

***EMBARGOED FOR RELEASE AT 6:30 PM EASTERN  
MONDAY, APRIL 2, 2001***

**Fear of Online Crime:**  
*Americans support FBI interception of  
criminal suspects' email and  
new laws to protect online privacy*

**By Susannah Fox, director of research  
Oliver Lewis, research assistant**

**Pew Internet & American Life Project  
1100 Connecticut Ave. NW  
Suite 710  
Washington, D.C. 20036  
202-296-0019  
<http://www.pewinternet.org/>**

## **Summary of findings**

Americans are deeply worried about criminal activity on the Internet, and their revulsion at child pornography is by far their biggest fear. Some 92% of Americans say they are concerned about child pornography on the Internet and 50% of Americans cite child porn as the single most heinous crime that takes place online.

In other areas, 87% of Americans say they are concerned about credit card theft online; 82% are concerned about how organized terrorists can wreak havoc with Internet tools; 80% fear that the Internet can be used to commit wide scale fraud; 78% fear hackers getting access to government computer networks; 76% fear hackers getting access to business networks; and 70% are anxious about criminals or pranksters sending out computer viruses that alter or wipe out personal computer files.

These concerns may be a factor in the public's support of the right of the FBI and other law enforcement agencies to intercept criminal suspects' email. Some 54% of Americans approve of the idea of FBI monitoring of suspects' email, while 34% disapprove. There is equal public support of the FBI monitoring of email, phone calls, and postal mail.

The overall public anxiety about online crime occurs at the same time that Americans express growing distrust of the government. Only 31% of Americans say they trust the government to do the right thing most of the time or all of the time. That figure is down from 41% in 1988.

So, it is perhaps not very surprising that while Americans express a willingness to let law enforcement agencies intercept suspects' email, they also support the general idea that new laws should be written to cover how law enforcement agencies monitor email. Just 14% of Americans say the laws that relate to intercepting telephone calls are good enough to cover Internet communications. Fully 62% of Americans say new laws should be written to make sure that ordinary citizens' privacy is protected from government agencies.

Among the relatively small number of Americans who have heard about the FBI's email sniffing program called "Carnivore" or "DCS1000," there is much more evenly divided opinion. Forty-five percent of people who have heard of it say Carnivore is good because it will allow the FBI a new way of tracking down criminals. Another 45% say Carnivore is bad because it could be used to read emails to and from ordinary citizens.

The results cited here are based on a survey of 2,096 American adults that was conducted between February 1 and March 1. Some 1,198 of the respondents are Internet users.

***Introduction: The Carnivore controversy***

In July 2000, the *Wall Street Journal* reported that the FBI had developed a computer system that can intercept a criminal suspect's Internet activities. The capabilities of the new system and its original name, "Carnivore," helped spark controversy about its potential as an "email wiretap" and potential method to monitor citizens' email and online activities. FBI officials say Carnivore is a rarely used, but vital, surveillance device, especially because a growing number of criminals are using the Internet to communicate and using it to commit crimes online. In March 2001, for example, FBI officials estimated that criminal hackers in Russia and the Ukraine have stolen over one million credit card numbers. Officials also say that terrorist groups and organized crime gangs are now using the Internet to communicate with far-flung compatriots.

Only the FBI has access to the software governing this digital collection system, which is now called "DCS1000." Law enforcement officials argue that such secrecy is necessary because if the source code were public, criminals could figure out how to trick the system. Civil libertarians and some lawmakers think there should be more oversight when it comes to Internet surveillance, arguing that the government could use it to infringe on citizens' Fourth Amendment right to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

Some advocates of new laws for Internet surveillance have called for special safeguards against abuse of the digital collection system's power. The critics point out that DCS1000 is capable of archiving a broad swath of data that is irrelevant to the investigation at hand, such as the Web-surfing habits of every customer on an Internet Service Provider's network. The FBI says DCS1000 can be highly customized to capture only narrowly proscribed details of a suspect's email traffic.

DCS1000, like all wiretapping devices, can only be used under a court order. Different laws and standards apply depending on whether a wiretap is used for obtaining the actual content of communications or just for the addressing information, like the numbers dialed from a telephone or the "To" and "From" lines of email. But some critics contend that the telephone-era distinction between content and addressing information applies poorly to the Internet, since the technology is so different. A "pen register" (the least intrusive form of telephone wiretap) captures the numbers dialed on a certain telephone line, but not the conversation. But no matter what it ultimately filters out, a "packet analyzer" like DCS1000 must initially capture both the sender/receiver information *and* the contents of each message because all the information is bound up as a unit. Moreover, a packet analyzer cannot restrict its search to just one user's activities. Everyone's packets are jumbled together and must be filtered by the software.

***Two sentiments at war with each other: Government isn't trustworthy, but crime must be fought***

The Pew Internet & American Life Project tested public sentiment on these controversies in its February tracking poll. Two contradictory views emerged: The first is that many Americans do not trust their government and its agencies very much. Just 31% of all Americans think that the federal government can be trusted to do what is right at least

## Pew Internet Tracking Report

most of the time, compared to 39% who said that in 1997, and 41% who said that in 1988.

Who doesn't trust government <i>The percentage of each group who say they trust the government "only some of the time" or "never":</i>	
All Americans	62%
Men	60
Women	64
Whites	61
Blacks	73
Hispanics	54
High school graduates	66
College graduates	60

*Source: Pew Internet & American Life Project Survey, February 2001. Margin of error is ± 2%.*

In contrast, 62% of Americans said in the current survey they could trust the government only some of the time. That figure has risen from the 56% who expressed distrustful views of the government in 1988, and there was a period through the mid-1990s when it rose above 70%.

Young people, Hispanics, and those with more education are relatively more likely than their counterparts to trust the government. Republicans are more likely than Democrats or Independents to trust the government. Thirty-six percent of Republicans say the government can be trusted to do what is right at least most of the time, compared to 31% of Democrats and just 22% of Independents.

Those most likely to say they do not trust the government also include African-Americans and those with educational attainment of a high school diploma or less.

Yet the second strong strain of opinion is that Americans are quite willing to grant to law enforcement agencies and the FBI the right to intercept the email of criminal suspects, perhaps because Americans are concerned about crime, especially new ways to perpetrate crime using the Internet.

Fully 73% of all Americans are concerned about criminals using the Internet to plan and carry out crimes and 43% of all Americans are "very concerned." Women, African-Americans and those with less educational attainment are more likely than their counterparts to be very concerned about Internet crime.

Americans who do not go online are more likely than Internet users to register concern about nefarious uses of the Internet. One in two (52%) non-users say they are very concerned, compared to one in three (34%) Internet users. Fifty percent of online newcomers (those with six months of online experience or less) are very concerned, compared to 29% of online veterans (those with three or more years of experience).

Who fears Internet crime <i>The percentage of each group who say they are "very concerned" about crime online:</i>	
All Americans	43%
Men	35
Women	50
Whites	40
Blacks	56
Hispanics	48
High school graduates	49
College graduates	31

*Source: Pew Internet & American Life Project Survey, February 2001. Margin of error is ± 2%.*

Possibly because their fears are so strong, Americans are just as willing to have criminal suspects' emails tracked as they are to have suspects' phone calls or mail intercepted.

## Pew Internet Tracking Report

- 56% of all Americans approve of the FBI or law enforcement agencies intercepting telephone calls to and from people suspected of criminal activities. 36% disapprove. 8% don't know.
- 55% of all Americans approve of the FBI or law enforcement agencies intercepting letters and packages sent by mail to and from people suspected of criminal activities. 36% disapprove. 9% don't know.
- 54% of all Americans approve of the FBI or law enforcement agencies intercepting email over the Internet sent to and from people suspected of criminal activities. 34% disapprove. 12% don't know.

Women, Republicans, and whites are among the strongest supporters of email monitoring by law enforcement agencies.

Not surprisingly, Americans who say they trust the federal government are more likely to approve of these law enforcement tactics. Americans who are “very concerned” about Internet crime are also more likely to approve of the tactics than those who are less concerned. For example, 65% of Americans who are “very concerned” about Internet crime approve of telephone wiretaps, compared to 56% of those who say they are “somewhat concerned” and 42% of those who are not at all concerned.

<b>Intercepting email</b>			
<i>A majority of Americans support government interception of criminal suspects' email:</i>			
	<i>Approve</i>	<i>Disapprove</i>	<i>Don't Know</i>
All Americans	54%	34%	12%
Men	52	38	10
Women	56	29	14
Whites	56	32	12
Blacks	47	38	15
Hispanics	55	35	10
Republicans	59	31	10
Democrats	52	36	12
Independents	53	35	12

Source: Pew Internet & American Life Project Survey, February 2001.  
Margin of error is ± 2%.

### ***Opinions on Carnivore***

While a majority of Americans approve of email interception to fight crime, only 21% of all Americans have heard about Carnivore,<sup>1</sup> the FBI's digital surveillance tool. Not surprisingly, Internet users, who are generally more likely to follow the news than non-users, are more likely to have heard about Carnivore. Twenty-six percent of Internet users have heard about it, compared to 15% of non-users. Online veterans (those with three or more years of online experience) are more likely to have heard about it than the newest users (those with six months' experience or less) – 36% compared to 16%.

Americans who have heard about Carnivore are split down the middle about whether it is good or bad. Forty-five percent of people who have heard of it say Carnivore is good because it will allow the FBI a new way of tracking down criminals. Another 45% say Carnivore is bad because it could be used to read emails to and from ordinary citizens.

<sup>1</sup> The survey was conducted before the FBI announced the name-change to “DCS1000.”

## Pew Internet Tracking Report

Four percent of these Carnivore-savvy Americans say “both” and 6% answer, “I don’t know.”

While Internet users are more likely to have heard of Carnivore, online experience does not seem to play a role in forming an opinion about it. Internet users and non-users express similar views on both sides. Online veterans hold the same views on Carnivore as newcomers.

As with telephone wiretaps and other law enforcement tactics, women are more likely to approve of Carnivore. Fifty-two percent of women who have heard of it say it is a good thing, compared to 41% of men who agree.

It is worth noting that most Internet users are not especially worried about email privacy. As we reported in August 2000, 27% of Internet users are concerned that someone besides the person they sent it to will read their email. Seventy-two percent say they are not concerned about that possibility. By comparison, 84% of Americans say they are concerned about businesses and people they don’t know getting personal information about them and their family online.

### *New laws are needed to protect online privacy*

When asked if existing laws protecting the privacy of telephone conversations are enough to protect email and online activities, 62% of all Americans say that new laws need to be written to protect online privacy. Fourteen percent of all Americans think that the existing laws that cover telephone conversations are enough to protect email and online activities. Fully one in four Americans (24%) say they don’t know, no doubt because many are not sure exactly how the Internet works or how current laws work, or both. Indeed, Internet technologies are new and mysterious to most Americans and that could be a reason they think older laws might not be appropriately applied to the Internet.

It is worth noting that since few Americans are aware of the intricacies of current wiretapping laws, a survey about specific changes in the law that are being discussed by experts or highly-involved advocates would be of little use. Instead, we sought to gauge Americans’ general feelings about the balance between digital privacy and law enforcement.

Internet users are more sensitive than non-users to potential breaches of their online privacy, and more users than non-users support the writing of new laws. Seventy percent of Internet users say that new laws need to be written to protect online privacy. Fifty-five percent of non-Internet users say new laws are needed, but more than one in three (36%) of non-users say they don’t know enough about it to answer the question.

Men and women roughly agree on the issue of whether there should be new laws or not, with men slightly more inclined to think that the existing laws are good enough (18% of men, 10% of women).

## Pew Internet Tracking Report

Eighteen percent of Republicans think existing laws are good enough, compared to 12% of Democrats and 9% of Independents.

There were no significant differences among whites, African-Americans, and Hispanics on this question. Older Americans, those with less education, and those with lower incomes are more likely to say, “I don’t know” when asked about the need for new online privacy laws. For example, 51% of Americans aged 65 and older say they “don’t know.”

### ***Support for the FBI is greater than for “law enforcement agencies” in general***

To test whether there was any inherent pro-FBI or anti-FBI public sentiment that would color respondents’ views, we asked our surveillance questions two ways. Half those surveyed were asked if they approve or disapprove of the FBI’s use of surveillance techniques. The other half were asked to register their feelings about surveillance by “law enforcement agencies.” As it turns out, Americans are slightly more willing to give the FBI leeway when it comes to wiretaps, mail interception, and email snooping.

FBI vs. law enforcement		
<i>The percent of Americans who support the monitoring of each medium by...</i>		
	<i>“the FBI”</i>	<i>“law enforcement agencies”</i>
Phone calls	57%	54%
Mail	59	51
Email	57	52

*Source: Pew Internet & American Life Project Survey, February 2001. Margin of error is ± 3%.*

For example, 59% of Americans approve of the FBI intercepting letters and packages sent to and from suspected criminals. That number drops to 51% when Americans are asked if they approve of “law enforcement agencies” intercepting postal mail. Hispanics react more negatively to “law enforcement agencies” than did whites or African-Americans.

### ***Internet crime***

When asked about specific Internet crimes, Americans are nearly united – **child pornography** is far and away the top concern. Ninety-two percent of all Americans say they are concerned about it and a whopping 80% say they are “very concerned.” Internet users and non-users are equally concerned about child pornography online. As with the general Internet crime question, women register higher levels of concern than men (86% of women are “very concerned” about child pornography, compared to 74% of men). There were no significant differences among age, race, income, or education groups. Furthermore, when asked which *one* type of Internet crime is most distressing, 50% of all Americans say they are most concerned about child pornography. This crime most repulses Americans. Some may also be aware that the Internet has allowed child pornography to proliferate. A recent *Newsweek* investigation found that the number of FBI investigations involving online pedophilia had quadrupled between 1998 and 2000.<sup>2</sup>

<sup>2</sup> From *Newsweek*, March 19, 2001: “In fiscal year 1998, the FBI opened up roughly 700 cases dealing with online pedophilia, most of them for posting child pornography, and about a quarter dealing with online predators trying to get children under 18 to meet with them. By 2000 that figure had quadrupled to 2,856 cases.”

**Credit card theft** is the next-highest concern when it comes to Internet crime. Eighty-seven percent of all Americans are concerned about credit fraud online and 69% are “very concerned.” Internet users and non-users are equally concerned about credit card theft online. Seventy-two percent of women are “very concerned” about credit card theft, compared to 65% of men. Seventy-four percent of African-Americans are “very concerned,” compared to 68% of whites and 70% of Hispanics. Younger Americans are less feverish in their concern about credit card theft than older Americans – 60% of 18-29 year-olds are “very concerned,” compared to 72% of 30-49 year-olds and 73% of 50-64 year-olds.

Most-feared Internet crimes	
<i>The percentage of all Americans who say they are most concerned about...</i>	
Child pornography	50%
Credit card theft	10
Organized terrorism	10
Destructive computer viruses	5
Hackers attacking the government	5
Wide-scale fraud	2
Hackers attacking businesses	1
Another crime not listed as a choice	13

*Source: Pew Internet & American Life Project Survey, February 2001. Margin of error is ± 2%.*

As we reported in August 2000, not that many Americans have had their credit card stolen. Very few victims cite the Internet as an accomplice in the theft. Nineteen percent of Internet users (and 15% of all Americans) have been victims of credit-card fraud or identity theft at some point in their lives. A vast majority of those who had been victimized (80%) say the theft occurred offline. Only 8% of those who say their credit card was swiped reported that the thief *might* have gotten the information because the consumer had provided it online. That means that fewer than 3% of Internet users might have had their credit card information swiped online. However, the threat may be worse than imagined by the average consumer. In March 2001, the FBI reported that hackers in Russia and the Ukraine have penetrated over 40 U.S. computer systems to steal more than one million credit card numbers.

Eighty-two percent of all Americans are concerned about **organized terrorism** online. Women, African-Americans, senior citizens, and those with less education are more likely than their counterparts to be highly concerned. Americans who do not go online are more concerned about online terrorist activity than Internet users (66% of non-users are “very concerned,” compared to 56% of Internet users). Such fears may be fueled by recent reports that terrorist groups have expanded their use of encryption and are even using popular bulletin boards to post scrambled maps for their collaborators.

Eighty percent of all Americans are concerned about **wide-scale fraud**. Women, African-Americans, senior citizens, and those with less education are more likely than their counterparts to be highly concerned. Fifty-seven percent of non-users are “very concerned” about wide-scale fraud online, compared to 47% of Internet users. Just last month, Americans were treated to an extraordinary tale of identity fraud when the *New York Post* broke a story about a busboy who stole millions of dollars from members of the “Forbes 400” list of the wealthiest people in the U.S. by guessing their passwords, ordering their credit reports, and using bogus email accounts to cover his tracks.



Seventy percent of all Americans are concerned about **destructive computer viruses**. Since 25% of Internet users have had their computer infected by a virus, most likely from an email message, it is not surprising that Internet users are more concerned than non-users about viruses (61% are “very concerned,” compared to 48% of non-users). Americans between 50-64 years old are the most fearful – 62% say they are “very concerned” about viruses, compared to 52% of 18-29s.

Some of the most worrisome cybercrimes			
<i>The percentage of each group who say they are “very concerned” about these online crimes:</i>			
	<i>Child Pornography</i>	<i>Credit Card Theft</i>	<i>Organized Terrorism</i>
All Americans	80%	69%	61%
Men	74	65	57
Women	86	72	64
Whites	81	68	60
Blacks	82	74	67
Hispanics	80	70	64
Age 18-29	76	60	53
30-49	81	72	59
50-64	82	73	65
65+	82	69	70
Internet users	78	68	56
Internet non-users	82	70	66

*Source: Pew Internet & American Life Project Survey, February 2001. Margin of error is ± 2%.*

Seventy-eight percent of all Americans are concerned about **hackers getting into government networks**, Web sites and files. Women and senior citizens fear hackers more than their counterparts. Internet users and non-users are equally concerned about hackers attacking the government.

Seventy-six percent of all Americans are concerned about **hackers getting into business networks**, Web sites and files. Senior citizens are more concerned than younger Americans, but otherwise, there are no significant differences among men and women, racial categories, or education groups. Internet users and non-users are equally concerned about hackers attacking businesses.

***Methodology***

This report is based on the findings of a daily tracking survey on Americans' use of the Internet. The results in this report are based on data from telephone interviews conducted by Princeton Survey Research Associates between February 1, 2001 and March 1, 2001, among a sample of 2,096 adults, 18 and older. For results based on the total sample, one can say with 95% confidence that the error attributable to sampling and other random effects is plus or minus 2 percentage points. For results based Internet users, the margin of sampling error is plus or minus 3 percentage points. In addition to sampling error, question wording and practical difficulties in conducting telephone surveys may introduce some error or bias into the findings of opinion polls.

The sample for this survey is a random digit sample of telephone numbers selected from telephone exchanges in the continental United States. The random digit aspect of the sample is used to avoid "listing" bias and provides representation of both listed and unlisted numbers (including not-yet-listed numbers). The design of the sample achieves this representation by random generation of the last two digits of telephone numbers selected on the basis of their area code, telephone exchange, and bank number.

New sample was released daily and was kept in the field for at least five days. This ensures that complete call procedures were followed for the entire sample. Additionally, the sample was released in replicates to make sure that the telephone numbers called are distributed appropriately across regions of the country. At least 10 attempts were made to complete an interview at every household in the sample. The calls were staggered over times of day and days of the week to maximize the chances of making contact with a potential respondent. Interview refusals were recontacted at least once in order to try again to complete an interview. All interviews completed on any given day were considered to be the final sample for that day. The final response rate for this survey is 38%.

Non-response in telephone interviews produces some known biases in survey-derived estimates because participation tends to vary for different subgroups of the population, and these subgroups are likely to vary also on questions of substantive interest. In order to compensate for these known biases, the sample data are weighted in analysis. The demographic weighting parameters are derived from a special analysis of the most recently available Census Bureau's Current Population Survey (March 2000). This analysis produces population parameters for the demographic characteristics of adults age 18 or older, living in households that contain a telephone. These parameters are then compared with the sample characteristics to construct sample weights. The weights are derived using an iterative technique that simultaneously balances the distribution of all weighting parameters.