The Internet Life Report
For release at 10:00 p.m. Eastern on Sunday, August 20, 2000

Trust and privacy online: Why Americans want to rewrite the rules

Principal author: Susannah Fox, Director of Research

Lee Rainie, Project Director
John Horrigan, Senior Research Specialist
Amanda Lenhart, Research Specialist
Tom Spooner, Research Specialist
Cornelia Carter, Manager

The Pew Internet & American Life Project
1100 Connecticut Avenue
Suite 710
Washington, DC 20036
202.296.0019
http://www.pewinternet.org/

SUMMARY OF FINDINGS

In a season of growing concern about privacy on the Internet, The Pew Internet & American Life Project surveyed 2,117 Americans, 1,017 of whom are Internet users, from May 19 to June 21 about trust and privacy online. Their responses illustrated some fascinating cross currents on these issues. Online Americans have great concerns about breaches of privacy, while at the same time they do a striking number of intimate and trusting things on the Internet, and the overwhelming majority have never had a seriously harmful thing happen to them online.

On some major points, though, there is a powerful consistency: The first point is that American Internet users overwhelmingly want the presumption of privacy when they go online. The second point is that a great many Internet users do not know the basics of how their online activities are observed and they do not use available tools to protect themselves. The highlights of the survey:

Put users first

The vast majority of American Internet users want the privacy playing field tilted towards them and away from online companies. They think it is an invasion of their privacy for these businesses to monitor users' Web browsing. By a two-to-one margin they reject the argument made by some firms that Web tracking can be a helpful, but users are willing to share personal information under certain circumstances.

- 86% of Internet users are in favor of "opt-in" privacy policies that require Internet companies to ask people for permission to use their personal information. This view challenges the policy just negotiated by the Clinton Administration, the Federal Trade Commission, and a consortium of Web advertisers, which gives Web sites the right to track Internet users unless the users take steps to "opt out" of being monitored.
- 54% of Internet users believe that Web sites' tracking of users is harmful because it invades their privacy. Just 27% say tracking is helpful because it allows the sites to provide information tailored to specific consumers.
- 54% of Internet users have chosen to provide personal information in order to use a Web site and an additional 10% say would be willing to provide it under the right circumstances. 27% are hard-core privacy protectionists and would never provide personal information.

Some users employ guerrilla tactics, but most don't exploit the privacy-protecting tools that already exist

In order to protect their privacy, a relatively small number of savvy users are devising their own "opt-in" policies and deciding that some Web sites are not worthy of getting their personal information. But most users do not use available

privacy-protection tools, perhaps because they are unaware of how Web sites work and how existing technologies can be deployed to protect them.

- 24% of Internet users have provided a fake name or personal information in order to avoid giving a Web site real information.
- 9% of Internet users have used encryption to scramble their email.
- 5% of Internet users have used "anonymizing" software that hides their computer identity from Web sites they visit.
- 56% of Internet users cannot identify the primary online tracking tool. It is called a "cookie," and it is a text file that is placed on a user's computer by a Web site to help track that user's browsing activities. Despite Americans' high anxiety about being monitored online, only 10% of Internet users have set their browsers to reject cookies.

Companies should keep their promises – or else

Internet users want to punish firms and their executives when they violate users' privacy.

- 94% of Internet users want privacy violators to be disciplined. If an Internet company violated its stated privacy policy and used personal information in ways that it said it wouldn't, 11% of Internet users say the company's owners should be sent to prison; 27% say the owners should be fined; 26% say the site should be shut down; 30% say the site should be placed on a list of fraudulent Web sites.

The actual incidence of unpleasant events is modest and the incidence of criminal events online is miniscule…

Despite their deep-seated concerns, Americans have not been victimized online in great numbers.

- 28% of Internet users have gotten an offensive email from a stranger.
- 25% of Internet users have had a computer infected by a virus, most likely from an email.
- 17% of Internet users (and 11% of Americans) know someone who was fired or disciplined because of email they sent or the Web browsing they did at work.
- 4% of Internet users have felt threatened in some way while they were online.
- 3% of Internet users have been cheated when they tried to buy something online.
- Fewer than 3% of Internet users say their credit card information has been swiped online.

… and the incidence of trusting activities is high

Americans continue to trust email, surf the Web for advice about intimate aspects of their lives, make friends online, and turn to Web sites for health information, for spending their money, and for material about their finances.

- 48% of Internet users have bought something online with a credit card; 55% have sought health information; 43% have sought financial information such as stock prices.
- 36% of Internet users have gone to a support-group site or one that provides information about a specific medical condition or personal situation. Of those, 24% have signed in with their real name or email address, or written about their own experiences for other people to read.
- 25% of Internet users have made friends with someone online that they never knew before in the offline world.
- 26% of Internet users have responded to an email from someone they don't know.
- 22% have put information on online calendars and used online address books.

The things that concern Internet users

Internet Users' Fears

	Concerned	Not Concerned
Businesses and people you don't know getting personal information about you and your family	84%	15%
Computer hackers getting your credit card number online	68%	30%
Having unqualified people give you medical information online	54%	43%
That you'll get a computer virus when you download information	54%	45%
Seeing false or inaccurate news reports online	49%	49%
People spreading false rumors online to affect stock prices	47%	50%
People you meet online lying about who they really are	39%	48%
Someone might know what Web sites you've visited	31%	68%
Your email will be read by someone besides the person you sent it to	27%	72%

Source: Pew Internet & American Life Project May-June 2000 Poll

MAIN REPORT

SECTION ONE: AMERICANS WANT A PRIVACY GUARANTEE

Privacy has emerged as a central policy concern about the Internet as more Americans go online every day – and recent weeks have brought a ceaseless number of new allegations about privacy violations by Internet companies. In the past three months, a series of events have heightened sensitivities.

Very Concerned About Privacy

Women, minorities, those with less online experience, and older Americans are the MOST concerned about keeping their personal information private

All Americans	60%
Not online	64%
Internet users	54%
Women	62%
Men	57%
African-American	72%
Hispanic	62%
White	57%
Less than 6 mos. online experience	62%
More than 3 years online experience	50%
Ages 50-64	67%
Ages 18-29	46%

Source: Pew Internet & American Life Project May-June 2000 Poll

In June, the federal Office of National Drug Control Policy (the so-called “drug czar’s” office) was found to be using Internet tools called cookies to track Web surfers’ drug-related information requests. After a storm of criticism that this might allow the drug czar’s office to clandestinely record citizens’ online activities, the federal Office of Management and Budget banned the use of cookies on federal government Web sites.

In July, the Federal Trade Commission forced a bankrupt Toysmart.com to abandon its plans to sell off customer data to the highest bidder. The firm had promised site users that it would not divulge information gleaned from tracking users’ activities on the site, but a court-appointed overseer believed the customer list was a valuable asset that could be sold to help pay off the firm’s creditors. That same month, Senator John McCain (R-Ariz.) introduced legislation that would require commercial Web sites to notify consumers about what kinds of personal information they collect and how they use it. Microsoft announced new third-party cookie controls for Internet Explorer, actively warning consumers and allowing them to reject cookies, which could be used to track their activities all across the Web. Fifty Dow Chemical Company employees were fired after a search of their email revealed pornography or violent images. The Clinton Administration and the Federal Trade Commission set privacy standards so favorable for online advertisers that shares in Doubleclick rose 13 percent in one day. The FBI came under fire from Congress and civil liberties groups for developing “Carnivore,” a wiretapping device that silently intercepts all traffic to and from a suspect’s email account.

Early this month, Toysrus.com was accused of feeding shoppers’ personal information to a data-analysis firm without revealing the relationship to consumers. In response to complaints, Toysrus.com added information to their privacy policy about how customer data is treated, but denies that the information is sold to outside vendors. One week after the customer lawsuit was filed, Amazon.com and Toysrus.com announced a strategic alliance and restated their commitment to consumer privacy online. And this past week, Pharmatrak Inc., a Boston technology firm, acknowledged tracking consumers' activities on health-related sites without informing the public.

Not surprisingly, a great many online Americans are fretful about the things that could happen online and the way in which data about them might be gathered and used. An overwhelming majority of Internet users (84%) are concerned about businesses or people they don't know getting personal information about themselves or their families. Some 54% say they are "very concerned."

Americans want the "opt-in" option

These wired Americans are anxious to take charge of their online lives and resoundingly prefer a different privacy protection scheme from the one promoted by major Internet industry and government leaders. Seven in ten Internet users (71%) say that people who use Web sites should have the most say over how Internet companies track users' activities.

Indeed, Internet users reject the notion that the government and Internet companies are the best stewards of their personal privacy. Two-thirds say Internet companies should not be allowed to track users' activities and 81% contend there should be rules governing how that tracking is done. Asked who would do the best job setting those rules, 50% of online Americans said Internet users' themselves would be best, 24% said the federal government would be best; and just 18% said Internet companies would be best.

And they are clear what that policy should be. Some 86% of Internet users favor an "opt-in" privacy policy and say that Internet companies should ask people for permission to use their personal information. This is the kind of system that has been adopted by the European Union. By contrast, the self-regulation plan recently embraced by the Clinton Administration, the Federal Trade Commission and a consortium of Internet advertisers is an "opt-out" scheme that would compel consumers to take steps to protect their privacy.

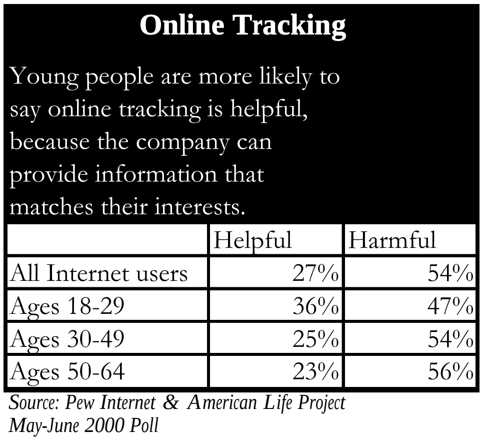
Many will share information – if they can choose when and where

When Internet users are given the choice between sharing their personal information or not being able to use a Web site, 54% have provided their real email address, name, or other personal information. Of those who have never done this, 23% (or 10% of all Internet users) say they are *willing* to provide that information in order to use a site. This two-thirds majority (64%) demonstrates that many Internet users are willing to enter into an exchange with Internet companies. That said, a solid majority of Internet users still do not think companies should track their behavior online without asking users' permission.

The making of cookies

The strong urge of online Americans to protect their privacy and put the onus on companies to get permission before exploiting data or passing it along to others is a pipe dream considering the current privacy arrangements on most Internet sites. Cookies are bits of encrypted information deposited on a computer's hard drive after the computer has accessed a particular Web site. The Web site stores these bits of information so when the same site is accessed again by that same computer, the Web site can recognize the computer and provide the same layout, shopping cart, search information, or even user's name with the exact personalization each time the site is visited. (No reliable figures exist about how many Web sites install cookies.) Some cookies track the activities of a user at a particular Web site. Others can track the user from Web site to Web site.

Netscape created cookies in 1994 as a special browser feature to make life easier for people browsing the Web. The concept is similar to that of a computer's preferences file. It keeps track of how the user wants a site to look or function. Once the preferences are set, the user does not have to input routine information upon each visit. Its creators thought it would be especially useful in enabling "shopping cart" services on Web sites. The idea was to allow consumers to click from page to page choosing items to buy, while a virtual clerk kept track of the items until the consumer was ready to check out. Cookies also allowed a site owner to observe which displays attracted the consumer's attention and which needed some sprucing up. Netscape did not initially inform consumers about the clandestine activity on their hard drives and probably did not foresee the firestorm that would follow.



Online Tracking

Young people are more likely to say online tracking is helpful, because the company can provide information that matches their interests.

	Helpful	Harmful
All Internet users	27%	54%
Ages 18-29	36%	47%
Ages 30-49	25%	54%
Ages 50-64	23%	56%

Source: Pew Internet & American Life Project May-June 2000 Poll

Chris Sherman has written for About.com that some believe the term cookie "comes from the story Hansel and Gretel, who marked their trail through a forest by regularly dropping crumbs along their path. Of course Hansel and Gretel used bright stones, not cookies to mark their trail; nonetheless, the legend persists."

After the media reported on the technology in January 1996, Netscape added a tool to disable cookies for the next version of their Web browsing software. But it was not very easy to do the disabling. Web site users had cookies implanted on their machines unless they took affirmative steps to reject cookies – a classic "opt-out" scheme. A user had to dig two menu screens down in his browser to find the place to opt out of cookies. There seemed to be no anticipation at the time that the use of cookies would create a problem. In 1996, Alex Edelstein, Netscape's product manager for Navigator 2.0, declared that cookie technology was an insignificant issue and would "blow over."

For a while, the use of cookies exploded and there were few complaints from consumers. Cookies themselves are not inherently bad or necessarily invasive to one's privacy. And they are instrumental in activating some of the Web's most appealing features. Web publications like iVillage.com use cookies to identify the preferences of regular readers and then direct appealing, tailored content to them. Merchants like Amazon.com use cookies to speed ordering and to suggest products to return customers. Soon enough, Web advertisers saw the possibility that cookies could help Web sites monitor users' activities and help discern consumer tastes. With that kind of information Web sites could deliver customized information to users.

Third-party advertising networks like Doubleclick sprang up to oversee banner ads on Web sites. These networks designed cookie files that track a user's activities all across the Web and trigger advertisements according to each user's apparent interests and needs. It is Web sites' ability through cookies to glean user's tastes and lifestyle that has led to the current debate about the appropriate ways to do tracking and maintain the privacy Americans want. In the most comprehensive and extreme cases, a Web company could build a profile of an Internet user that combines information about her purchases, her taste in music, the investment information she seeks, the health issues that concern her most, and the kind of news stories that seize her interest.

Unarmed in the privacy wars

The rise of third-party ad networks has raised the issue of cookies to prominence in legal and policy-making circles. But fewer than half of Internet users are aware of cookies. Eight in ten Internet users (79%) think it's common for Internet companies to track Web activities, yet only 43% of Internet users know that creating cookies is the way this is done. Of those who can identify cookies, just 24% set their browsers to refuse cookies. That means just 10% of all Internet users have set their browsers to reject cookies.

Most Online Shoppers Don't Know They're Being Tracked

	Know what a "cookie" is	Refuse "cookies"
All Internet users	43%	10%
Internet users who have clicked on an ad	51%	12%
Internet users who have bought a product online	56%	11%

Source: Pew Internet & American Life Project May-June 2000 Poll

To a considerable degree, members of the two groups most likely to be targeted by Internet companies – those who click on ads online and those who buy things online – are unaware that their computers' hard drives are implanted with cookies. The Pew Internet Project survey found that 69% of Internet users have clicked on a Web advertisement and about 46% have bought products online. Yet only about half of each of those groups know what a cookie is. Of those shoppers and ad-clickers who are aware of cookies, just a fifth choose to block the tracking devices and surf more anonymously (23% of ad-clickers and 20% of online buyers). That means almost 90% of Internet users who shop online are being tracked by cookies and many are unaware that is happening.

There are other notable differences between groups when it comes to cookie awareness. Men are more likely than women to say they know what a cookie is (51% of online men; 34% of online women). Internet veterans are much more likely than Internet novices to say they know what a cookie is. Sixty percent of users who have been online for three or more years know what a cookie is, compared to just 23% of new users.

The verdict on tracking

A majority of Internet users (54%) are certain that online tracking is harmful because it invades their privacy. Advocates of cookies make the case that consumers will eventually come to appreciate cookies because they allow sites to provide information that is important and relevant to an individual Web user. In the case of advertising and marketing, cookie advocates argue that there is a great deal of waste that everyone hates in mass marketing through the mails (junk mail) and the media. These advocates argue that the ideal world created by cookies and tracking is one where the clutter of information and advertisements is cut to a minimum and only useful material is put in users' and consumers' hands. There is a distance to go, though, before that argument persuades Internet users. Only 27% say that tracking is helpful because it allows Web sites to tailor information for users.

Richard Purcell, director of the Corporate Privacy Group at Microsoft, says that new cookie controls for Internet Explorer will be part of a set of "empowerment tools" for consumers that will soon be available in the upgraded browser. Users will be alerted when a site tries to place a third-party cookie – that is, one that could help track their activities all across the Web. "We don't want to tell businesses how to act, beyond being truthful, but instead we want to let consumers be a force to be reckoned with," says Purcell. Purcell believes that consumer education is the key to allaying Internet users' fears – not behavior modification on the part of the industry.

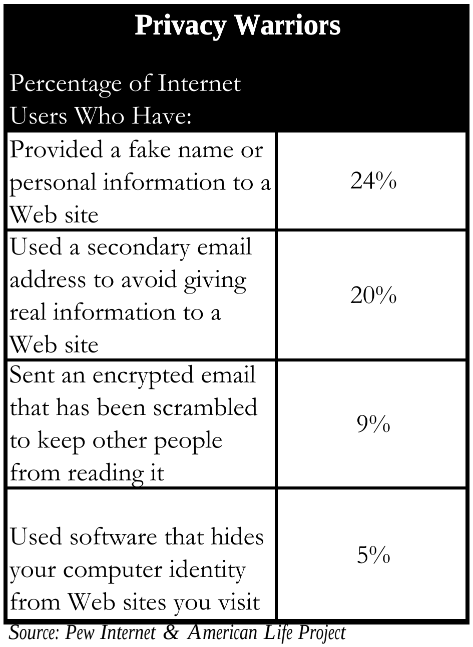
Hard-core privacy protectionists

While online Americans say they are concerned about breaches of privacy and that control is important to them, about half of all Internet users are trusting valuable personal information to Web companies that require it. Fifty-four percent of Internet users have provided their real email address, real name, or other personal information in order to use a Web site.

Of the 45% of Internet users who have not provided real personal information to a site, 61% are hard-core privacy defenders and say they are not willing to provide that information in order to use a site. This hard-core group is more likely to believe that tracking is harmful, that online activities are not private, and that there is reason to be concerned about businesses getting their personal information. Women and men are equally likely to be in this hard-core group, as are new and veteran Internet users. Young people (18-29 years old) are more likely to say they are not willing to provide personal information, as are users who go online only from home.

SECTION TWO: GUERRILLA TACTICS

There is a small group of Internet users resorting to "guerilla tactics" to defend their privacy online. About a quarter of Internet users have provided a fake name or personal information in order to avoid giving a Web site real information about themselves. A fifth of online Americans have used a secondary email address to avoid giving a Web site real information. Just one in ten Internet users have sent an encrypted email and only one in twenty have used software that hides their computer identity from Web sites.



Privacy Warriors

Percentage of Internet Users Who Have:	
Provided a fake name or personal information to a Web site	24%
Used a secondary email address to avoid giving real information to a Web site	20%
Sent an encrypted email that has been scrambled to keep other people from reading it	9%
Used software that hides your computer identity from Web sites you visit	5%

Source: Pew Internet & American Life Project
May-June 2000 Poll

Men are more likely to engage in these guerrilla tactics than women. Twenty-eight percent of men have provided fake personal information to a Web site, compared to 19% of women. Twelve percent of men have used encryption to scramble their email, compared to 6% of women. Seven percent of men have used identity-masking software, compared to 4% of women.

Young people and those with more online experience are also more likely to resort to lying in order to protect their personal information. Thirty-five percent of 18-29 year olds have provided fake personal information, compared to 22% of 30-49 year olds and 17% of 50-64 year olds. Only 18% of the newest users (online for six months or less) have provided fake personal information, compared to 31% of those with three or more years of online experience.

The use of online deception tactics such as fake names highlights the compartmentalization that is the basic tool of people who want to control their privacy. Judith Donath, an MIT professor who studies identity and online behavior, says that until Web sites design spaces that are clearly public or clearly private, users will have trouble choosing what information to share and what to hide. She adds that such fundamental decisions about what to share "shouldn't be about reading the fine print" of a Web site's privacy policy, but instead should be as obvious as the difference between staying in the privacy of your own home versus walking down the street. When a user is in "public" Internet space such as an online store, she suggests, the user would be correct in assuming that her movements were watched. When the user was in "private" space, he would have a right to expect that nothing about his activities there would be monitored, gathered into a profile, or sold to anyone or any firm unless he authorized it. Just as people act one way in their dens and another way at a party, Internet users want to make sure that the Internet world recognizes nuances about when "public" and viewable events are occurring as opposed to "private" and sensitive communications.

Internet users are pretty savvy about at least one safeguard: passwords. Sixty-eight percent of Internet users use different passwords when they register at various Web sites. Men are more likely than women to use different passwords (72% of men, compared to 64% of women).

SECTION THREE: A PUNISHING MOOD

Internet users may not know all the tricks when it comes to protecting their privacy online, but they know problems when they see them. And if their trust is betrayed, they want vengeance.

If an Internet company violated their own privacy policy and used personal information in ways that it said it wouldn't, 94% of Internet users said the company should be punished. When given four choices of punishment, 11% of Internet users say the company's owners should be put in jail, 27% say the company's owners should be fined, 26% say the site should be shut down, and 30% say the site should be placed on a list of fraudulent Web sites.

If an Internet company cheated its customers or committed a fraud online, again, 94% of Internet users said the company should be punished. When presented with the same four options, 26% of Internet users say the company's owners should be put in jail, 22% say the company's owners should be fined, 33% say the site should be shut down, and 13% say that placing the site on a "fraudulent site" list is the right punishment.

Men are somewhat more passionate to punish dot-com executives. Fourteen percent of online men say a privacy-violating company's owners should be put in jail, compared to 7% of online women. Thirty percent of online men think a fraudulent company's owners should be put in jail, compared to 22% of online women.

More experienced Internet users are also less forgiving. Thirteen percent of veteran Internet users (three or more years of experience) would put the privacy-violating executives in jail, compared to 7% of the newest users (less than six months of experience). Thirty percent of veteran users say jail is the right place for owners of a fraudulent company, compared to 23% of the newest users.

Jason Catlett, founder of Junkbusters Corp. and a privacy advocate, argues the case for punishment this way: "Many Americans know that violation of copyright is a crime, and many believe that violation of their privacy should be a crime too. Why is distributing a corporation's software without its permission called 'piracy,' while distributing a person's information without permission is called 'sharing'?"

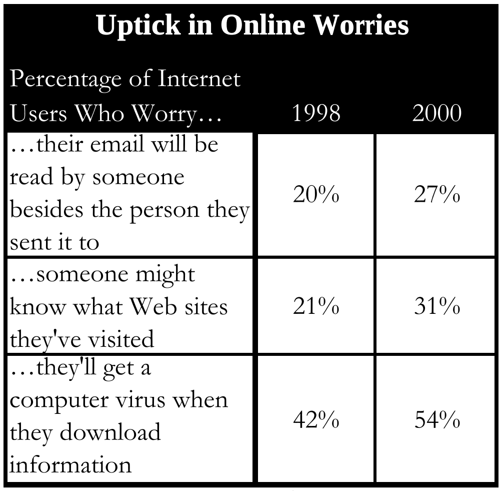
The Federal Trade Commission currently lacks the authority to enforce privacy standards on commercial Web sites, unless the content is directed at children. In May this year, the FTC released a report on privacy online that noted "only 20% of the busiest sites" implement the four widely-accepted fair information practices: 1) notice, displaying a clear and conspicuous privacy policy; 2) choice, allowing consumers to control the dissemination of information they provide to a site, 3) access, opening up the consumer's personal information file for inspection, and 4) security, protecting the information collected from consumers. The commission maintained that industry self-regulation had fallen short. Even as it agreed to a self-regulation scheme with Internet advertisers, the FTC called on Congress to expand the agency's enforcement power "to ensure adequate protection of consumer privacy online."

<u>SECTION FOUR: FEAR VS. TRUST</u>

This survey's attempt to assess the level of trust online found three strong and sometimes conflicting patterns. In their attitudes, Internet users express considerable fears about a number of problems they might face online. They report, though, that the actual incidence of online problems is not very substantial. Finally, despite those fears, they behave in surprisingly trusting ways in many sensitive online areas. However, those fears cannot be discounted because they do seem to inhibit some groups, especially Internet novices and parents, from participating in some kinds of Internet activities.

Many anxieties

A strong sense of distrust shades many Internet users' view of the online world and the uneasiness has grown in the past two years. Eighty-six percent of Internet users say they are concerned about businesses or people they don't know getting personal information about them or their families. Seven in ten Internet users are concerned about hackers getting their credit card number and six in ten are concerned about someone learning personal information about them because of things they've done online. More than half of Internet users worry about receiving bad medical information online or downloading a virus to their computer. Nearly half of Internet users worry about seeing false news or financial reports online. Forty-six percent are not confident that their online activities are private. Only 10% of Internet users are "very confident" that the things they do online are private and will not be used by others without their permission.



Uptick in Online Worries

Percentage of Internet Users Who Worry…	1998	2000
…their email will be read by someone besides the person they sent it to	20%	27%
…someone might know what Web sites they've visited	21%	31%
…they'll get a computer virus when they download information	42%	54%

Sources: Pew Internet & American Life Project May-June 2000 Poll and The Pew Research Center for the People and the Press 1998

Older users are more concerned than younger users about the integrity of the information they see on the Internet. Fifty-nine percent of Internet users 50-64 years old are concerned about people spreading false rumors online to affect stock prices, compared to 37% of 18-29 year old users and 49% of 30-49 year old users. Fifty-five percent of

Internet users 30-49 years old are concerned about seeing false or inaccurate news reports online, compared to 40% of 18-29 year old users and 50% of 50-64 year old users.

Credit card concerns: Not much different from the offline world

It is important to understand that while Americans are concerned about their privacy online, there is no evidence in this survey that the Internet is a more menacing threat to privacy than activities in the offline world. In the case of credit card information, Americans' online concerns are no greater than the concerns they have offline. Of all those Americans who had used their credit card to buy something over the phone, 56% said they worried about someone else getting their credit card number. Of all those with Internet access who used their credit card to buy something online, 54% said they worried about someone else getting their credit card number. And the proportion of those using credit cards online has leaped in the last five years. Only 8% of Internet users had used their credit card to make a purchase online in 1995, compared to 48% of Internet users who had done this by June 2000.

This survey found that 19% of Internet users (and 15% of all Americans) have been victims of credit-card fraud or identity theft. A vast majority of those who had been victimized (80%) said the theft occurred offline. Only 8% reported that the thief got the information because the consumer had provided it online. That means that fewer than 3% of Internet users have had their credit card information swiped online.

Viruses and unwanted email

The most frequent online problems are tied to email, but that has not seemed to affect the Internet's most popular activity. Almost everyone who goes online (98%) knows what a computer virus is and one in four Internet users (25%) has had a computer infected by a virus. According to CERT, the Internet security emergency response team at Carnegie Mellon University, the number of "security incidents" reported held steady at about 2,400 per year in the mid-1990s. But such incidents grew to 3,700 in 1998, nearly 10,000 in 1999, and 8,836 through the first two quarters of 2000. An infected email message is the most likely suspect for Internet users who have had a virus – 46% cite that suspicion.

Users who go online from both home and work are the most fearful of computer viruses, possibly because they are more likely to have downloaded a virus and would miss the Internet the most if their access were taken away. Seventy-five percent of home-and-work users say they are worried, compared to just 51% of work-only users (who are often protected by impenetrable firewalls) and 52% of home-only users. Thirty-one percent of home-and-work users have had a computer infected with a virus, compared to 30% of work-only users and 18% of home-only users. Nevertheless, email users are very fond of this form of communication; and the people most victimized by viruses are the most likely to express affection for email. In a March 2000 Pew Internet Project poll, 83% of home-and-work users said they would miss the Internet if they could no longer go online, compared to 54% of work-only users and 71% of home-only users.

Viruses are not the only stink bombs lurking in Americans' email in-boxes. Twenty-eight percent of Internet users have received an offensive email from someone they have never heard of. Men and women are equally likely to have received an offensive email, as are Internet users across all age, education, and income groups. Veteran users – Americans who have been online for more than three years – are the most likely to have received an offensive email from a stranger. Thirty-six percent of veteran users said that has happened to them, compared to just 14% of users with less than six months of experience online.

In a March 2000 Pew Internet Project poll, 37% of email users reported that they get a lot of spam or unwanted email messages. For those who feel inundated by unwanted email, 70% say the offending messages are sales solicitations, 17% say the emails are from other people they don't care to hear from as much, and 7% say the unwanted emails come from list-serves, or online discussion groups.

Email continues to be the most popular online activity – 92% of Internet users have ever sent an email and 48% do this on a typical day.

Work surveillance and discipline

The incentive to monitor Internet users' behavior is not simply confined to those who want to sell them products and services. There are legal encouragements to monitor online actions. Business executives can be sued if they do not maintain a safe and harassment-free work environment. That gives these executives encouragement to watch what happens on their computer systems. Moreover, the Internet is bursting with opportunities for workers to use their computers for fun or profit that is not related to their jobs. That can prompt executives to make sure workers are productively engaged when they are on the clock.

The Pew Internet Project survey shows how aggressively firms are already acting on those incentives. Eleven percent of all Americans and 17% of Internet users know someone who was fired or disciplined because of an email they sent or a Web site they went to at work. The survey suggests this kind of thing is happening most frequently at the level of those with the highest paying, most sophisticated jobs. Americans with higher levels of education and income are more likely to know someone in that situation. Fifteen percent of Americans with a college degree know someone who was fired or disciplined because of online activities, compared to 3% of Americans with have not finished high school. Nineteen percent of Americans with a household income exceeding $75,000 per year know someone in that situation, compared to 8% of those whose household income falls below $30,000 per year.

Yet many Internet users continue to conduct personal business during working hours. According to the Pew Internet Project's four-month tracking poll, 10% of Internet users who only go online from work are surfing the Web "just for fun" or to pass the time on a typical day. In addition, on that typical day, 8% of work-only Internet users are looking for information online about a hobby or interest; 3% are looking for a new job; 4% are looking for information about books, movies, music or other leisure activities; and 5% are checking sports scores on that day.

Making friends and meeting strangers

Twenty-six percent of Internet users have responded to an email from a stranger and 25% of Internet users have made friends with someone online. Men are much more likely to respond to an email from someone they've never met or talked to than women. Some 31% have done that compared to 20% of women. Young people are also more likely to have responded to unexpected emails than older Internet users – 31% of 18-29 year olds have responded to a stranger's email. After age thirty, an Internet user's likelihood to respond drops significantly, with 25% of users between 30-49 years old and 22% of 50-64 year olds responding to a stranger's email.

The incidence of making friends online has held steady for years. Pew Research Center polls show that 23% of Internet users reported that they had made a friend online in 1995 and a similar percentage reported that in 1998. As with responding to emails from a stranger, men are more likely to make friends online with 29% claiming an online friend, compared to 21% of women. Twenty-eight percent of those with a high school education or less have made friends online, compared to 18% of those with a college degree.

And although most Internet users are wary of other people, only 4% have ever felt personally threatened when they were online.

Dating and support-group sites

Despite their privacy concerns, Americans are finding ways to reach out to each other online. Large majorities of those who email family and friends say email is useful for these communications (88% and 90% respectively). Half of those who email friends (51%) say the electronic communication has brought them closer, while among those who email family 40% say it has brought them closer to their families.

Nine percent of Internet users have gone to a dating site and 36% have gone to a support-group site or one that provides information about a specific medical condition or personal situation. Interestingly, men are twice as likely as women to visit a dating site (12% of men have done this, compared to 6% of women). Women are almost twice as likely as men to visit a support-group site (44% of women have done this, compared to 29% of men).

Online calendars or address books

Internet users are also taking advantage of online services that aim to simplify their lives, despite their concerns about security risks. Twenty-two percent of Internet users have entrusted their personal calendar or address book to a Web site service. Internet users who upload intimate life details such as anniversaries and doctor's appointments may well be nervous that the Web calendar company will protect their privacy. Not surprisingly, many of the sites are part of the TRUSTe privacy program and post very tough-sounding policies. For example, the Daily Drill site states, “Your calendar and all its information is absolutely private and will never ever be shown to anyone else. Period.”

Women and African-American users are more likely to use these types of sites, despite the fact that these groups are among the most frequent to say they are concerned about their online privacy.

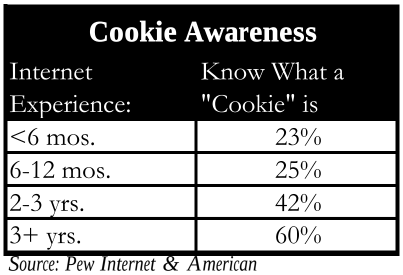
SECTION FIVE: WHY PRIVACY CONCERNS COULD LIMIT THE NET’S POTENTIAL

Concerns about privacy are notably higher among some groups, especially Internet novices (those who first got online within the past six months), parents, older Americans, and women. In some instances, these fears are associated with lower participation in some online activities, especially commercial and social activities. There is no way to know yet whether these groups will eventually become more comfortable and less fearful in the online world or whether their wariness will permanently limit their use of the Internet until their concerns about protecting personal information are met.

Internet newcomers and veterans

Fifteen percent of Internet users just got online in the last six months. These users are more likely to be highly concerned about privacy and Web site security than more experienced Internet users. Sixty-two percent of Internet users with less than six months of experience are “very concerned” about businesses and people they don’t know getting personal information about them or their family. In comparison, 50% of Internet users with three or more years of experience feel that way.

These pronounced privacy concerns among newer Internet users are driven in part by their fears about the technology, rather than first-hand experience with fraud or other online invasions. For example, new users are no more likely than experienced users to have been victims of any kind of credit card fraud. Some 19% of these newcomers have had their credit card number stolen, compared to 23% of Internet veterans who have suffered the same problem. And very few in each group have been victims of credit card theft online.



Cookie Awareness

Internet Experience:	Know What a "Cookie" is
<6 mos.	23%
6-12 mos.	25%
2-3 yrs.	42%
3+ yrs.	60%

Source: Pew Internet & American Life Project May-June 2000 Poll

New users are less likely than Internet veterans to know what a “cookie” is. Among those who know what a cookie is, veteran users are the most likely to set their browser to accept them – 72% of users with three or more years of experience allow Web sites to track their activities using cookies, compared to 55% of users with two or three years of experience. The percentage of new users who block cookies is too small to accurately evaluate.

New users are much less likely than veteran users to lie to protect their personal information. Only 18% of the newest users (online for six months or less) have provided fake personal information to a Web site, compared to 31% of those with three or more years of online experience.

The more time someone has been online, the more likely they are to be confident about Web site security. For example, an equal proportion (23%) of the most experienced Internet users (3+ years of experience) and relatively new users (6-12 months of experience) have had their credit card or other personal information used without permission. But only 46% of the most experienced Internet users say they worry about online credit-card theft, compared to 70% of less-experienced users.

This lack of confidence is reflected in the fact that Internet newcomers are also less likely to purchase products or services online. Twenty-seven percent of users who got access within the last six months have bought something online such as books, music, toys, or clothing, compared to 60% of users who have been online for three or more years. Only 18% of the newest users have purchased an airline ticket or made a hotel reservation online, compared to 36% of the most experienced Internet users.

New users are more wary and less friendly online than veteran users. Just 18% of Internet users with less than six months of experience have responded to an email from someone they don’t know, compared to 34% of those with three or more years of experience. Eighteen percent of new users have made a friend online, compared to 28% of veteran users.

The parents’ story

Forty-two percent of Internet users are parents and they bring a unique perspective to the privacy debate. Eighty-four percent of parents think Internet companies should have to ask for permission to use any personal information that they collect, compared to 76% of non-parents.

Parents with Internet access whose children also go online are much more nervous about computer viruses, perhaps out of concern that their children will unwittingly infect the family machine. Sixty-two percent of these “wired family” parents worry about downloading a virus to their computer, compared to 50% of non-parents and 54% of all Internet users.

Now What Have You Downloaded?

Do you ever worry that you'll get a computer virus when you download information?	
Internet users	54%
Online parents whose children go online	62%
Online non-parents	50%

Source: Pew Internet & American Life Project May-June 2000 Poll

Parents who are online are less friendly and more wary of other people than non-parents online. Only 20% of parents have responded to an email from someone they didn't know, compared to 30% of non-parents. Parents are also less likely to make friends online – 20% of parents said they had, compared to 28% of non-parents.

APPENDIX:
HOW TO LOOK FOR COOKIES ON YOUR COMPUTER
– AND DISABLE THEM

Any Internet user reading this report can find out how extensive the “cookies” phenomenon is by reading his or her own cookie file.

Finding cookies on a Windows computer

On a Windows machine, click the “Start” button, go to pop up menu to “Find” and then click on “Files or Folders.” When the “Find all Files” window pops up make sure the “Name & Location” screen is open and type “cookies” on the line for “Named.” Make sure the search is being conducted on your “local hard drive” (usually drive C) and then click “Find Now.” Open the cookies text document. A cookie set by CNN’s Web site, for example, will begin “.cnn.com TRUE …” In Netscape, you can delete a cookie by clicking on it and hitting the delete key. Be sure to save your edited cookie file. In Internet Explorer, go to “Tools,” select Internet Options. Under the “General” tab, select the “Settings” button and the “View Files.” Click on the “name” header to alphabetize the files, then scroll down to the files that begin with cookies. Individually delete each cookie file that you wish to remove.

Finding and disabling cookies on a Macintosh computer

If you’re a Macintosh user, finding your cookies is a little different and depends on which browser you use. If you use Netscape, go to your systems folder and select “preferences.” In the folder, there is a text file called “MagicCookies” which lists all of the cookies on your hard drive. This file is for viewing only and cannot be edited. If you would like to edit your cookie file, you will need to download a free piece of software called “CookieCutter” at http://www.macdownload.com/ that allows you to edit your cookie file selectively. To disable cookies in Netscape, open a Communicator window and pull down the “Edit” menu and select “Preferences,” and then “Advanced.” Select one of the four levels of protection you desire, and then click OK. Re-start your browser to put your choice into effect.

If you use Internet Explorer, open a browser window, pull down the “Edit” menu, select “Preferences.” Scroll down the menu and double-click on “Cookies.” All of the cookies on your computer will be listed along with choices from “never ask” (or accept all cookies) to “never accept.”

Disabling cookies on a Windows computer

Please note: All information is for the latest version of each browser.

Netscape:
Launch Netscape and open a new browser window. Select the “Edit” pull down menu, and on the menu select “Preferences.” In the white "Category:" column, select

“Advanced.” In the Cookies section, Netscape gives you four choices--to accept all cookies, to accept only the cookies that get sent back to the originating server (and thus do not stay on your hard drive), to disable all cookies, or to warn you every time you are being asked to accept a cookie. Select your desired option and click OK. Close and then re-start Netscape to begin browsing with your selected level of protection.

Internet Explorer:
Launch Internet Explorer and open a new browser window. Pull down the “Tools” menu and select “Internet Options.” In Internet Options, select the top “Security” tab. Select the “Internet” icon (a globe) and click on the “Custom Level” button. Scroll down through the options until you encounter "cookies." IE breaks up its options for cookies that are stored on your computer and those which are not. To block stored cookies, go to the first section and select Disable. To be warned each time your computer is asked to receive a cookie, select Prompt. To block or be warned about unsaved cookies, select Disable or Prompt in that section.

For more information and detailed instructions on how to find, disable and delete cookies, check the State of Michigan Attorney General’s site on cookies at: http://www.ag.state.mi.us/AGWebSite/inet_info/ii_cookie01.htm.

A good discussion of the pros and cons of cookies can be found at: http://www.cookiecentral.com/cm002.htm

METHODOLOGY

The survey results are based on telephone interviews conducted by Princeton Survey Research Associates among a sample of 2,117 adults, 18 years of age or older, in the continental United States during the period May 19-June 21, 2000. The survey was conducted using a rolling daily sample, with a target of completing 100 interviews each day throughout the month.

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 2.5 percentage points. Many questions in the survey were asked only of 1,017 adults who are Internet users. For these results, the 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.

A new sample was released daily and was kept in the field for at least five days. This insures that the complete call procedures are followed for the entire sample. Additionally, the sample was released in replicates to insure 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 re-contacted 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.

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 1999). This analysis produced 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.

Throughout this report, the survey results are used to estimate the approximate number of Americans, in millions, who engage in Internet activities. These figures are derived from the Census Bureau’s estimates of the number of adults living in telephone households in the continental United States. As with all survey results, these figures are estimates. Any given figure could be somewhat larger or smaller, given the margin of sampling error associated with the survey results used in deriving these figures.

Questionnaire

Editor's Note: Not all the questions asked on the survey are available here. Data analysis is still being done on several aspects of this survey.

Daily Internet Tracking Survey

May-June 2000

Princeton Survey Research Associates
for the Pew Internet & American Life Project

Sample: *n* = 2,117 adults 18 and older
Interviewing dates: May 19-June 21, 2000
Margin of error is plus or minus 2.5 percentage points for results based on the full sample
Margin of error is plus or minus 3 percentage points for results based on Internet users

ASK ALL — INTERNET USERS AND NON-USERS: [N = 2,117]

1 Generally speaking, would you say that most people can be trusted, or that you can't be too careful in dealing with people?

			JUNE 1997	FEB 1997
%	32	Most people can be trusted	42	45
	61	Can't be too careful in dealing with people	54	52
	5	Other/Depends	3	2
	2	Don't know/Refused	1	1

2 Do you think most people would try to take advantage of you if they got the chance, or would they try to be fair?

			JUNE 1997	FEB 1997
%	39	Most people would try to take advantage	39	37
	49	Most people would try to be fair	56	58
	9	Depends	4	4
	3	Don't know/Refused	1	1

3 How concerned are you, if at all, about businesses and people you don't know getting personal information about you and your family — very concerned, somewhat, not too, or not at all?

%	59	Very concerned
	25	Somewhat concerned
	8	Not too concerned
	7	Not at all concerned
	1	Don't know/Refused

4 Have you ever used your credit card to buy something over the phone?

%	54	Yes
	46	No
	*	Don’t know/Refused

IF YES IN 4, ASK: [N = 1,174]

5 When you do this, how much, if at all, do you worry that someone else might get your credit card number — a lot, some, not very much, or not at all?

%	21	A lot
	35	Some
	27	Not very much
	17	Not at all
	*	Don’t know/Refused

6 And have you ever used your credit card to buy something on the Internet?

Based on Internet users [N = 1,017]

%	48	Yes
	52	No
	*	Don’t know/Refused

IF YES IN 6, ASK: [N = 489]

7 When you do this, how much, if at all, do you worry that someone else might get your credit card number — a lot, some, not very much, or not at all?

%	18	A lot
	36	Some
	28	Not very much
	18	Not at all
	0	Don’t know/Refused

8 Has anyone ever gotten your credit card number or other type of personal information and used it without your permission, or hasn't that happened to you?

%	15	Yes
	84	No, not happened
	1	Don’t know/Refused

IF YES IN 8, ASK: [N = 330]

9 As far as you know, did this happen because someone got a credit card number or personal information that you provided ONLINE over the Internet, OR did this happen because someone got a credit card number or personal information that you provided in some other way?

%	8	Had provided information online over the Internet
	80	Had provided information some other way (not online)
	12	Don’t know/Refused

10 Now a few questions about some Internet topics that sometimes come up. Not everyone will have heard about these.

Do you happen to know what an Internet "cookie" is?

Based on Internet users [N = 1,017]

%	43	Yes
	56	No
	1	Don’t know/Refused

IF YES IN 10, ASK: [N = 434]

11 Is your browser set to accept cookies, or not?

%	65	Yes
	24	No
	11	Don’t know/Refused

12 Do you happen to know what a computer virus is?

Based on Internet users [N = 1,017]

%	98	Yes
	2	No
	*	Don’t know/Refused

IF YES IN 12, ASK: [N = 1,000]

13 As far as you know, has your computer ever been infected by a virus? **(IF YES, ASK:** Was this on a computer at home, or at work?**)**

%	12	Yes, at home
	9	Yes, at work
	4	Yes, both
	75	No
	*	Don’t know/Refused

IF YES (13=1,2,3) HAD VIRUS, ASK: [N = 248]

14 Did this virus come from a computer disk, from an email message, or from downloading something from the Internet, or aren't you sure where it came from?

%	17	Computer disk
	46	From an email message
	14	Downloading something from the Internet
	18	Not sure where
	3	Came from all of these/Several different ways
	2	Don’t know/Refused

QUESTIONS 15 - 24 BASED ON INTERNET USERS [N = 1,017]

15 How confident are you that the things you do online are private and will not be used by others without your permission — very confident, somewhat confident, not too confident, or not at all confident?

%	10	Very confident
	42	Somewhat confident
	28	Not too confident
	18	Not at all confident
	2	Don’t know/Refused

16 On another subject...How much do you ever worry that... **(INSERT ITEM; ROTATE ITEMS)** — a lot, some, not very much, or not at all?

	A LOT	SOME	NOT VERY MUCH	NOT AT ALL	DON’T KNOW
a. Your email will be read by someone besides the person you sent it to	7	20	29	43	1
b. Someone might know what Web sites you’ve visited	8	23	23	45	1
c. You’ll get a computer virus when you download information	17	37	25	20	1

17 How common do you think it is, if at all, for Internet companies to keep track of the Web pages you go to — very common, somewhat, not too, or not at all?

%	44	Very common
	35	Somewhat common
	8	Not too common
	6	Not at all common
	7	Don’t know/Refused

18 If an Internet company DID track the pages you went to while online, do you think that would be...**(ROTATE 1 and 2)**

%	27	Helpful, because the company can provide you with information that matches your interests
	54	Harmful, because it invades your privacy
	11	Both
	4	Neither
	4	Don’t know/Refused

19 Have you ever provided your real email address, your real name, or other personal information at a Web site in order to use the site?

%	54	Yes
	45	No
	1	Don’t know/Refused

IF HAVE PROVIDED INFORMATION AT WEB SITE (YES IN 19), ASK: [N = 562]

20 When you register at Web sites, do you always use the same password, or do you happen to use different passwords?

%	29	Always use the same password
	68	Use different passwords
	3	Don’t know/Refused

IF HAVE NOT PROVIDED INFORMATION (NO OR DON'T KNOW IN 19), ASK: [N = 455]

21 Would you be WILLING to provide your real email address, real name, or other personal information at a Web site in order to use the site?

%	23	Yes
	61	No
	15	Depends
	1	Don’t know/Refused

22 Have you ever provided a FAKE name or personal information in order to avoid giving a Web site real information about yourself?

%	24	Yes
	76	No
	*	Don’t know/Refused

23 Have you ever used an email address that is NOT your main email address, in order to avoid giving a Web site real information about yourself?

%	20	Yes
	80	No
	*	Don't know/Refused

24 Here is another list. Some people have done these things, but other people have not. What about you...
Have you ever...**(READ ITEMS; ROTATE ITEMS)**

		YES	NO	DON'T KNOW/ REFUSED
a.	Responded to an email from someone you've never met or talked to?	26	74	*
b.	Clicked on an advertisement on a Web site to learn more about a product or service?	69	31	*
c.	Been cheated when you tried to buy something online?	3	97	*
d.	Gotten and offensive email from someone you've never heard of?	28	71	*
e.	Gotten an "instant message" from someone you've never heard of	37	63	*
f.	Made friends or gotten to know someone you'd never spoken to by communicating online	25	75	*
g.	Sent an encrypted email that has been scrambled to keep other people from reading it?	9	91	*
h.	Used an online calendar or address book to record appointments and lists of people you know	22	78	*
i.	Used software that hides your computer identity from Web sites you visit	5	93	2
J	Felt personally threatened when you were doing something online	4	96	*

ASK ALL — INTERNET USERS AND NON-USERS: [N = 2,117]

25 Now, on another subject...Do you think Internet companies should be allowed to track the activities of people who visit their Web sites, or shouldn't Web sites be allowed to do this?

%	22	Internet companies should be allowed to track activities
	63	Internet companies should not be allowed to track activities
	15	Don't know/Refused

26 Do you think all Internet companies should ask people for permission to use personal information when people give it to them, or don't you think that's necessary?

%	79	Internet companies should ask people for permission to use personal information
	15	Don’t think that’s necessary
	6	Don't know/Refused

27 Who do you think should have the MOST say over how Internet companies track people's activities online and use personal information — should it be the federal government; Internet companies; or should it be left up to people who use Web sites?

%	19	Federal government
	6	Internet companies
	62	People who use Web sites
	13	Don't know/Refused

28 How concerned are you, if at all, about...**(INSERT ITEM; ROTATE ITEMS)** — very concerned, somewhat, not too, or not at all?

Based on Internet users [N = 1,017]

		VERY CONCERNED	SOMEWHAT CONCERNED	NOT TOO CONCERNED	NOT AT ALL CONCERNED	DON’T KNOW REFUSED
a.	computer hackers, getting your credit card number online	43	25	10	20	2
b.	seeing false or inaccurate NEWS reports online	23	26	19	30	2
c.	people spreading false rumors online to affect stock prices	28	19	16	34	3
d.	having unqualified people give you MEDICAL information online	37	17	13	30	3
e.	someone learning personal information about you because of things you’ve done online	31	27	17	24	1
f.	people you meet online lying about who they really are	23	16	15	43	3

29 If an Internet company used personal information in ways that it said it wouldn't, what do you think should happen...**(READ)**

(IF ANSWERS "ALL OF ABOVE", ASK: Well, if you had to choose, which ONE thing do you think should happen? **)**

Based on Internet users [N = 1,017]

%	11	Should the company's owners be put in jail
	27	Should the company's owners be fined
	26	Should the Internet site be shut down
	30	Should the Internet site be placed on a list of fraudulent Web sites
	2	Nothing/Neither/None of the above
	4	Don't know/Refused

30 If an Internet company cheated its customers or committed a fraud online, what do you think should happen...**(READ)**
(IF ANSWERS "ALL OF ABOVE", ASK: Well, if you had to choose, which ONE thing do you think should happen?**)**

Based on Internet users [N = 1,017]

%	26	Should the company's owners be put in jail
	22	Should the company's owners be fined
	33	Should the Internet site be shut down
	13	Should the Internet site be placed on a list of fraudulent Web sites
	2	Nothing/Neither/None of the above
	4	Don't know/Refused

ASK ALL — INTERNET USERS AND NON-USERS: [N = 2,117]

31 Has anyone you work with ever been fired or gotten in trouble because of an email they sent or Web site they went to at work? **(IF YES, ASK:** Was this person fired, or were they disciplined but not fired?**)**

%	6	Yes, person was fired
	5	Yes, person was discipline but not fired
	84	No, has not happened
	5	Don't know/Refused