

POSITION PAPER

From

CONSUMER REPORTS WEBWATCH

<http://www.consumerwebwatch.org>

For the

**National Science Foundation/OECD Workshop, *Social and Economic Factors
Shaping the Future of the Internet***

January 31, 2007

Report Date: Jan. 23, 2007
Consumer Reports WebWatch
Beau Brendler, Director
101 Truman Avenue
Yonkers, New York 10703
(914) 378-2600
consumerwebwatch@consumerwebwatch.org

Increasing numbers of Americans are altering their Internet behavior in response to concerns about identity theft, privacy, security, online predators, fraud and other problems.¹ As of late 2005, almost a third of U.S. Web users over 18 (30 percent) said they have reduced overall Internet use and, more specifically, a quarter (25 percent) said they have stopped buying things online.²

It is not difficult to understand why. Current cultural and economic factors have placed a burden on the home computer user to a degree that he or she must develop significant expertise in complex topics of computer and information security, information value assessment and media literacy in order to safely and effectively operate computers at home. Some have fallen victim to identity theft or fraud, or at the least, have been annoyed by spam or malware.

Yet a recent national survey shows only 21 percent of U.S. households have installed basic home computer security measures such as a firewall.³ Web users frequently proclaim frustration that the Web contains a lot of information, but not a lot of it particularly valuable, especially on critical matters such as health. The rise of decentralized, unfiltered media, characterized by blogs, vlogs and community sites such as Flickr, has dramatically increased options for finding information, entertainment and distractions, while calling into question the credibility of content created by authors with little or no training in basic principles of information quality.

As the Canadian newsmagazine *Macleans* said in a controversial October 2006 article titled, "Pornography, gambling, lies, theft and terrorism: The Internet sucks – where did we go wrong?":

The idealists who conceived and pioneered the Web described a kind of enlightened utopia built on mutual understanding, a world in which knowledge is limited only by one's curiosity. Instead, we have constructed a virtual Wild West, where the masses indulge their darkest vices, pirates of all kinds troll for victims, and the rest of us have come to accept that cyberspace isn't the kind of place you'd want to raise your kids. The great multinational exchange of ideas and goodwill has devolved into a food fight. And the virtual marketplace is a great place to get robbed. The answers to the great questions of our world may be out there somewhere, but finding them will require you to first wade through an ocean of misinformation, trivia and sludge. We have been sold a bill of goods. We're paying for it through automatic monthly withdrawals from our PayPal accounts.

Let's put this in terms crude enough for all cyber-dwellers to grasp. The Internet sucks.⁴

¹ Consumer Reports WebWatch, "*Leap of Faith: Using the Internet Despite the Dangers*," Oct. 26, 2005, p. 19. <http://www.consumerwebwatch.org/dynamic/web-credibility-reports-princeton.cfm>

² *Ibid.*

³ State of the Net Survey 2006, Consumer Reports Magazine. http://www.consumerreports.org/cro/electronics-computers/online-protection-9-06/state-of-the-net/0609_online_prot_state.htm?resultPageIndex=1&resultIndex=1&searchTerm=state%20of%20the%20net

⁴ *Macleans*, Oct. 30, 2006.

http://www.macleans.ca/topstories/life/article.jsp?content=20061030_135406_135406

Many have characterized Macleans' essay as something of a screed. But in the context of the National Science Foundation/OECD workshop, this point is made: Consumers have endured more than a decade of hyperbolized promise about the capabilities of the Internet to transform their lives. It is true the Internet has transformed aspects of modern life in a number of ways, but its full potential has not yet been reached. Unless some significant changes occur, consumer dissatisfaction and distrust may limit the Web's transforming potential to a sort of walled garden for the business and economic elite, while the home user must fend for himself or herself in less desirable real estate.

Three areas need attention:

1. **Privacy.** Evidence mounts that consumers are surrendering personal information and, concurrently, privacy, without knowing how and to what degree.⁵ At the same time, consumers cite privacy as a major concern and value. Further, lack of consumer awareness has created a situation in which consumers tolerate surveillance in the online world they would not tolerate offline. It is not unrealistic to assume a relentless online collection of data, from mundane behavior cues to personally identifiable information, could one day create an environment in which several data sets compiled discretely could easily be aggregated into a single profile, laying bare any number of attributes no reasonable person would publicly admit.⁶ The Center for Digital Democracy and the U.S. Public Interest Research Group recently published a set of recommendations to the U.S. Federal Trade Commission to address these issues. We believe they are succinct and appropriate, broadly applied: Investigate the online marketplace in light of new developments in the field; expose marketing practices that compromise user privacy; issue the necessary injunctions to halt current practices that abuse consumers; and create policies and recommend federal legislation that prevents such abuses in the future.⁷ With its extensive experience in cross-border issues, the OECD can be a force for balancing and harmonizing privacy protections internationally. Consumer privacy protections in Europe are far more stringent and detailed. At the same time, some international companies have begun locating server operations in the United States in an attempt to circumvent European privacy protections. American consumers would benefit from European-style privacy regulations and organizational or governmental oversight. European consumers would benefit by retention of privacy protections in place.
2. **Meaningful consumer education.** Continuing increases in the numbers of consumers defrauded by phishing, Nigerian 419 and other scams, and the proliferation and increasing virulence of spyware, demonstrate that current methods of consumer education about online hazards are ineffective. The average

⁵ Turow, Hoofnagle, Mulligan, Good, Grossklages, *The FTC and Consumer Privacy in the Coming Decade*. Technical report, November 2006. <http://www.truststc.org/pubs/142.html>

⁶ <http://www.democraticmedia.org/PDFs/FTCadprivacy.pdf>

⁷ <http://www.democraticmedia.org/PDFs/AFTechadeFAQs.pdf>

consumer comes armed with little more than a few hastily-typed, poorly formatted “read me” text documents or quick-start tutorials when purchasing a new piece of hardware or software. We recommend computer hardware and software manufacturers be encouraged to provide meaningful and useful “out-of-the-box” education material “in-the-box” with their products. The materials should be developed in consultation with usability experts and consumer advocates, not exploited as a venue for marketing. Consumers buying computers and entering the online world are expected to rapidly gain a depth and breadth of knowledge about machine operations unprecedented in any other category of consumer product. As points of entry into the home may become concentrated into a single cable, signal or satellite feed that provides computer, entertainment and telecommunications services, so should consumer safeguards come built into hardware and software.

3. ***Potential access limits by corporate interests.*** “Net neutrality” must be maintained and enforced, or else, in theory, broadband providers could block Web sites with political viewpoints they disagree with, or could slow down sites of companies they are not affiliated with, in order to drive a casual browser elsewhere. If users want to run certain Web browsers, Internet providers should not be able to force use of their Web browser. Someone shopping for a refrigerator should not be limited to an access provider-preferred store. Internet Service Providers should remain neutral. In the United States, telephone companies are prohibited from discriminating against content offered over their basic telephone connections. However, those prohibitions might not apply over DSL or fiber-optic networks. U.S. cable companies are not covered by any requirement. Instead, the U.S. Federal Communications Commission says Internet freedom principles are statements of their policy, but the agency has no built-in enforcement mechanism. The Internet should not be held hostage by broadband giants. Government and other organizations need the ability to enforce restrictions with substance. For instance, when a small local U.S. telephone company, Madison River, blocked DSL customers from using Vonage service in 2004, the FCC stepped in. Madison River stopped the practice and paid a fine. But the regulations that explicitly banned blocking have since been overturned. Currently, a statement of FCC policy prohibits similar blocking, but it remains unclear how the FCC might make future enforcement decisions. Other companies, like ClearWire, a wireless broadband company that serves many customers who can get broadband nowhere else, blocks Vonage and other VOIP providers, but not their own affiliated VOIP service. In Canada, the major phone company that dominates the western-half of the country, Telus, was in the midst of a labor dispute and blocked their customers from visiting a website sympathetic to its union.⁸ These types of blocking efforts are bad for consumers and should be considered in any conceptual discussions of an Internet for the future.

⁸ HearUsNow.org, Internet Issues. Consumers Union. <http://www.hearusnow.org/internet/5/>