered: 3/28/00
Referred: Judiciary, Finance

Sponsor(s): REPRESENTATIVE ROKEBERG

A BILL

FOR AN ACT ENTITLED

"An Act relating to computer networks and to electronic mail advertisements."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

* **Section 1.** AS 11.46.480(a) is amended to read:

(a) A person commits the crime of criminal mischief in the first degree if, having no right to do so or any reasonable ground to believe the person has such a right,

(1) with intent to cause a substantial interruption or impairment of a service rendered to the public by a utility or by an organization **that** [WHICH] deals with emergencies involving danger to life or property, **or rendered to the public by another person over a computer network,** the person damages or tampers with property of that utility, [OR] organization**, or person** and causes substantial interruption or impairment of service to the public;

(2) with intent to damage property of another by the use of widely dangerous means, the person damages property of another in an amount exceeding $100,000 by the use of widely dangerous means;

(3) the person intentionally damages an oil or gas pipeline or supporting facility; or

(4) with intent to cause physical injury to another person, the person [:]

(A) tampers with an item that is a food, drug, or cosmetic or a container for the item; or

(B) delivers, dispenses, or distributes an item described in (A) of this paragraph knowing that a person has tampered with the item.

* **Sec. 2.** AS 11.46.490(7) is amended to read:

(7) "utility" means an enterprise, whether publicly or privately owned or operated, **that** [WHICH] provides gas, electric, steam, water, sewer, or communications service, and any common carrier; **in this paragraph, "communications service" includes Internet service providers and the Internet and its ancillary services;**

* **Sec. 3.** AS 45.50.471(b) is amended by adding a new paragraph to read:

(43) violating AS 45.50.479 (unsolicited electronic mail advertisements).

* **Sec. 4.** AS 45.50 is amended by adding a new section to read:

Sec. 45.50.479. Provider's restriction on use of electronic mail service. (a) A registered user of an electronic mail service may not use or cause to be used the provider's service or equipment in violation of the provider's published policy prohibiting or restricting the use of its service or equipment for the initiation of unsolicited advertisements if the user has previously sent an unsolicited advertisement to 25 or more people or has previously been warned by the provider or recipient for sending unsolicited advertisements.

(b) A person may not, by initiating an unsolicited advertisement, use or cause to be used the service or equipment of an electronic mail service provider in violation of the provider's published policy prohibiting or restricting the use of its service or equipment to deliver unsolicited advertisements if the user has previously sent an unsolicited advertisement to 25 or more people or has previously been warned by the provider or a recipient for sending unsolicited advertisements.

(c) This section may not be interpreted to require an electronic mail service provider to adopt a policy prohibiting or restricting the use of its service or equipment for the initiation or delivery of unsolicited advertisements. This section does not limit or restrict the authority of an electronic mail service provider to enforce its policies or to prohibit or restrict the use of its services or equipment.

(d) An electronic mail service provider is considered to have published the provider's policy on unsolicited advertisements if the provider

(1) makes the policy available on request in written form at no charge to the requester; or

(2) displays the policy through an on-line notice on the provider's Internet home page or on a page accessible through a conspicuous link on the provider's Internet home page.

(e) In this section,

(1) "advertisement" means an electronic mail message, the principal purpose of which is to promote, directly or indirectly, the sale or other distribution of real property, goods, or services;

(2) "electronic mail" means a message or a file that is transmitted through a local, regional, or global network, regardless of whether the message, file, or other information is

(A) viewed;

(B) stored for retrieval at a later time;

(C) printed onto paper or other similar material; or

(D) filtered or screened by a computer program that is designed or intended to filter or screen items of electronic mail;

(3) "electronic mail service provider" or "provider" means a business or organization qualified to do business in the state or a governmental entity that provides registered users with the ability to send or receive electronic mail;

(4) "initiation" of an unsolicited advertisement refers to the action by the initial sender of the advertisement; it does not refer to the actions of any intervening electronic mail service providers that may handle or retransmit the electronic message;

(5) "network" means a network made up of one or more computers that may be accessed by a modem, electronic or optical technology, or other similar means;

(6) "recipient" means a person who receives an item of electronic mail;

(7) "registered user" means an individual, corporation, or other person that maintains an electronic mail address with an electronic mail service provider;

(8) "unsolicited advertisement" means an electronic mail advertisement that is

(A) addressed to a recipient with whom the initiator does not have an existing business or personal relationship; and

(B) not sent at the request of or with the express consent of the recipient.

FISCAL NOTE

STATE OF ALASKA
2000 LEGISLATIVE SESSION

BILL NO. HB 401

Revision Date/Time (Note if correction) 3/23/00
Dept. Affected Administration
Title "An Act relating to computer networks and to electronic mail advertisements."
BRU Legal and Advocacy Services
Component Public Defender Agency
Sponsor Representative Rokeberg
Requester (H) L&C
Component No. 1631

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006
Personal Services	*	*	*	*	*	*
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	*	*	*	*	*	*
CAPITAL EXPENDITURES	*	*	*	*	*	*
CHANGE IN REVENUES ( )	*	*	*	*	*	*

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts	*	*	*	*	*	*
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type)						
TOTAL	*	*	*	*	*	*

Estimate of any current year (FY2000) cost:

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: *(Attach a separate page if necessary)*

See attached.

Prepared by: Barbara Brink, Director
Phone 264-4414
Division Public Defender Agency
Date/Time
Approved by Commissioner -- Robert Poe, Jr.
Date 3/23/00
Agency Department of Administration

PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE
For further distribution information, call the Governor's Legislative Office

(Rev 10/99) 2000/inform.xls/OMB

FISCAL NOTE

STATE OF ALASKA **BILL NO. HB 401**
2000 LEGISLATIVE SESSION

ANALYSIS CONTINUED:

This bill amends the Criminal Mischief in the First Degree statute. First degree criminal mischief is a class B felony and outlaws such things as intentionally interrupting public utility services and causing over $100,000 damage to private property by widely dangerous means.

The amendment proposed by this bill would include damaging a computer network that provides service to the public with intent to cause a substantial interruption or impairment of a service rendered to the public in first degree criminal mischief. Also, the definition of "utility" is modified to include Internet Service Providers.

The Public Defender Agency is unable to estimate how many additional cases it would be appointed to if the bill becomes law. It is clear, however, that these will be serious cases. They will also be difficult to defend because these offenses will probably be highly technical in nature. Therefore, although we do anticipate some fiscal impact, we are not able to quantify it and are submitting an indeterminate fiscal note.

FISCAL NOTE

STATE OF ALASKA
2000 LEGISLATIVE SESSION

BILL NO. HB 401

Revision Date/Time (Note if correction) _____ Dept. Affected Department of Corrections

Title An Act relating to computer networks and to electronic mail advertisements

BRU Administration and Operations

Component All

Sponsor Representative Rokeberg

Requester House Labor and Commerce Committee

Component No. #0694

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	***	***	***	***	***	***
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type)						
TOTAL	***	***	***	***	***	***

Estimate of any current year (FY2000) cost: 0.0

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: *(Attach a separate page if necessary)*

See attached analysis.

Prepared by: Candy Brower, Legislative Liaison Phone 465-3307

Division Commissioner's Office Date/Time 3/22/00 1:42 PM

Approved by Commissioner Margaret M. Pugh Margaret M. Pugh Date 3/22/00

Agency Dept. of Corrections

PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE

For further distribution information, call the Governor's Legislative Office

FISCAL NOTE

STATE OF ALASKA
2000 LEGISLATIVE SESSION
DEPARTMENT OF CORRECTIONS

BILL NO. HB 401
PAGE 2 of 2
DATE 3/22/00

ANALYSIS:

If passed, this legislation would make it a B Felony (Criminal Mischief I) to intentionally cause a substantial interruption or impairment of a service rendered to the public by another person over a computer network by damaging or tampering with that person's property. This includes the Internet service providers and the Internet and its ancillary services. There has been attention in the media regarding such incidents recently, however, it is difficult to project how often this might occur and whose jurisdiction such an offender would be under. Federal jurisdiction might supersede State jurisdiction in some cases.

While it is the Department of Corrections assumption that these cybercrimes are the wave of the future, and that these offenders are likely to be first time offenders, it is difficult to estimate fiscal impact to the Department. Therefore, the Department of Corrections is submitting an indeterminate fiscal note.

FISCAL NOTE

STATE OF ALASKA
2000 LEGISLATIVE SESSION

BILL NO. HB 401

Revision Date/Time (Note if correction) _____
Dept. Affected Law
Title "An Act relating to computer networks and to electronic mail advertisements."
BRU Criminal Division/Civil Division
Component 1st-4th Jud Dist; Criminal Appeals/ Special Lit/Fair Business Practices
Sponsor Representative Rokeberg
Requester House Labor and Commerce Committee
Component No. 2198-99,2201,03,61,79,06

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	*******	*******	*******	*******	*******	*******
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type)						
TOTAL	*******	*******	*******	*******	*******	*******

Estimate of any current year (FY2000) cost: _____

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: *(Attach a separate page if necessary)*

HB 401 makes it a class B felony to intentionally and substantially interrupt or impair a service rendered to the public by another person over a computer network by damaging or tampering with that person's property. In addition, the bill adds to the Unfair Trade Practices and Consumer Protection Act restrictions on the use of a provider's electronic mail service to initiate unsolicited e-mail advertisements .

The Department of Law does not anticipate a fiscal impact on the Consumer Protection unit from the latter change. The addition of a new felony level crime will impact the department; however, it is difficult to quantify what the impact will be. We have no way of estimating how widespread this terroristic conduct is in Alaska, and how often prosecution would fall to state as opposed to federal law enforcement as this type of hacking often crosses state, and national, boundaries.

Prepared by: Joan M. Kasson Joan M Kasson Phone 465-3370
Division Attorney General's Office Date/Time 3/20/00, 9:09 AM
Approved by Commissioner Bruce M. Botelho, Attorney General Date 3/20/00
Agency Department of Law

PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE

For further distribution information, call the Governor's Legislative Office

(Rev 10/99) 2000/norm.xls/OMB

ALASKA STATE LEGISLATURE
House of Representatives

COMMITTEE ASSIGNMENTS:

LABOR &COMMERCE COMMITTEE, CHAIRMAN
JUDICIARY COMMITTEE, MEMBER
LEGISLATIVE COUNCIL, MEMBER
SPECIAL COMMITTEE ON UTILITY RESTRUCTURING, MEMBER
SPECIAL COMMITTEE ON ECONOMIC DEVELOPMENT & TOURISM, MEMBER

e-mail: Representative_Norman_Rokeberg@legis.state.ak.us

INTERIM:
716 WEST 4TH AVENUE, SUITE 640
ANCHORAGE, AK 99501
PHONE: (907) 269-0117
FAX: (907) 269-0119

SESSION:
ALASKA STATE CAPITOL
JUNEAU, AK 99801-1182
PHONE: (907) 465-4968
FAX: (907) 465-2040

Representative Norman Rokeberg

SPONSOR STATEMENT
CSHB 401 (L&C)
An Act relating to computer networks and to electronic mail advertisements
By Representative Norman Rokeberg

CSHB 401 (L&C) adds protections for consumers and internet service providers from such things as intentional disruption (e.g., a denial of service attack) or impairment of a service rendered to the public by a utility or emergency organization, or computer network, etc. Such actions would be a crime of criminal mischief in the first degree under CSHB 401 (L&C).

In the definition of "utility", CSHB 401 (L&C) adds language stating that a "communications service" includes Internet service providers and the Internet and its ancillary services.

Next CSHB 401 (L&C) provides that a user of an e-mail service may not use the provider's service in violation of any published policy of the provider (e.g., anti-spamming provisions). Additionally, the bill provides that the e-mail service provider does not have to adopt a policy prohibiting or restricting use of its services for delivery of unsolicited advertisements – in other words, if the provider wants to adopt a policy, that is fine. "Published" can be by means of written form, or display through on-line notice.

As we all move towards greater involvement with e-commerce, consumers need to know that some protections are available to them from such things as unsolicited advertisements. CSHB 401 (L&C) would provide this protection.

I would urge your support of this legislation.

ED 2:04/03/00

ALASKA STATE LEGISLATURE
House of Representatives

COMMITTEE ASSIGNMENTS:

LABOR &COMMERCE COMMITTEE, CHAIRMAN
JUDICIARY COMMITTEE, MEMBER
LEGISLATIVE COUNCIL, MEMBER
SPECIAL COMMITTEE ON UTILITY RESTRUCTURING, MEMBER
SPECIAL COMMITTEE ON ECONOMIC DEVELOPMENT & TOURISM, MEMBER

e-mail: Representative_Norman_Rokeberg@legis.state.ak.us

INTERIM:
716 WEST 4TH AVENUE, SUITE 640
ANCHORAGE, AK 99501
PHONE: (907) 269-0117
FAX: (907) 269-0119

SESSION:
ALASKA STATE CAPITOL
JUNEAU, AK 99801-1182
PHONE: (907) 465-4968
FAX: (907) 465-2040

Representative Norman Rokeberg

SECTIONAL ANALYSIS
CSHB 401 (L&C)
An Act relating to computer networks and to electronic mail advertisements
By Representative Norman Rokeberg

Section 1: Amends criminal law to provide that it is the crime of criminal mischief in the first degree if a person, having no right to do so, causes substantial interruption or impairment of a service rendered to the p public by a utility or organization dealing with emergencies, or rendered to the public by another person over a computer network.

Section 2: Amends the definition of "utility" and the subdefinition of "communications service" to include Internet service providers, and the Internet and its ancillary services.

Section 3: Adds reference to 45.50.479 (unsolicited electronic mail advertisements) to AS 45.50.471(b).

Section 4: Adds new section concerning provider's restriction on use of electronic mail service. Includes description of the provider's policy and how it can be published. Defines "advertisement", "electronic mail", "electronic mail service provider", "provider", "initiation", "network", "recipient", "registered user", and "unsolicited advertisement".

ED 02:04/03/00

[ackers increase attacks on Web sites

Associated Press

EW YORK—An electronic assault on e of the biggest sites in cyberspace is re- ing calls for better high-tech security by nesses and government. But even propo- s of stricter measures acknowledged e was no ironclad defense.

ackers stepped up this week's attack on nesday, inconveniencing millions of In- et users and unnerving Wall Street. The urently coordinated attacks spread to ade, ZDNet and other major sites—all of n disturbed by a barrage of messages.

ederal officials urged businesses to install ective software and take other security precautions.

"We are committed to in every way possible to tracking those who are responsible," Attorney General Janet Reno said in Washington.

Sensitive government systems were being quickly secured against potential attacks, Commerce Secretary William Daley said in a teleconference Wednesday.

"Right now there is no surefire defense, but we are trying to take some steps," he said. "First we are taking special action to ensure that all federal systems, including civilian agency systems, and those of the Defense Department, are clean of these infections, which make some systems the unwitting partner in these attacks."

Some security experts said the publicity could encourage pranksters.

"It's what these guys go after—to be known as the person or group of people who've pulled these attacks off," said Simon Perry, security business manager at Computer Associates International, a maker of business software. "Instead of graffiti on the subway wall, they've climbed up to the 40th floor of the Empire State Building and put their messages there."

The growing anxiety about the Internet's

See HACKERS, Page A-9

Fairbanks Daily News Miner, Feb 10, 2000, pg 1A

Fairbanks Daily News-Miner, Thursday, February 10, 2000

HACKERS BO[illegible]

Continued from Page A-1

vulnerability contributed to a 258-point slide in the Dow Jones average Wednesday and halted three straight record-high closings for the Nasdaq Composite Index, which is heavy with high-tech stocks.

The hacker technique—called a "denial of service attack"—involves directing a flood of messages to computers that run Web sites. The effect is comparable to unleashing a wave of calls to tie up a city's phone lines.

The ETrade online brokerage's Web site was hit Wednesday, but "customer accounts were never compromised," spokesman Patrick Di Chiro said. Less than one-fifth of its customers were affected by the clogged traffic for about 90 minutes before the company blunted the attack, he said.

ZDNet.com, a popular news site that covers technology, said its Web site was shut down for two hours and "appeared to have been the target of a denial-of-service attack."

Major sites attacked this week include eBay, Amazon.com, CNN, Buy.com and Yahoo!

Web hackers widen attacks

Message flood cripples more major sites; Wall Street jittery

By DAVID E. KALISH
The Associated Press

NEW YORK — Hackers stepped up a three-day electronic assault Wednesday against some of the most popular sites on the Web, inconveniencing millions of Internet users and unnerving Wall Street.

The apparently coordinated attacks spread to ETrade, ZDNet and other major sites Wednesday. All of them were crippled by a barrage of messages generated by hackers.

The growing anxiety about the Internet's vulnerability contributed to a 258.44 point-slide in the Dow Jones average and halted three straight record-high closings for the NASDAQ Composite Index, which is heavy with high-tech stocks.

"Right now there is no surefire defense, but we are trying to take some steps."

— Commerce Secretary William Daley

The attacks also prompted top federal officials to reassure Americans that authorities are doing everything they can to fight the on-line vandalism.

"We are committed in every way possible to tracking those who are responsible," Attorney General Janet Reno said in Washington.

She said the motives of the vandals are not known, "but

See Back Page, HACKERS

ADN, Feb 10, 2000, pg A1

HACKERS: Businesses urged to protect themselves

they appear to be intended to interfere with and disrupt legitimate electronic commerce."

The hacker technique, called a "denial of service attack," involves directing a flood of messages to computers that run web sites. The effect is comparable to erecting human barricades to block shoppers from entering a mall or unleashing a wave of calls to tie up a city's phone lines.

Hackers could face maximum penalties of 5 to 10 years behind bars and fines up to $250,000, or in some cases "twice the gross loss to the victim," said FBI cyber-security expert Ronald Dick.

In the latest attacks, the ETrade brokerage's web site was hit, but "customer accounts were never compromised," spokesman Patrick Di Chiro said. Less than one-fifth of its customers were affected by the clogged traffic for about 90 minutes.

ZDNet.Com, which covers technology, said its site was shut down for two hours.

Microsoft's MSN.com said it was indirectly affected because of disruptions to several Internet service providers carrying its traffic. Major sites that came under attack Tuesday included eBay, Amazon, CNN and Buy.Com, all in aggressive assaults similar to one that overwhelmed Yahoo! a day earlier.

Federal officials urged businesses to install protective software.

"Right now there is no surefire defense, but we are trying to take some steps," Commerce Secretary William Daley said. "First we are taking special action to ensure that all federal systems, including civilian agency systems, and those of the Defense Department, are clean of these infections, which make some systems the unwitting partner in these attacks."

Juneau Empire, Feb 15, 2000

Clinton meets computer experts

■ *Web security sought after hacker attacks; FBI has suspects*

By SONYA ROSS
THE ASSOCIATED PRESS

WASHINGTON – With the FBI seeking to question several hackers about last week's Internet attacks, President Clinton today began exploring ways to tighten security on the World Wide Web but cautioned the attacks were not an "electronic Pearl Harbor."

Surrounded by technology experts and a hacker known as Mudge, Clinton said the attacks nevertheless served as a needed wake-up call. The assault was hardly so devastating that it could be compared to Japan's bombing of Pearl Harbor, which wiped out the Pacific Fleet and drew the United States into World War II, he said.

"It's a source of concern, but I don't think we should leave here with this vast sense of insecurity," Clinton said. "We ought to leave here with a sense of confidence that this is a challenge that was entirely predictable. It's part of the price of the success of the Internet."

Clinton gathered in the White House Cabinet Room with about 20 industry representatives, national security experts and Attorney General Janet Reno. He said the goal of the meeting was to ensure that the Internet remains "open and free."

One participant, Whitfield Diffie of Sun Microsystems, set up his laptop on the conference table, an agenda on the screen. Mudge, in a business suit with his long brown hair hanging down on his chest, sat quietly with his fingers interlocked atop his blue briefing books.

Meantime, a computer believed to have been used in last week's attacks, was seized by federal agents, Hillsboro, Ore., Police Sgt. Allen Zaugg, head of a group of officers trained for high-tech cases, said today.

The FBI is now analyzing that computer, which was seized within the last two days from a home business in the Portland, Ore., area, a federal official in Washington said, requesting anonymity. Its owner apparently was not aware the computer was used as a middleman in the attacks, this official said.

The threat of an "electronic Pearl Harbor" was raised in March 1999 by then-Deputy Defense Secretary John Hamre, who predicted in congressional testimony that cyberterrorists would target America's commercial interests.

The initial idea of the session was to address the problem of terrorists using cyberspace. But Clinton told CNN.com on Monday that last week's attacks underscore a need for the government to focus on protecting the Internet itself.

The FBI was seeking to interview several hackers known by their Internet screen names, including one who calls himself "mafiaboy" and another who calls himself "coolio," a Justice Department official said.

Internet attacks raise concerns about risks of growth

By ANICK JESDANUN
AP Internet Writer

NEW YORK — A swarm of recent hacking attacks highlight one emerging concern about the Internet: It may be growing too fast for security to keep up with technology.

Some security experts believe it's time to focus on making the Net safer, which could mean rebuilding much of the underlying infrastructure from scratch. After all, consumers and businesses now use the Internet for tasks unforeseen 30 years ago.

Security was an afterthought when Internet standards were developed by university thinkers and computer administrators, says Russ Cooper, who runs the NTBugtraq Web site devoted to security.

"This is now the foundation for billions of dollars worth of commerce," Cooper said. "It is inherently flawed because we don't check to see if what it's being used for is what it is intended for."

Randy Sandone of Argus Systems Group Inc. is blunter: "The Web is rotten at its core."

Yahoo!, Buy.com, eBay, ETrade and other prominent sites were paralyzed for hours at a time last week when hackers overloaded them with fake traffic.

The attacks followed several computer virus outbreaks last year — such as Melissa — which spread rapidly by taking advantage of functions that were designed to make Internet use friendlier.

And last month, a hacker stole credit card numbers from the Internet music retailer CD Universe, then released thousands of them on a Web site after the firm refused to pay $100,000 ransom.

"I fully expect the Internet to ultimately be safe and stable," said Stephen Gorrell, program manager for Norton Internet Security software. "However, in the period of record growth, it's not surprising new holes are discovered."

The Internet's developers could not have effectively countered threats to commerce because e-businesses did not yet exist, Gorrell said.

As the Internet grows, so do the numbers of hackers and potential victims. And hackers are becoming more sophisticated, with some even developing tools to automate their attacks.

'I fully expect the Internet to ultimately be safe and stable. However, in the period of record growth, it's not surprising new holes are discovered.'

—Stephen Gorrell, program manager for Norton Internet Security software

Software companies, some critics say, contribute to the problems by releasing products that still have security holes.

"Each day, technology is changing," said Robert Ing, who handles electronic security for SBR International Inc. in Toronto. "There's a rush to get products out to market because it is a competitive marketplace. Sometimes, security is overlooked."

Steve Hunt, security analyst at Giga Information Group in Chicago, hopes the latest attacks will encourage companies to take security more seriously.

"We owe quite a debt of gratitude to hackers to show us where our pants have been down," he said.

Security and Internet experts differ on how far they need to go — and that itself is a problem. Some believe in completely updating equipment and software to reduce users' anonymity and improve authentication.

In the offline world, businesses have experience with security guards and special locks. Some practices are even required by law or insurance companies.

But the Internet community has yet to agree on such standards, said Harris Miller, president of the Information Technology Association of America.

Phil Attfield, director of technical marketing at McAfee.com, said Internet security will eventually catch up.

"The approaches are going to have to become more formal rather than ad hoc," he said. "We've been getting there incrementally. That's the way technology is evolving."

But hacking will never completely disappear, said Keith Teare, the chairman and chief executive of RealNames. Vandals broke into RealNames' computers Wednesday, and the company had to warn some 20,000 customers that their credit card numbers might have been stolen.

"For every secure environment, there will be somebody prepared to try to break in," Teare said. "If they are clever enough, they will find holes."

Greg Hawkins, chief executive of Buy.com, said the attacks on his shopping site and others raised awareness.

"This is a new frontier. It's big, it's fast, and it's growing rapidly," he said. "With that growth will come continued challenges to make sure it's a secure and effective environment. We are clearly going to have growing pains like this from time to time."

BUSINESS

Catching hackers won't be easy

FBI seeks expansion of racketeering laws against organized electronic assault

By TED BRIDIS
AP Technology Writer

WASHINGTON — The nation's top law enforcement officials acknowledged on Wednesday serious challenges finding the electronic vandals who shut down major Internet sites last week, but they also described "fast-developing leads."

They said the hackers involved were sophisticated enough to falsify their digital fingerprints. Attorney General Janet Reno said such a disguise technique "makes it difficult, and sometimes impossible, to hold the perpetrator criminally accountable."

"I would simply say that we are taking the attacks very seriously and that we will simply do everything in our power to identify those responsible and bring them to justice," Reno told a Senate panel.

FBI Director Louis J. Freeh, who also testified, said there were "fast-developing leads as we speak, and hopefully we can provide more details in coming days." He said FBI field offices in five cities have opened investigations into the attacks: Los Angeles, San Francisco, Atlanta, Boston and Seattle. More agents in other cities and overseas are also involved.

Reno and Freeh also conceded important shortcomings coordinating the myriad government agencies and public and private experts who help investigate high-tech crimes. "We're not doing so good," admitted Freeh, adding that cooperation was improving.

The FBI also urged Congress on Wednesday to consider expanding use of federal racketeering "RICO" laws — traditionally used against the mafia and drug cartels — to apply against organized and persistent hackers. It also urged Congress to lower the $5,000 minimum in damages that victim companies must suffer before attackers can be prosecuted under federal computer crime laws.

Freeh said lawmakers should consider "whether some of this activity, which goes beyond a single episode of fraud or hacking, gets into the realm of enterprise criminal activity."

"RICO was intended to get gangsters," said Jennifer Granick, a California lawyer who has represented hackers. "Now, it's getting a bunch of kids in black concert T-shirts."

Freeh said hackers in many of last week's attacks falsified the Internet addresses of the computers they used, "meaning that the address that appeared on the target's log was not the true address of the system that sent the messages."

eBay Inc. disclosed new details Wednesday about the electronic assault launched against it Feb. 8, which shut down the world's largest online auction site for 90 minutes. Similar attacks disrupted other major commercial sites, including those of Yahoo!, Amazon, Buy.Com, CNN and ETrade.

eBay's lawyer, Robert Chesnut, described an "insidious, organized attack" that was "obviously well planned."

The attackers flooded eBay's site with 10 times its normal incoming data, transmitting a specific type of information identical to that used against Yahoo! on Feb. 7.

Chesnut told the Appropriations subcommittee on Commerce, Justice, State and judiciary that eBay also was attacked the evening of Feb. 9, but engineers were able to repel the second attack quickly.

The FBI is contacting several hackers known by their online nicknames. The bureau would not say whether its agents have talked with any suspects, but it appeared some interviews have begun, hacker sources said.

The testimony from Reno and Freeh followed President Clinton's meeting Tuesday with technology experts about ways to improve Internet security. Participants said that during the talks, industry leaders urged the government to lead by example by making its computer systems secure.

But overnight Tuesday, a hacker vandalized at least four Web sites at the Transportation Department, including the page for the agency's information officer, George Molaski.

Those attacks were first noted by Attrition.Org, a computer security Web site that records such hacks.

The computer breached by the hacker "was in the process of being fixed," Molaski said Wednesday. "Unfortunately, they got to it before we closed that door. It was a relatively simple vulnerability."

Also Wednesday, House Commerce Chairman Tom Bliley, R-Va., criticized "highly vulnerable" computers at the Environmental Protection Agency and urging it to shut down its Internet connection immediately, citing an unreleased report by the General Accounting Office.

EPA spokesman David Cohen said the agency has no plans to disable Internet access, adding that experts there have taken steps to strengthen security of computers with sensitive information.

Expert sees rising cyber-terror risk

By Nancy Pounds
Journal Assistant Editor

TECHNOLOGY

America's growing dependence on the Internet and major industry networks has put the nation at the highest risk yet for cyber-terrorism attacks, according to one technology expert.

The nation's Internet systems are more vulnerable than other countries' operations since more than half of the Internet is in the United States, he said.

Although more cyber-crime has been identified than techno-terrorism, the criminals could be practicing now, said Seymour Goodman, a professor at Stanford and Georgia Tech universities. He also is director of the Consortium for Research on Information Security and Policy at Stanford.

Goodman, who has visited 80 countries to offer international public policy advice on technology, spoke Feb. 25 at the Alaska World Affairs Council luncheon at the Hilton Anchorage Hotel.

Cyberspace crimes can range from robbery to intimidation to warfare, including attacking military networks, he said.

"And the United States is a prime target since we rely on these systems," Goodman said.

Alaska's vulnerability to cyberspace attacks could climb depending on the security of systems controlling a proposed National Missile Defense System that could be built in Alaska, he said.

From his experience, Goodman has seen that many network technology systems lack needed security to fend off criminals.

"We've made ourselves more vulnerable at the same time as we're taking advantage of the efficiencies of the systems," he said.

In the last 10 years, activity in cyberspace has experienced an explosion, especially in Internet users and networks that power industries like the banking and finance sector, Goodman said.

Started 30 years ago, the Internet has grown from the six countries connected 15 years ago to 214 entities today, he said. Each year the Internet grows another 50 percent to 100 percent.

"This represents one of the most rapid infusions of technology," Goodman said.

Accompanying growth is increased efficiency and connectivity, which in turn spurs greater dependence on Internet and network systems, he said.

"I would argue that what has happened in cyberspace, particularly in the last 10 years, is that we have created a new medium of great importance for a tremendous spectrum of human activity," Goodman said.

This technology-driven medium, similar to physical media of air, sea and land, is the stage for social and financial transactions on a large scale, he said.

However, the systems that make up the Internet often lack security as a main function, according to Goodman.

One of Goodman's Stanford colleagues was one of the initial Department of Defense Internet operators who says that as early Internet programmers, they di d not design security into the operation, but planned to come back to it. But now the Internet is much more complex, Goodman said.

Vulnerable systems lead to more opportunities for conflict, whether it's offensive content or decaying ethics, he said. Also, from the standpoint of crime, there are increased opportunities for terrorism because terrorists can be distant from their victims, he said. "Crime out there on the Internet is growing as quickly as the Internet itself.

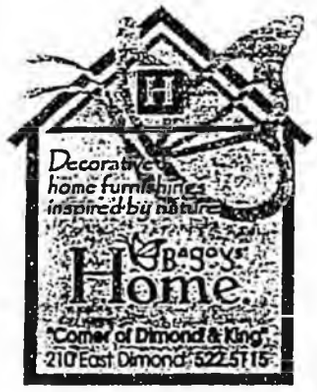
"Some of us think that we still need to civilize cyberspace. Otherwise it will be like the wild West. But how do we do that? This is an international, borderless medium."

One means of defense is passive — making computers less easy to hack, he said. But without a penalty for breaking in, attackers will try until they succeed or become bored, he added.

An active defense includes collecting evidence in the difficult task of apprehending cyberspace criminals internationally, although this plan requires countries to agree on what would be considered a crime, he said.

The cost of technology crime won't be paid by industries or governments, Goodman said.

"We as individuals will pay for this if it's not fixed, or we will pay as a nation if a terrorist attack occurs," he said.



Selling Your Company?

Let Me Help.

- Consultation
- Value Assessment
- Packaging
- Results

Matthew Fink
Commercial Properties/Business Specialist
3111 'C' Street, Suite 100 • Anchorage, Alaska 99503
Office (907) 261-7620 • Fax (907) 261-7685

DYNAMIC PROPERTIES

www.usatoday.com

THE NATION'S NEWSPAPER

USA TODAY

NO. 1 IN THE USA . . . FIRST IN DAILY READERS

LATESPORTS

USA TODAY

John Smoltz: Injury ends season.

ABC

Boomer Esiason: Sacked by ABC.

AP

Dennis Rodman: Released by Mavs.

They're out

1C

GOD LI TOAST PASTR

God, the De is a new TV whimsical tw Almighty loo Garcia, an au must save the Satan has an accent. A rev

THURSDAY MARCH 9, 2000

NEWSLINE

A QUICK READ ON THE NEWS

WALL STREET: Dow Jones industrial average jumps 60.50 points to 9856.53; Nasdaq index soars 49.33 points to 4897.17; 30-year Treasury bond yield climbs to 6.16%. 1,4B.
▶ USA TODAY Internet 100 rises 0.88 points to 189.04. 4B.
▶ Japan's Nikkei average is up 119 points to 19,886 midday; yen is 107.04 per dollar. Hong Kong's Hang Seng index is 198 points to 18,149 early today.

Four killed in Memphis ambush

By A.J. Wolfe, The Commercial Appeal, via AP

Aftermath: Firefighters console one another Wednesday after arriving at a house fire and being shot at by an off-duty firefighter; four people were killed and two were injured. 4A.

OIL PRICES FALL: OPEC pledge to provide "adequate and timely oil supplies in coming months" is linked to a more than 8% drop in crude oil prices. 1B.

SOUTHWEST AIRLINES CRASH: Pilots are blamed for approaching Sunday's landing in California too fast and too steep. 3A.

FASTEST-GROWING COUNTY: Virginia's Sussex County zooms from 10,000 to more than 12,000 from 1998-99, thanks to two new prisons and 2,400 inmates. 3A.

TODAY'S DEBATE: Interest rate hikes. In USA TODAY's opinion, "Greenspan hits the brakes. Risky? Yes. But less risky than letting inflation take hold."
▶ "We are in a New Era economy that is different from the economies of the past. As a result, it requires a different monetary policy," Brian S. Wesbury says.

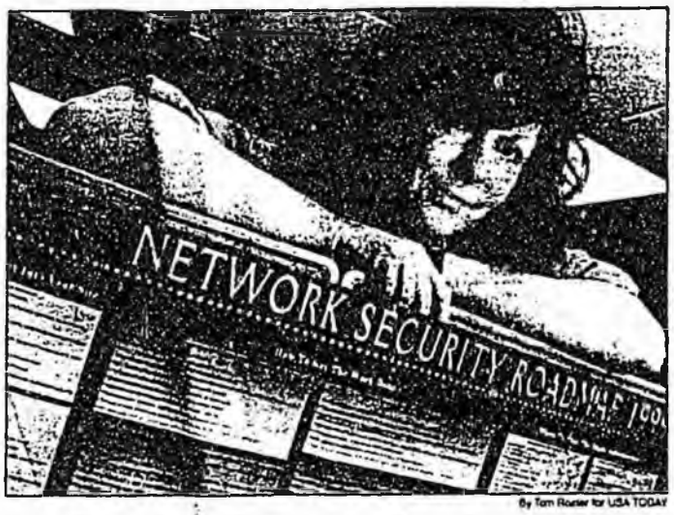
MONEY: Homebuyers basking in new no-down payment, 100%-plus mortgages; experts express concern. 1B.
▶ Low-cost Linux is giving Windows a run for its money. 1B.
▶ Traffic safety officials warn about use of vans instead of buses to transport students. 1B.
▶ Miller rolling out beer in plastic bottles. 3B.

SPORTS: Tony Hawk has turned skateboarding into big bucks. Critics wonder whether that's a good deal. 3C.
▶ Buffalo tops Boston in overtime 2-1. NHL. 13-14C.

LIFE: Marketing firms that work for drug companies teach doctors about the products, raising ethical flags. 1D.
▶ Andrew Huebner writes a haunting first novel about the Indian wars. Books, reviews, best sellers. 6-8D.

CORRECTION: Rhode Island election results were transposed in some editions Wednesday. McCain won the state over Bush 60%-36%. Super Tuesday results. 14A.

Written by John O. Buckley



By Tom Rosier for USA TODAY

Watched her system get buried: Susan Levy Haskell of the University of Minnesota.

How the government failed to stop the world's worst Internet attack

By M.J. Zuckerman
USA TODAY

COVER STORY

Susan Levy Haskell arrived at her office at the University of Minnesota as usual before 8 a.m. on Monday, Aug. 16, 1999, where she watched at first curiously, then later in horror, as the university computer system came under attack from a massive yet anonymous Internet adversary.

Haskell, the university's computer security coordinator, says that as hours passed the volume of incoming malicious traffic rose from a mere annoyance to an all-consuming electronic dissonance. The Internet connection grew ever less responsive, degrading steadily until the university was cut off from the world.

"It became pretty terrifying to realize how many machines had to be involved. It seemed like hundreds."

Investigators later determined that 2,200 computer systems, including those at more than 30 universities in the United States, had become unwitting "zombies," serving a still unidentified master computer, which directed the attacks and forced the university off the Internet for two days.

In a matter of weeks after the Minnesota incident, academics and elite computer security firms began spreading the word to clients and colleagues that this newly enhanced "denial of service" (DoS) attack was a clear and immediate danger to the Internet.

But it would take more than a month before federal officials at the National Infrastructure Protection Center (NIPC), which is responsible for national computer security matters, to learn of the incident and three more months for them to conclude that it was a threat worthy of a warning to the public.

It is now apparent that throughout the end of 1999, cybervandals were infecting large, insufficiently secured computer systems as zombies and laying the groundwork for a series of attacks last month that rocked e-commerce.

The delayed response and limited distribution of threat information is one of several criticisms being leveled at the NIPC and its sister agencies as the investigation into the attacks progresses slowly, according to recent congressional testimony.

"It was not enough," says Jamie Gorelick, the former deputy attorney general, who from 1994 to 1997 directed the administration's creation of the current electronic defense policy.

Please see COVER STORY next page ▶

COVER STORY

Agencies defend their response

Continued from 1A

She and others say the protection center failed, leaving many e-commerce firms unprepared for the attacks Feb. 8-11 that slowed the global Internet by 20% and shut down the world's most popular commercial Web sites and the FBI's home page.

"There needs to be some agile operational capacity in the government, an ability to move quickly to provide warnings," she says. "This doesn't sound at all like what we had in mind."

Michael Vatis, director of the NIPC, an interagency fusion of federal, local and international organizations based at the FBI, defends his agency's response. It says it permitted the private sector to prepare for the worst while avoiding public hysteria.

"Three years ago we wouldn't have been able to respond at all," Vatis says. "Today we have an effective resource" for investigating crimes and issuing threat alerts.

Critics say the protection center and its sister agencies have fallen short of the vision President Clinton had two years ago when he issued a plan to "create a genuine public-private partnership to protect America in the 21st century' from devastating cyberattacks. The plan called for the private sector, which owns and operates both the Internet and the infrastructure that supports it — electricity, banking and communications — to create secure information-sharing centers in which companies could anonymously share threat information, new vulnerabilities and crises data. It also created a Commerce Department coordinating center to work with those industry clearinghouses and the NIPC.

But as the administration seeks $37 million in new spending for cybersecurity, the NIPC and its sister agencies are troubled by confusion within their own ranks as well as a lack of cooperation from companies and other government agencies:

▶ Other government agencies are refusing to work with the NIPC, privately pointing to the FBI's longstanding reputation for not sharing well with others. "That's something we're still working on," Vatis says.

The Pentagon is the only Cabinet-level agency represented at the NIPC. The Secret Service, Transportation Department and Treasury Department, each of which is designated to have representation at the protection center, refuse to take part. The Department of Energy, which is supposed to play a major role at the center, is not represented. The CIA, which has four slots at the center, has filled one.

> "There needs to be some agile operational capacity in the government, an ability to move quickly to provide warnings. This (last incident) doesn't sound at all like what we had in mind."
>
> — Jamie Gorelick, former deputy attorney general

▶ Friction and turf battles between the new cybersecurity agencies may be hampering operations. The National Coordinator for infrastructure protection and counterterrorism is Richard Clarke, a White House official, who must get clearance on a case-by-case basis before the NIPC will brief him about investigations.

Vatis says Justice Department guidelines bar the FBI from briefing anyone outside the department about ongoing cases unless the attorney general grants a waiver.

▶ The Internet community is demanding broader distribution of more timely threat in-

their compute[illegible] attack "zombies."

On Dec. 8 [illegible]IPC sent a note briefing FBI Director Louis Freeh for the first time. On Dec. 17, Vatis personally briefed Attorney General Janet Reno as part of an overview of preparations being made for Y2K.

By that point, several DoS attacks already had occurred, but "people weren't getting the message," Dittrich says. "CERT and NIPC were really worried. They had obviously been hearing about a lot more intrusions. They went back and recategorized a whole bunch of incident reports going back to April-May time frame, and they started telling me that this is a really big thing."

But not until the NIPC, working with Dittrich and Mitre Corp., developed a tool for identifying zombies in a system did the protection center decide to warn the public Dec. 30 and post the tool for anyone to download.

By that time, Vatis says, "someone was setting the groundwork for an attack, and that is when we decided to make a public announcement."

Electronic 'night of the living dead'

The NIPC was convinced that New Year's Eve "could be a day for people to start sending marching orders to these zombies. We were afraid that Dec. 31 might become the night of the living dead," he says.

"Thanks for giving us plenty of time to prepare," says a sarcastic Vinton Cerf, an MCI WorldCom executive who is widely regarded as a founder of the Internet. "The timing of this all was singularly unfortunate."

But the protection center gets high praise from many security firms for being the first to provide an effective tool to locate and remove the zombie infections. Vatis says far more damage would have occurred in February otherwise.

"You know, I'm sensing a little bit of doublespeak here," Vatis says. "Business is saying, 'We don't want the government telling us what to do; we can fix this ourselves.' And I agree. But then I hear people saying, 'Gosh, government didn't warn us loud enough.' "

"People have been saying for a long time that it's going to take an electronic Pearl Harbor for people to take security seriously," he says. "There's a kernel of truth there because we live in an event-driven society."

deputy attorney general waiver.

▶ The Internet community is demanding broader distribution of more timely threat information, beyond the security professionals with whom the NIPC typically deals. "If you are only spreading the word to specialists, then you are not getting threat information out across the board to small universities or e-tailers," says Harris Miller of the Information Technology Association of America, a leading trade association representing 11,000 corporations.

▶ Though some companies are warming to the idea of sharing information with the government, many complain that they remain uneasy about government efforts to police the Internet.

"Where (the federal government) is completely failing is to be a place people trust" with delicate information, says Alan Pallar of the SANS Institute, an education facility for computer system administrators that claims 100,000 members. "Ninety-eight percent of the time they won't share with the FBI because they fear having their (computers) confiscated, that their troubles will become public knowledge and that the agents will scare (clients) to death."

▶ The president's plan has created so many entities gathering data on Internet vulnerabilities that it is causing confusion. "Imagine living in a community where there are seven different numbers to call for 911 services," says Mark Rasch, chief counsel to Global Integrity, a leading cybersecurity firm that hosts the financial industry's information sharing center. "You need to have one number, one place, that everyone trusts."

Adds Tom Noonan, CEO of Internet Security Systems, probably the fastest-growing firm in its field and a major booster of the NIPC: "Quite frankly, I'm confused by all these different government groups."

Word spreads slowly

In the days after the University of Minnesota attack, Haskell says her 911 instinct was to notify academic colleagues or other trusted computer professionals.

One of those she contacted was David Dittrich, director of software engineering at the University of Washington in Seattle. He became the first person to track down and unlock the codes that make the attacks operate.

It was a matter of days before he realized the new attack technique required immediate action. But the wheels of government turn slowly.

Dittrich first alerted CERT, the Computer Emergency Response Team at Carnegie-Mellon University, the nation's premier clearinghouse for data on computer vulnerability. By early September, it began organizing an unprecedented international conference to examine the emerging threat.

Based on CERT's letters of invitation to the conference, a handful of high-end security firms learned of the attack technique, and in October and November the firms quietly briefed clients about the impending threat.

Though the NIPC is a sponsor of CERT and has a liaison for the emergency response team on its staff, it received its first substantial report from CERT in late October. The response team has declined to comment on the apparent delay.

The three-day CERT conference in early November adjourned with this determination: "There is essentially nothing a site can do with currently available technology to prevent becoming a victim" of a denial-of-service attack.

The only prevention, the conferees said, was for system operators to update their security precautions to prevent vandals from exploiting known system weaknesses to gain control of

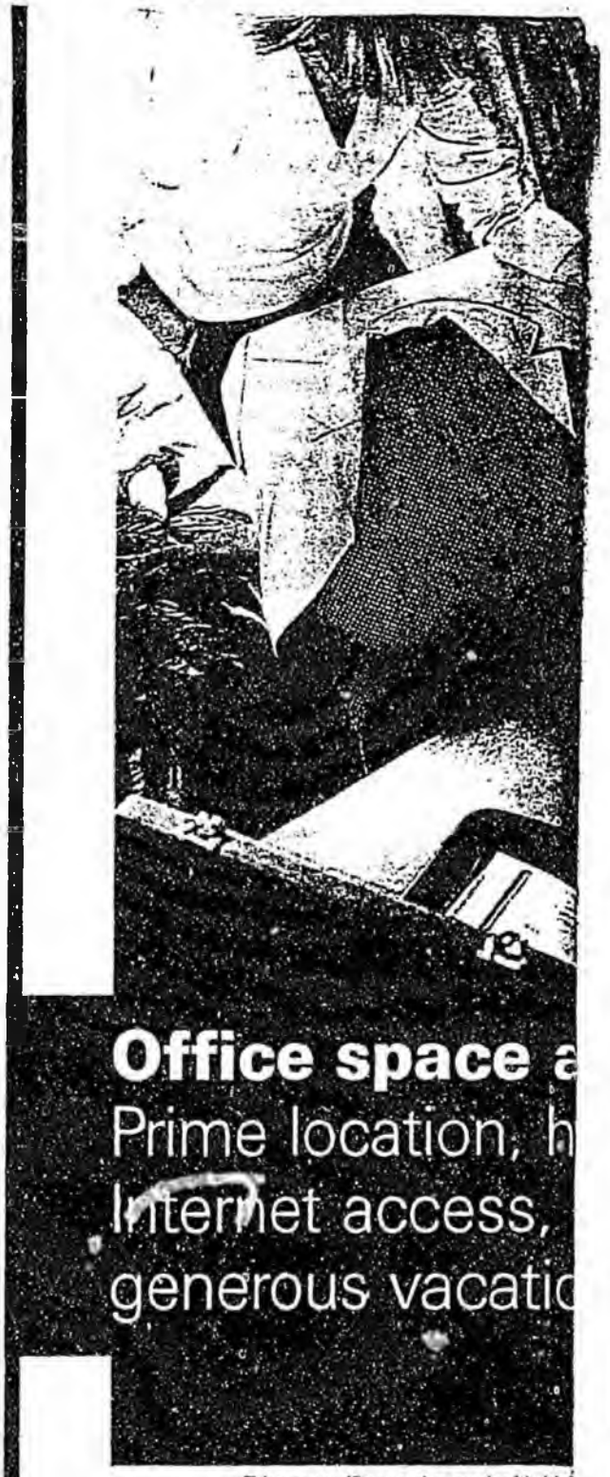
USA TODAY

Editorial and publication headquarters:
1000 Wilson Blvd., Arlington, VA 22229
Phone: 703-276-3400

Published by Gannett Co., Inc. Volume 18, No. 125 (ISSN 0734-7456)

Subscriptions and general information:
1-800-USA-0001
Hours: Mon. - Fri., 6:30 a.m. - 9 p.m. Eastern Time.
Subscription rates in the U.S.: 13 wks, $39; 26 wks, $78; 39 wks, $117; 52 wks, $156. Rates to foreign countries available. Send correspondence about subscriptions to Sheila Riggs, Director of National Customer Service, P.O. Box 4170, Silver Spring, Md. 20914. Fax subscription information: 1-800-732-3631
Deaf or hard of hearing with TTY equipment: 1-800-331-1706

Classified advertising: 1-800-USA-CLAS
All advertising published in USA TODAY is subject to the current applicable rate card, copies of which are available from the advertising department. USA TODAY may, in its sole discretion, edit, classify, reject or cancel at any time any advertising submitted by an advertiser.
National and Regional advertising: 1-800-242-5858
Reprint permissions, copies of articles, glossy reprints: 703-558-5619 Fax: 703-247-3139



Take your office on the road with hig

Closing the deal on the way to breakfast

Seattle Times 12 Nov 2000

Hackers' Web-site assaults take toll

Victims and experts call randomness frightening

JIMI LOTT / THE SEATTLE TIMES

Blaine Hadlock, *owner of Zebra Marketing Online Services, changed his business plan after a hacker attack.*

BY PETER LEWIS
Seattle Times technology reporter

Compared with a street mugging, an attack on a Web site lacks a certain reality. The "crime" seems thin, the consequences soft.

Tell that to Blaine Hadlock, owner of a small, Bainbridge Island-based business that got hacked last year, allegedly by a total stranger who turned out to be a computer-science student in Boston. When Hadlock finished picking up the pieces, the tab exceeded $30,000.

It is a phenomenon expected to grow worse before it improves, said Richard Power, spokesman for the Computer Security Institute, a San Francisco-based association of information security professionals.

"As the cybercrime problem grows, the smaller and medium-sized businesses will be more targeted for fraud or malicious mischief," predicted Power, "simply because there will be more sharks in the water interested in smaller prey."

What's particularly disturbing is the apparent randomness of such attacks. Hackers can use fairly simple scanning programs to hunt for vulnerable systems.

PLEASE SEE *Hack* ... D 2

After attack, victim takes his company out of harm's way

HACKERS

CONTINUED FROM D 1

"It did not put us out of business, but it stung real bad," recounted Hadlock, whose Zebra Marketing Online Services (ZMOS) has five full-time employees and has since moved to Federal Way. "You don't lose that kind of money without it hurting you. It caused me some significant problems."

Authorities contend the hacker is a Northeastern University student named Ikenna Iffih, who in federal charges filed recently in Boston was also accused of illegally entering federal computers at the National Aeronautics and Space Administration and the Defense Department.

Last spring, investigators with the FBI and the Department of Defense kept asking Hadlock, "Why you? Why him?"

And Hadlock had a stock answer: " 'Ask him (the hacker).'

"I really don't know from whence he came and why. I'd love to sit with him and ask 'Why?' "

Power, with the security institute, said the public often has difficulty understanding the motive behind such stranger-on-stranger cyber attacks. "People say, 'Well, why do they do this?' And the answer they can't understand is, 'Just because,' " Power said.

He said attacks on smaller businesses are particularly damaging because the owners cannot absorb the hit like a major corporation, and they generally lack insurance to cover such losses.

Assistant U.S. Attorney Steve Schroeder of Seattle, who helped investigate the ZMOS case, agrees.

"It's the smaller systems that can't afford to spend resources on security that are going to remain vulnerable," he said. "The little mom-and-pop sites. It (a hacker attack) would bury them."

Most of the hacking incidents Schroeder is aware of in Western Washington involve stranger-on-stranger attacks. Several remain under active investigation. But another threat comes from disgruntled employees.

That's what occurred to small-business owner Bud Robinson, who runs an ice-machine rental business called Automatic Ice Makers in San Diego. Two years ago, a disgruntled programmer "just walked out one day and said 'I'm going to own you,' " Robinson recalled.

Before leaving, the employee placed some malicious code in the system – a "logic bomb" that disabled access and caused about $50,000 in damage. It took nearly two years for Robinson to recover, repairing the system in stages as he could afford to.

James Crowell, aka Jamie Crowell, ultimately pleaded guilty to a felony charge of recklessly damaging a protected computer. Crowell was sentenced to serve six months in a halfway house and ordered to make restitution, among other conditions.

In Hadlock's case, the intrusion influenced him to shift business models. Instead of hosting other companies' Web pages, ZMOS now acts as an "e-business facilitator," Hadlock said, meaning the company helps e-businesses figure out what their message is and provides marketing assistance.

Besides being disruptive, Hadlock said the attack caused him to realize how legally vulnerable he was as the guardian of other people's information. If a Web-hosting company is housing "hundreds or thousands or millions of dollars' worth of (intellectual-property) investment and somebody (a hacker) gets to you, guess who is on the line?" Hadlock asked rhetorically.

"So we changed after this little scenario," he said. "It led us to not being in that (Web-hosting) business."

As far as prosecutors know, ZMOS was the most seriously damaged victim. Iffih's other alleged unauthorized forays caused no disruption to the nation's defenses, no meddling with satellite control, and no improper use of personal information – including private information on about 9,000 students, faculty and alumni at Northeastern that Iffih is accused of downloading and copying.

The 28-year-old student now faces three felony counts related to unauthorized access to various computers. If convicted, he could serve up to 15 years in prison and pay a $250,000 fine.

Iffih was charged by criminal information instead of indictment, which generally is a sign that a plea agreement is in the works.

Authorities have asserted that Iffih also went by the hacker name "DigiAlmty" and that he was responsible for defacing an Interior Department Web page. On that page, Iffih is accused of writing in part: "Yes, you guessed it right, the WAR is on. The (expletive) FBI vs. everyone who calls him-/herself a true hacker."

Peter Lewis: 206-464-2217. E-mail: plewis@seattletimes.com

"People say, 'Well, why do they do this?' And the answer they can't understand is, 'Just because.' "

RICHARD POWER

Spokesman, Computer Security Institute

Arch Daily News 12 Mar 2000

Cookies' maker chews over their fate

By THOMAS E. WEBER
The Wall Street Journal

Cookies, those tiny computer files that web sites use to track visitors, have come to symbolize the worst fears about on-line privacy. But the man who baked up the very first batch says that's just not fair.

"They're actually relatively harmless," said Lou Montulli, the computer whiz who invented cookies in 1994 and went on to be named "Sexiest Internet Mogul" by People magazine last year.

Montulli's brainchild has evolved into one of the Web's most pervasive technologies, invisibly shoring up everything from e-commerce to on-line advertising. If you spend much time on the Web, chances are you've accumulated anywhere from dozens to hundreds of cookies on your PC.

Lately Internet companies have figured out how to make them do all sorts of tricks their creator didn't foresee. On-line ad network DoubleClick has turned them into huge consumer dossiers, and now finds itself under scrutiny from consumers and the Federal Trade Commission for its efforts.

The tale of how and why the cookie came to be — and why it now arouses such fears among Internet users — is a dramatic example of how the on-line world has been shaped by the decisions of a few key people. It also shows how those decisions can morph in unintended ways as the Net evolves at breakneck speed.

In the summer of 1994, Montulli was a young college dropout at a brand-new company called Netscape. It wanted to commercialize the Internet, which meant making it possible for people to buy things on-line. The problem was, web sites made poor shopkeepers. Designed to treat all requests for information separately, sites couldn't perceive individual shoppers at the other end of the line. All they saw were flurries of unrelated queries.

That meant you couldn't mark items as you browsed for later purchase. Instead of paying for everything at once, consumers would have been forced to buy their CDs and books one at a time. The challenge for Montulli was to get a web site to see its users as distinct individuals so that it could remember things about them.

His answer was the cookie, a tiny computer file that could be stored on a user's PC. (Programmers had long used the term to refer to an arbitrary piece of data.) With a cookie, a web server essentially says: Here, hang on to this file and show it to me the next time you ask me something. It will remind me who you are and what we've already talked about.

Netscape built cookies into the first version of its browser, making them a de facto standard for the Web. Like any good programmer, Montulli designed cookies to be flexible. "Netscape was about building the infrastructure for the Web," he said. "We tried to build things that would be useful for the entire community."

Use it they did. When web sites began to run paid advertisements, advertisers wanted to know the size of the audience. Sites counted up "hits," but couldn't tell if 10 hits represented 10 different users or one person visiting 10 times. By assigning each visitor a unique cookie, sites could discern one visitor from another and make accurate tallies.

From there, it wasn't much of a leap to use cookies to track visitors' habits, noting things like which pages they visited most frequently. DoubleClick, which sells advertising on a network of sites, figured it could charge more for ads if they were targeted based on consumer behavior.

Now DoubleClick wants to go a step further, matching up cookie data with information in traditional direct-marketing data bases. Faced with a company that can potentially track where you surf and knows your mail-order shopping habits to boot, some consumers have started getting anxious. Earlier this month, DoubleClick disclosed that the FTC was examining its practices, which depend heavily on cookies.

Montulli, 29 years old, says DoubleClick and dozens of other web marketers are using cookies in ways he never intended. But he admits his design gave an unintended boost to tracking efforts. Here's why: When a web site displays a page you've requested, it can pull elements, including ads, from other sites. That allowed ad networks to put their own cookies on consumers' PCs and track them across many sites. Montulli later added to Netscape an option that lets users refuse cookies from sites other than the one they're visiting.

Efforts to reform cookies further haven't met with much success. After building cookies into Netscape Navigator, Montulli helped develop an official standard for the Internet Engineering Task Force.

The proposal calls for each cookie to include a description of its purpose so consumers could inspect their cookies and find out what they're up to.

The idea hasn't gotten very far. The fact is, it's too late to tinker with cookies now. They power practically every on-line shopping cart and every paid advertisement. In less than six years, they've become part of the fabric of the Web.

A lot has changed for Montulli in that time. Once the quintessential unkempt geek, he's now a Netscape millionaire with a steady girlfriend, a great haircut and stylish clothes. The People magazine story even compared him to hunky actor Dylan McDermott.

He's working at a buzzy start-up called Epinions.com, a shopping guide where visitors can read and post product reviews. Naturally, it uses cookies.

Technology creator warns of its threat to mankin

AON 13 mar 2000

By JOEL GARREAU
The Washington Post

A respected creator of the Information Age has written an extraordinary critique of accelerating technological change in which he suggests that new technology could cause "something like extinction" of humankind within the next two generations.

The alarming prediction, intended to be provocative, is striking because it comes not from a critic of technology but rather from a man who invented much of it: Bill Joy, chief scientist and co-founder of Sun Microsystems Inc., the leading web technology manufacturer.

Joy was an original co-chairman of a presidential commission on the future of information technology. His warning, he said in a telephone interview, is meant to be reminiscent of Albert Einstein's famous 1939 letter to President Roosevelt alerting him to the possibility of an atomic bomb.

In a 24-page article in the April issue of Wired magazine that hits stands today, Joy says he finds himself essentially agreeing, to his horror, with a core argument of the Unabomber, Theodore Kaczynski — that advanced technology threatens humans.

"I have always believed that making software more reliable, given its many uses, will make the world a safer and better place," Joy writes in the article, which he worked on f months. "If I were to come to b the opposite, then I would be m obligated to stop this work. I ca imagine that such a day may co

Joy enjoys a level-headed r tion in the industry.

"Nobody is more phlegmatic Bill," said Stewart Brand, an In pioneer. "He is the adult in the r

See Back Page, EXTIN

Anchorage Daily News

EXTINCTION: Exec varns of technology

Continued from Page A-1

Joy is disturbed by a suite advances. He views as redible the prediction that 2030, computers will be a illion times more powerful an they are today. He rejects the possibility that rots may exceed humans in ntelligence while being able replicate themselves.

He points to nanotechnoloy — the emerging science at seeks to create any dered object atom by atom — nd agrees that it has the poential to allow inexpensive roduction of smart machines so small they could fit iside a blood vessel. Genetic chnology, meanwhile, is inxorably generating the powr to create new forms of life at could reproduce.

What deeply worries him s that these technologies colectively create the ability to nleash self-replicating, muating, mechanical or biologial plagues. These would be a replication attack in the hysical world" comparable the replication attack in he virtual world that recenty caused the shutdowns of major commercial web sites.

"If you can let something ose that can make more opies of itself," Joy said, "it s very difficult to recall. It is s easy as eradicating all the osquitoes. They are everyhere and make more of hemselves. If attacked, they nutate and become immune. That creates the possibility f empowering individuals or extreme evil. If we don't o anything, the risk is very igh of one crazy person dog something very bad."

What further concerns im is the huge profits from y single advance that may em beneficial in itself.

"It is always hard to see the gger impact while you are in the vortex of a change," Joy wrote. "We have long been driven by the overarching desire to know that is the nature of science's quest, not stopping to notice that the progress to newer and more powerful technologies can take on a life of its own."

Finally, he argues, this threat to humanity is much greater than that of nuclear weapons because those are hard to build. By contrast, he says, these new technologies are not hard to come by. Therefore, he reasons, the problem will not be "rogue states but rogue individuals."

Joy's critique is striking because computer industry technologists, almost without exception, take a more sanguine view of the social consequences of advances. They typically argue that any negative effects will be far outweighed by the positive effect of new technologies.

Nathan Myhrvold, a physicist on leave from his job as the chief technology officer at Microsoft Corp., said in an e-mail interview: "People have made apocalyptic predictions about technology constantly for as long as there has been technology. I think it is because change frightens them." What is more, the most common form these dire predictions take is 'this next generation of stuff — wow! that is really different and really scary.'"

Asked if he thinks a technological species could expect to survive the accelerating evolution of its market-driven technologies, Joy said: "The answer is yes but not without additional care. I think it's possible but it's not a given. Survival won't come for free."

The New York Times contributed to this story.

USA TODAY CLASSIFIEDS AND MORE MARKETPLACE

The Nation's e-mail news to start your day. USATODAY.com
DAILYBRIEFING featuring News from around the globe.

SHOP AT MARKETPLACE

OnVia
All of your small business needs.
iTool
Build your own e-commerce site today.
Point.com
Cellular plans, phones and accessories.

USA TODAY Nation

02/13/00- Updated 11:59 PM ET

Web attacks raise concerns about growth

NEW YORK (AP) - A swarm of recent hacking attacks highlight one emerging concern about the Internet: It may be growing too fast for security to keep up with technology.

Some security experts believe it's time to focus on making the Net safer, which could mean rebuilding much of the underlying infrastructure from scratch. After all, consumers and businesses now use the Internet for tasks unforeseen 30 years ago.

Security was an afterthought when Internet standards were developed by university thinkers and computer administrators, says Russ Cooper, who runs the NTBugtraq Web site devoted to security.

"This is now the foundation for billions of dollars worth of commerce," Cooper said. "It is inherently flawed because we don't check to see if what it's being used for is what it is intended for."

Randy Sandone of Argus Systems Group Inc. is blunter: "The Web is rotten at its core."

Yahoo!, Buy.com, eBay, ETrade and other prominent sites were paralyzed for hours at a time last week when hackers overloaded them with fake traffic.

The attacks followed several computer virus outbreaks last year - such as Melissa - which spread rapidly by taking advantage of functions that were designed to make Internet use friendlier.

And last month, a hacker stole credit card numbers from the Internet music retailer CD Universe, then released thousands of them on a Web site after the firm refused to pay $100,000 ransom.

"I fully expect the Internet to ultimately be safe and stable," said Stephen Gorrell, program manager for Norton Internet Security

Find books up to 50% off BARNES&NOBLE

Resources
E-mail
Index
Feedback
What's hot
About us
Jobs at USA TODAY

Free premiums
USA TODAY Update
Software

CLICK HERE for.... USA TODAY.com MOMENTS IN BLACK HISTORY

software. "However, in the period of record growth, it's not surprising new holes are discovered."

The Internet's developers could not have effectively countered threats to commerce because e-businesses did not yet exist, Gorrell said.

As the Internet grows, so do the numbers of hackers and potential victims. And hackers are becoming more sophisticated, with some even developing tools to automate their attacks.

Software companies, some critics say, contribute to the problems by releasing products that still have security holes.

"Each day, technology is changing," said Robert Ing, who handles electronic security for SBR International Inc. in Toronto. "There's a rush to get products out to market because it is a competitive marketplace. Sometimes, security is overlooked."

Steve Hunt, security analyst at Giga Information Group in Chicago, hopes the latest attacks will encourage companies to take security more seriously.

"We owe quite a debt of gratitude to hackers to show us where our pants have been down," he said.

Security and Internet experts differ on how far they need to go - and that itself is a problem. Some believe in completely updating equipment and software to reduce users' anonymity and improve authentication.

In the offline world, businesses have experience with security guards and special locks. Some practices are even required by law or insurance companies.

But the Internet community has yet to agree on such standards, said Harris Miller, president of the Information Technology Association of America.

Phil Attfield, director of technical marketing at McAfee.com, said Internet security will eventually catch up.

"The approaches are going to have to become more formal rather than ad hoc," he said. "We've been getting there incrementally. That's the way technology is evolving."

But hacking will never completely disappear, said Keith Teare, the chairman and chief executive of RealNames. Vandals broke into RealNames' computers Wednesday, and the company had to warn some 20,000 customers that their credit card numbers might have been stolen.

"For every secure environment, there will be somebody prepared to try to break in," Teare said. "If they are clever enough, they will find holes."

Greg Hawkins, chief executive of Buy.com, said the attacks on his shopping site and others raised awareness.

"This is a new frontier. It's big, it's fast, and it's growing rapidly," he said. "With that growth will come continued challenges to make sure it's a secure and effective environment. We are clearly going to have growing pains like this from time to time."

- Go to Nationline
- Go to News front page

Quick checkup: CLICK HERE! HOW HEALTHY ARE YOU? USA TODAY.com

Front page. News. Sports. Money. Life. Weather. Marketplace

© Copyright 2000 USA TODAY, a division of Gannett Co. Inc.

You get 8 seconds
to keep a customer online. GO
intel

NEWS & VIEWS
Financial News
@ Net Index
Web Reviews
Columnists
ZDNN News

RESOURCES
Subscription Info
Downloads
Industry Events
Recruitment
Ad Marketplace
Ad Index
Forums

ABOUT US
General Info
Masthead
Edit Calendar
Contact Us
Copyright

NETdelivery Delivers!
PC ZD Magazines

Inter@ctive Week April 20, 1998

ISP Posts Blacklist Of Smurf-Friendly Networks

By Randy Barrett

One Chicago-based Internet service provider is blocking more than 40 Internet networks from its access system, until they stop allowing hackers to use bandwidth for "smurf" attacks.

Macro Computer Solutions Inc. (www.mcs.net) owner Karl Denninger posted a notice April 11 on the North American Network Operators Group e-mail list stating he was fed up with smurf attacks and would no longer exchange traffic with networks that originated the assaults.

"I'm going to start posting the blacklist here weekly in the hopes that peer pressure will cause people to clean up their acts," Denninger wrote.

Denninger listed the Internet Protocol addresses -- but not names -- of 30 networks and has added 12 more since. Most are larger Internet providers and academic networks, he said.

For network administrators, being a collaborator in a smurf attack means doing nothing at all. The attacks are often aimed at Internet Relay Chat servers or the Internet service providers (ISPs) that host them. Johnny Hacker typically gets mad at Betty Hacker during a chat session and tries to knock her offline by burning down her provider. All the assault requires is a basic Internet account.

Here's how it works: Johnny Hacker sends a stream of diagnostic "ping" messages to a second-party network's host servers. Many of those servers are set to automatically respond, but Johnny places a false return address and those responses stream to a third-party ISP that is really the target of the assault. So a single ping stream is amplified hundreds or thousands of times and clogs the target network's bandwidth -- particularly smaller providers using a single T1 (1.5-million-bit-per-second) line.

The fix is simple, Denninger said: Networks must turn off the "directed broadcast forwarding" function in their routers, and the ping responses will never be sent.

"Some of them honestly don't know about it. My response is, I'll deny you access to my network until you get your act together," he said.

Denninger's smurf amplifier blacklist is getting some support from network

administrators, but it is unclear whether any are using it to block errant networks or might be compiling their own rogues' gallery.

Jason Weisberger, chief of network operations at SoftAware Inc. in Marina del Rey, Calif., said he's not interested because a blacklist limits his own customers' connectivity. "Punitive filtering, while a good short-term fix, can create problems farther out," he said.

Denninger has been similarly zealous about the Enhanced Domain Name System (www.edns.net), an alternative to InterNIC, which splintered last fall and is now in limbo.

Sponsored Links

NextCard VISA: As low as 9.9% Fixed APR and no hidden fees!
800.COM **Digital cameras priced from $99.94**
Netpliance Discover the new one-button-access Internet Appliance
News Flash **Tiny Video Camera, Color & Sound Only $79.99 - X10.com!**
Books Save on taxes! Learn how at barnesandnoble.com!
Great PCs Buy your Dream PC at Micronpc.com. Click here!

ZDNet Featured Links

Downloads Top 50 **FREE** files - utilities, games, Internet & more
NEW! Shop the Outlet Store for **best buys** on computer products
Bargains Shop and save with **FREE** digital coupons and **special offers!**

Magazine Offers

Click Here Apply for a **FREE subscription to Sm@rt Reseller**

ZDNet Reviews | News | Downloads | Shop | MyZDNet | Games | ZDTV | Forums
AnchorDesk | PC Magazine | PC Week | Help! | Yahoo! Internet Life
HOME | FREE MEMBERSHIP | CONTACT ZD | AD INFO | ZIFF-DAVIS

Copyright (c) 1998 Ziff Davis, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission of Ziff Davis, Inc. is prohibited. Inter@ctive Week and the Inter@ctive Week logo are trademarks of Ziff Davis, Inc.

Welcome to the Office of Senator Frank Murkowski

Inbox Privacy Act

ALASKA HOME

ALASKA CONSTITUENT RESOURCES

ALASKA LEGISLATIVE RESOURCES

ALASKA ALASKA RESOURCES

ALASKA PRESS RESOURCES

ALASKA INTERNET ISSUES

ALASKA CONTACTING ME

For Immediate Release

ANTI-SPAM BILL INTRODUCED TO SOLVE A NATIONAL INTERNET PROBLEM

WASHINGTON -- Senators Frank Murkowski (R-AK), Robert Torricelli (D-NJ), Conrad Burns (R-MT), and Harry Reid (D-NV) today introduced the Inbox Privacy Act to address the growing concerns of Internet consumers over the issue of junk email, or spam.

"Internet consumers nationwide have been speaking out against the growing flood of unwanted and fraudulent e-mails in the inboxes. It's time that we had a nationwide solution to this problem. E-mail shouldn't be a way for every huckster to sell the Brooklyn Bridge," Murkowski noted.

Senator Torricelli added, "Accessing the Internet should not be an invitation for every shyster in the world to beat down your door with junk e-mail. American consumers deserve a level of privacy and protection and our legislation provides it to them."

Junk e-mail burdens Internet consumers by shifting delivery costs onto consumers, particularly in rural areas like Alaska where a connection to the Internet often requires a long distance call.

The Inbox Privacy Act would require e-mail marketers to honestly identify themselves, honor consumer remove requests, and allow Internet domain owners to set up electronic "stop signs" to give domain owners the ability to block unwanted solicitations. In order to allow the Internet consumer to have the ultimate choice, unsolicited e-mails could be sent to those who still wish to receive such solicitations. Internet Service Providers, state attorney generals, and the Federal Trade Commission would have the authority to seek up to $50,000 per day in damages.

The legislation has been referred to the Senate Commerce Committee where hearings will be held later this year. Similar legislation was passed by the Senate in the 105th Congress by a vote of 99-0 although a final conference

between the House and Senate could not be scheduled prior to adjournment.

Senator Torricelli also noted that "Our legislation continues to allow legitimate uses of e-mail, but empowers consumers and Internet service providers to eliminate the unwanted e-mail they receive."

Comments on the bill can be made to spamfree@murkowski.senate.gov .

106TH CONGRESS
1ST SESSION

S. 759

To regulate the transmission of unsolicited commercial electronic mail on the Internet, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MARCH 25, 1999

Mr. MURKOWSKI (for himself, Mr. TORRICELLI, Mr. BURNS, and Mr. REID) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To regulate the transmission of unsolicited commercial electronic mail on the Internet, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Inbox Privacy Act of 1999".

SEC. 2. TRANSMISSIONS OF UNSOLICITED COMMERCIAL ELECTRONIC MAIL.

(a) PROHIBITION ON TRANSMISSION TO PERSONS DECLINING RECEIPT.—

(1) IN GENERAL.—A person may not initiate the transmission of unsolicited commercial electronic mail to another person if such other person submits to the person a request that the initiation of the transmission of such mail by the person to such other person not occur.

(2) FORM OF REQUEST.—A request under paragraph (1) may take any form appropriate to notify a person who initiates the transmission of unsolicited commercial electronic mail of the request, including an appropriate reply to a notice specified in subsection (d)(2).

(3) CONSTRUCTIVE AUTHORIZATION.—

(A) IN GENERAL.—Subject to subparagraph (B), for purposes of this subsection, a person who secures a good or service from, or otherwise responds electronically to an offer in a commercial electronic mail message shall be deemed to have authorized the initiation of transmissions of unsolicited commercial electronic mail from the person who initiated transmission of the message.

(B) NO AUTHORIZATION FOR REQUEST FOR TERMINATION.—A reply to a notice specified in subsection (d)(2) shall not constitute au-

thorization for the initiation of transmissions of unsolicited commercial electronic mail under this paragraph.

(b) PROHIBITION ON TRANSMISSION TO DOMAIN OWNERS DECLINING RECEIPT.—

(1) IN GENERAL.—Except as provided in paragraph (2), a person may not initiate the transmission of unsolicited commercial electronic mail to any electronic mail addresses served by a domain if the domain owner has elected not to receive transmissions of such mail at the domain in accordance with subsection (c).

(2) EXCEPTIONS.—The prohibition in paragraph (1) shall not apply in the case of the following:

(A) A domain owner initiating transmissions of commercial electronic mail to its own domain.

(B) Any customer of an Internet service provider or interactive computer service provider included on a list under subsection (c)(3)(C).

(c) DOMAIN-WIDE OPT-OUT SYSTEM.—

(1) IN GENERAL.—A domain owner may elect not to receive transmissions of unsolicited commercial electronic mail at its own domain.

(2) NOTICE OF ELECTION.—A domain owner making an election under this subsection shall—

(A) notify the Federal Trade Commission of the election in such form and manner as the Commission shall require for purposes of section 4(c); and

(B) if the domain owner is an Internet service provider or interactive computer service provider, notify the customers of its Internet service or interactive computer service, as the case may be, in such manner as the provider customarily employs for notifying such customers of matters relating to such service, of—

(i) the election; and

(ii) the authority of the customers to make the election provided for under paragraph (3).

(3) CUSTOMER ELECTION TO CONTINUE RECEIPT OF MAIL.—

(A) ELECTION.—Any customer of an Internet service provider or interactive computer service provider receiving a notice under

paragraph (2)(B) may elect to continue to receive transmissions of unsolicited commercial electronic mail through the domain covered by the notice, notwithstanding the election of the Internet service provider or interactive computer service provider under paragraph (1) to which the notice applies.

(B) TRANSMITTAL OF MAIL.—An Internet service provider or interactive computer service provider may not impose or collect any fee for the receipt of unsolicited commercial electronic mail under this paragraph (other than the usual and customary fee imposed and collected for the receipt of commercial electronic mail by its customers) or otherwise discriminate against a customer for the receipt of such mail under this paragraph.

(C) LIST OF CUSTOMERS MAKING ELECTION.—

(i) REQUIREMENT.—An Internet service provider or interactive computer service provider shall maintain a list of each of its current customers who have made an election under subparagraph (A).

(ii) AVAILABILITY OF LIST.—Each such provider shall make such list available to the public in such form and manner as the Commission shall require for purposes of section 4(c).

(iii) PROHIBITION ON FEE.—A provider may not impose or collect any fee in connection with any action taken under this subparagraph.

(d) INFORMATION TO BE INCLUDED IN ALL TRANSMISSIONS.—A person initiating the transmission of any unsolicited commercial electronic mail message shall include in the body of such message the following information:

(1) The name, physical address, electronic mail address, and telephone number of the person.

(2) A clear and obvious notice that the person will cease further transmissions of commercial electronic mail to the recipient of the message at no cost to that recipient upon the transmittal by that recipient to the person, at the electronic mail address from which transmission of the message was initiated, of an electronic mail message containing the word "remove" in the subject line.

(e) ROUTING INFORMATION.—A person initiating the transmission of any commercial electronic mail message shall ensure that all Internet routing information contained in or accompanying such message is accurate, valid according to the prevailing standards for Internet protocols, and accurately reflects the routing of such message.

SEC. 3. DECEPTIVE ACTS OR PRACTICES IN CONNECTION WITH SALE OF GOODS OR SERVICES OVER THE INTERNET.

(a) AUTHORITY TO REGULATE.—

(1) IN GENERAL.—The Federal Trade Commission may prescribe rules for purposes of defining and prohibiting deceptive acts or practices in connection with the promotion, advertisement, offering for sale, or sale of goods or services on or by means of the Internet.

(2) COMMERCIAL ELECTRONIC MAIL.—The rules under paragraph (1) may contain specific provisions addressing deceptive acts or practices in the initiation, transmission, or receipt of commercial electronic mail.

(3) NATURE OF VIOLATION.—The rules under paragraph (1) shall treat any violation of such rules as a violation of a rule under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a), relat-

ing to unfair or deceptive acts or practices affecting commerce.

(b) PRESCRIPTION.—Section 553 of title 5, United States Code, shall apply to the prescription of any rules under subsection (a).

SEC. 4. FEDERAL TRADE COMMISSION ACTIVITIES WITH RESPECT TO UNSOLICITED COMMERCIAL ELECTRONIC MAIL.

(a) INVESTIGATION.—

(1) IN GENERAL.—Subject to paragraph (2), upon notice of an alleged violation of a provision of section 2, the Federal Trade Commission may conduct an investigation in order to determine whether or not the violation occurred.

(2) LIMITATION.—The Commission may not undertake an investigation of an alleged violation under paragraph (1) more than 2 years after the date of the alleged violation.

(3) RECEIPT OF NOTICES.—The Commission shall provide for appropriate means of receiving notices under paragraph (1). Such means shall include an Internet web page on the World Wide Web that the Commission maintains for that purpose.

(b) ENFORCEMENT POWERS.—If as a result of an investigation under subsection (a) the Commission deter-

mines that a violation of a provision of section 2 has occurred, the Commission shall have the power to enforce such provision as if such violation were a violation of a rule prescribed under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a), relating to unfair or deceptive acts or practices affecting commerce.

(c) INFORMATION ON ELECTIONS UNDER DOMAIN-WIDE OPT-OUT SYSTEM.—

(1) INITIAL SITE FOR INFORMATION.—The Commission shall establish and maintain an Internet web page on the World Wide Web containing information sufficient to make known to the public for purposes of section 2 the domain owners who have made an election under subsection (c)(1) of that section and the persons who have made an election under subsection (c)(3) of that section.

(2) ALTERNATIVE SITE.—The Commission may from time to time select another means of making known to the public the information specified in paragraph (1). Any such selection shall be made in consultation with the members of the Internet community.

(d) ASSISTANCE OF OTHER FEDERAL AGENCIES.—Other Federal departments and agencies may, upon re-

quest of the Commission, assist the Commission in carrying out activities under this section.

SEC. 5. ACTIONS BY STATES.

(a) IN GENERAL.—Whenever the attorney general of a State has reason to believe that the interests of the residents of the State have been or are being threatened or adversely affected because any person is engaging in a pattern or practice of the transmission of electronic mail in violation of a provision of section 2, or of any rule prescribed pursuant to section 3, the State, as parens patriae, may bring a civil action on behalf of its residents to enjoin such transmission, to enforce compliance with such provision or rule, to obtain damages or other compensation on behalf of its residents, or to obtain such further and other relief as the court considers appropriate.

(b) NOTICE TO COMMISSION.—

(1) NOTICE.—The State shall serve prior written notice of any civil action under this section on the Federal Trade Commission and provide the Commission with a copy of its complaint, except that if it is not feasible for the State to provide such prior notice, the State shall serve written notice immediately after instituting such action.

(2) RIGHTS OF COMMISSION.—On receiving a notice with respect to a civil action under paragraph (1), the Commission shall have the right—

(A) to intervene in the action;

(B) upon so intervening, to be heard in all matters arising therein; and

(C) to file petitions for appeal.

(c) ACTIONS BY COMMISSION.—Whenever a civil action has been instituted by or on behalf of the Commission for violation of a provision of section 2, or of any rule prescribed pursuant to section 3, no State may, during the pendency of such action, institute a civil action under this section against any defendant named in the complaint in such action for violation of any provision or rule as alleged in the complaint.

(d) CONSTRUCTION.—For purposes of bringing a civil action under subsection (a), nothing in this section shall prevent an attorney general from exercising the powers conferred on the attorney general by the laws of the State concerned to conduct investigations or to administer oaths or affirmations or to compel the attendance of witnesses or the production of documentary or other evidence.

(e) VENUE; SERVICE OF PROCESS.—Any civil action brought under subsection (a) in a district court of the United States may be brought in the district in which the

defendant is found, is an inhabitant, or transacts business or wherever venue is proper under section 1391 of title 28, United States Code. Process in such an action may be served in any district in which the defendant is an inhabitant or in which the defendant may be found.

(f) DEFINITIONS.—In this section:

(1) ATTORNEY GENERAL.—The term "attorney general" means the chief legal officer of a State.

(2) STATE.—The term "State" means any State of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, the United States Virgin Islands, the Commonwealth of the Northern Mariana Islands, the Republic of the Marshall Islands, the Federated States of Micronesia, the Republic of Palau, and any possession of the United States.

SEC. 6. ACTIONS BY INTERNET SERVICE PROVIDERS AND INTERACTIVE COMPUTER SERVICE PROVIDERS.

(a) ACTIONS AUTHORIZED.—In addition to any other remedies available under any other provision of law, any Internet service provider or interactive computer service provider adversely affected by a violation of section 2(b)(1) may, within 1 year after discovery of the violation,

bring a civil action in a district court of the United States against a person who violates such section.

(b) RELIEF.—

(1) IN GENERAL.—An action may be brought under subsection (a) to enjoin a violation referred to in that subsection, to enforce compliance with the provision referred to in that subsection, to obtain damages as specified in paragraph (2), or to obtain such further and other relief as the court considers appropriate.

(2) DAMAGES.—

(A) IN GENERAL.—The amount of damages in an action under this section for a violation specified in subsection (a) may not exceed $50,000 per day in which electronic mail constituting such violation was received.

(B) RELATIONSHIP TO OTHER DAMAGES.—Damages awarded under this subsection for a violation under subsection (a) are in addition to any other damages awardable for the violation under any other provision of law.

(C) COST AND FEES.—The court may, in issuing any final order in any action brought under subsection (a), award costs of suit, reasonable costs of obtaining service of process,

reasonable attorney fees, and expert witness fees for the prevailing party.

(c) VENUE; SERVICE OF PROCESS.—Any civil action brought under subsection (a) in a district court of the United States may be brought in the district in which the defendant or in which the Internet service provider or interactive computer service provider is located, is an inhabitant, or transacts business or wherever venue is proper under section 1391 of title 28, United States Code. Process in such an action may be served in any district in which the defendant is an inhabitant or in which the defendant may be found.

SEC. 7. PREEMPTION.

This Act preempts any State or local laws regarding the transmission or receipt of commercial electronic mail.

SEC. 8. DEFINITIONS.

In this Act:

(1) COMMERCIAL ELECTRONIC MAIL.—The term "commercial electronic mail" means any electronic mail or similar message whose primary purpose is to initiate a commercial transaction, not including messages sent by persons to others with whom they have a prior business relationship.

(2) INITIATE THE TRANSMISSION.—

(A) IN GENERAL.—The term "initiate the transmission", in the case of an electronic mail message, means to originate the electronic mail message.

(B) EXCLUSION.—Such term does not include any intervening action to relay, handle, or otherwise retransmit an electronic mail message, unless such action is carried out in intentional violation of a provision of section 2.

(3) INTERACTIVE COMPUTER SERVICE PROVIDER.—The term "interactive computer service provider" means a provider of an interactive computer service (as that term is defined in section 230(e)(2) of the Communications Act of 1934 (47 U.S.C. 230(e)(2)).

(4) INTERNET.—The term "Internet" has the meaning given that term in section 230(e)(1) of the Communications Act of 1934 (47 U.S.C. 230(e)(1)).

○