

Susannah Fox
“Future of the Internet”

AARP event
November 10, 2005

The Pew Internet Project is a non-partisan, non-profit research organization, funded by the Pew Charitable Trusts. We study the social impact of the internet, which means we measure who's online and what they do, but also who is not online and why. Most of our research is based on telephone surveys, which we feel provide a pretty accurate picture of the changing population. All our reports and data sets are available for free on our site: pewinternet.org.

I thought I'd start by describing the current internet population and then go into a few aspects of the future of the internet. I should also hasten to add that this speech is a departure from what the Pew Internet Project usually emphasizes. We normally focus on facts, whereas today I'll build on that with a look into my crystal ball.

Our latest data shows that while internet penetration continues to rise, the new recruits to the online army are actually veterans signing up for a second or third tour. That is, people who used to drop on & off-line are now more likely to keep their internet access. Internet users with less than one year of experience have become a rare breed online. Those who are online and those who are offline seem to be closing ranks in their respective camps. If you're on, you're on. If you're off, you're off.

(pie chart of access speeds and not online)

When we began our research in the year 2000, less than 5% of Americans had high-speed internet access at home. We just got data back this week from our September tracking survey that shows that broadband access at home is now installed for 37% of American adults. And access speed has replaced years of experience as the most significant factor in our data.

(age chart)

Age is a strong predictor for whether someone has internet access. Note that half of non-users in their 20s have been online in the past – they just currently don't have access. That's not true with people over age 65 – if they're offline, they are probably what we call “Truly Disconnected.” They have never used the internet and do not live in a connected household. Many of these people say they don't even know anyone who goes online.

One of the most striking findings in our latest study is that, despite a 10-point increase in the percentage of adults who go online over the past 3 years, the percentage of those who are Truly Disconnected remains 22%. They are overwhelmingly over age 70 and have less than a high school education. Again, if you're on, you're on. If you're off, you're off.

(education chart)

Education is also a strong predictor for whether someone has internet access and if they have high-speed access at home.

While we look at the disparities on this chart keep in mind that our research has shown that an upgrade in access speed usually upgrades that person to a higher level of usage. On a typical day, a dial-up user takes part in an average of 3 activities and a broadband user takes part in 7.

A broadband user is more likely to say they will turn to the internet first when they have a health question, rather than call a health professional. Broadband users are confident in their search abilities and many don't hesitate to use the Web to save time, to save money, and to get the best information for themselves and their families.

(future slide)

In September 2004, the Pew Internet Project sent an email invitation to a list of respected technology experts and social analysts, asking them to complete an online survey about the future of the internet. This was a very different kind of research for us. We usually stick to national phone surveys to measure the changing population. But we thought these internet pioneers and other experts could give us a new perspective on what lies ahead in the next 10 years.

There was little disagreement among experts that broadband adoption will grow and that broadband speeds will improve. Nor was there much doubt that vastly more people and objects would be linked online in the next decade. Experts envision benefits ranging from the ease and convenience of accessing information to changed workplace arrangements and relationships. At the same time, a majority of experts agreed that the level of surveillance by governments and businesses will grow.

We asked for reactions to a wide range of predictions. I'll highlight two areas today: education and security.

Experts cautioned that each new technology – motion pictures, radio, television, and now the internet – rekindles the hope that it will transform education for the better. They threw cold water on that idea.

Moira Gunn, host of public broadcasting's Tech Nation, wrote, "I do not now, and have never, witnessed successful benefits in virtual classrooms. While the role of the teacher will change from authority figure with all the information to one-on-one educational coach, the one-teacher-one-student paradigm will remain the most effective."

Another wrote, “Harvard and other major universities are not likely to go virtual. In fact, being on campus will become a thing of status. I see enhanced classrooms and dorm rooms ... but not a radical change in how learning occurs.”

Forget virtual learning for now, is most experts’ advice. However, in one of our more traditional phone surveys, we have found that people facing an education choice benefit from having access to the information available online.

(major life moment slide)

In this survey, which has not yet been released publicly, we repeated some questions we had asked in 2002 about “major life moments.” In the past two years, has the respondent dealt with a major illness, bought a new car, changed jobs, or found a new place to live, among other things. If so, then we asked follow up questions about whether the internet had played a role in that decision or event.

39% of internet users, or about 53 million adults, have gotten additional training for their career within the last two years. Of those, about 4 in 10 say the internet played a crucial or important role in going through this process or decision – about 21 million people.

29% of internet users, or about 39 million adults, have chosen a school or college for themselves or their child in the past 2 years. Of those, the same percentage – about 4 in 10 – say the internet played a crucial or important role – about 17 million people.

Interestingly, the percentage of internet users who have faced those kinds of decisions did not change much between 2002 and 2005. But the number of Americans with internet access did increase – many more people experienced the benefit of the internet’s “just in time” information flow.

That got me thinking about what would happen if there was universal high-speed, high-quality service, which is one possible future.

I thought I’d borrow from the Global Business Network’s playbook and make up some news headlines from that “rising tide” future of universal access to information about education opportunities:

- “Unemployment drops to an all-time low as millions find job training opportunities online.”
- “College application process streamlined by a partnership between eHarmony and Princeton Review which yields perfect matches between students and schools.”

Of course there is another possible future – that internet access stagnates and even declines as fewer Americans are able to afford good access to the internet or some other unforeseen event, like a devastating attack on the network, occurs. Here are some news headlines from that possible future:

- “Last known American IT worker was laid off yesterday, but already has a new job... serving Mochaccinos as Dulles Airport.”
- “Britney Johnson, age 18, sets new record by submitting applications to 341 colleges. ‘I just didn’t know how to choose,’ she says.”

(spyware slide)

The second topic I wanted to touch on is network security and our evidence that internet users may be changing their behavior out of concern about bad things happening to them online.

In a survey last spring, we wanted to know if the threat of software intrusions was changing people’s behavior online. Spyware, by the way, are those programs that can sneak onto your computer as you download a fun screensaver. The spyware program can then send reports about your activities and even what’s on your hard drive back to a central source.

34% of internet users, or about 47 million American adults, say they have had a spyware program on their home computer.

61% of those people say spyware is a serious threat to their online security.

By contrast, internet users who say they have not experienced spyware are less likely to view spyware as a serious threat and more likely to say it’s just part of life online.

This attitude difference is showing up in online behavior.

Overall, 9 out of 10 internet users say they have made at least one change in their online behavior to avoid getting unwanted software programs like viruses and spyware on their computer. This chart shows 4 of the evasive actions that people say they have taken to avoid software intrusions. Note that people who have had direct experience with spyware are more likely to say they have taken action. And they may actually be acting rationally. Holding all other factors constant, internet users who engage in the following activities are more likely to have had spyware or adware on their computer: visiting adult sites, downloading computer programs, playing online games, downloading music, sharing files, downloading computer games, downloading screensavers, and buying a product online. If an internet user avoids those activities online, he may be able to reduce his chances of contracting spyware.

The far left column shows the percent who have who stopped visiting particular Web sites. Fully 60% of spyware-sufferers say they have curtailed their use of certain sites. (After we released this report, I got my first and only interview with Adult Video News. The reporter was especially interested on behalf of his readers, who maintain adult sites. As you may know, the adult industry is often on the cutting edge of technology adoption – they get credit for the proliferation of VCRs, they were among the first to do

transactions online. If the porn industry is watching this trend, it's a good bet that most of you should be too.)

The next column shows the percent who stopped downloading software from the internet – a chilling statistic for some vendors.

The “P2P” column shows the percent who stopped downloading music or video files from peer-to-peer networks. The recording industry may be jumping for joy about this development – their lawsuits and spyware form a sort of one-two punch on peer-to-peer activities.

The far right column shows the percent who started using a different Web browser. By the way, we found that about 9% of internet users have Firefox installed, which jibes pretty well with what NetApplications has found using Web traffic statistics.

The choices that consumers are making illustrate Alan Westin's findings about the importance of context.

Westin has found three types of people:

- Privacy Fundamentalists. These are people who are strongly resistant to any further erosion of their privacy. Walt Mossberg, the tech columnist for the Wall Street Journal, may fall into this camp since he thinks that cookies are spyware. Privacy Fundamentalists make up one-quarter of Americans.
- Privacy Pragmatists make up about two-thirds of Americans and are willing to entertain trade-offs – discounts in return for allowing their purchases to be tracked, for example.
- Privacy Unconcerned. One in ten Americans. They would probably give up their Social Security Number for a free t-shirt.

At a telcom policy conference I attended last month, I heard a speech by Randal Picker, a law professor at the University of Chicago. He was discussing peer-to-peer networks and the Grokster decision, but I think his insights will help us think about the future of security as well.

In the 1970s, centralized processing was coupled with centralized control, a Soviet-style computer architecture. Computers were huge, lumbering and highly secure – they took up a whole room and very few had access to the network, just as in the Soviet Union, few had access to power. In the 80s, we moved to distributed processing power in freestanding PCs. Viruses could be transferred on floppy disks, but it was hard to proliferate a really bad virus – as Picker says, the “transaction costs” of what we used to call the “sneaker net” were too high. In the 1990s, the internet exploded access to half the population – it was every man or woman for themselves in the thrill of hooking in to the network, just as in Russia, democracy burst on the scene with all the messy aftermath of that explosion of access. Crime runs rampant, some get very rich and others lose their footing.

One possible future is to continue to let things go – again, every man or woman for themselves. In that case, you might see a lot more charts like this one – examples of how consumers are turning away from some aspects of the internet. People might shun the open internet in favor of “walled garden” solutions where they feel safe, not trying new things, sticking to the straight and narrow online. Some consumers might respond with guerrilla tactics, creating all sorts of online identities and throwing up what they think are security gates in their attempts to stay one step ahead of the intrusions and privacy violations. Some organizations here might benefit in that every man for himself scenario, providing safe havens and security tools for the individual.

Again, borrowing heavily from the AARP session last spring, here are some news headlines for that possible future:

- “Pew survey finds that 85% of internet users feel helpless”
- “Privacy consultant in Manhattan now charges \$1,000 per hour to safeguard home networks and finds she can’t keep up with demand”

Another possible future is to enforce a clampdown – email authentication, mandatory patches and the like so that some uninformed individual doesn’t allow their computer to become the spam node of the universe. A return to the “good old days” (or “bad old days” depending on your perspective) of command and control over the network. My hometown of Princeton, NJ, was recently found to be the epicenter of zombie PCs. Symantec released a report that in September, Princeton had the highest percentage of bot-infected computers in the Americas, which might be related to the influx of students back to Princeton University. Should the university clamp down on those students? Should the university be held responsible for the clueless actions of their students who allow their computers to become infected and remotely controlled?

Here are some headlines from this “command and control” future:

- “Salem, Massachusetts, returns to public shaming practices. Citizens found to have opened an unknown email attachment are put in the stocks for one full day”
- “California defunds its own university system in retaliation for gross negligence in network practices”
- “Unemployment hits historic low as the new Department of Network Security hires thousands to enforce the new 100% Compliance Act of 2007”

Again these are just two possible futures for cyber security. You might think about how your organization would react to each of them – or how other scenarios would affect you.

(Last slide)

The Pew Internet Project can provide data about the present and I’d be very interested in your thoughts about the future. Thank you.