pc monitor

Walt Crawford
RLG

Firefox and Future Dangers: The Open and Closed of It

An open marketplace serves libraries as it serves everyone else; a future of closed and controlled technology has its charms for system administrators and copyright holders but harms everyone else.

What the heck is Firefox? A year ago, that was a reasonable question. Six months ago, it would suggest you didn't spend much time online. Now—well, I suppose there's some of you who don't know that Mozilla Firefox is the hottest Internet browser around.

Firefox may be the most successful example of open source software in the personal computer market. I'm not going to write a column about the wonders of open source, partly because I'm not a true believer. A little Web searching will yield more propaganda and advocacy than you'd ever want to read, some of it thoughtful and eloquent.

Instead, I want to consider two related topics: Firefox as an illustration of the benefits of an open, complex, competitive PC marketplace—and the forces working to close the open PC architecture. An open marketplace serves libraries as it serves everyone else; a future of closed and controlled technology has its charms for system administrators and copyright holders but harms everyone else.

OPEN SOFTWARE CHALLENGES MICROSOFT

Firefox is a Web browser.

Yawn.

Who cares about another Web browser?

Internet Explorer (IE) comes with your PC; Safari comes with your Mac. Both work. There's Opera, but the free version annoys you with ads, and both versions have difficulties with too many Web sites. Netscape seems old hat and mostly a sales tool for AOL/Netscape services. I've tried Netscape. I've tried Opera. I always came back to IE because it was faster and more reliable, despite its worrisome vulnerabilities.

Why Firefox?

Firefox is different. It's lean, clean, fast, and surprisingly feature-filled.

At work, I use Firefox 1.01 for 99 percent of all Internet work. The only exception: Onyx, our customer relations software, which is coded so that you can only log in from Internet Explorer.

At home, I have Firefox installed. As soon as I get broadband, I'll use Firefox for 90 percent of my home Internet work. Why 90 percent? Because iNotes, the Web Lotus Notes e-mail client, only runs on Internet Explorer. I check work mail from home. With dialup, once I've checked work mail, it's not worth the trouble to switch browsers. With broadband, I'll do it.

I don't hate IE...but Firefox seems to work better and should be substantially less vulnerable to attack.

Firefox supports tabs: You can open many different sites simultaneously in different tabs, labeled across the top of the screen. Tabs should be less resource-intensive than multiple windows. Firefox auto-senses RSS feeds: If a site has a feed, there's an RSS logo in Firefox's bottom-right corner, which you can click to activate the feed. It uses Ctrl+ and Ctrl- to change text sizes instead of IE's arbitrary five-level pull-down menu.

Firefox's native security is better than IE's. It comes configured to block unrequested pop-ups. Its default settings for blocking third-party cookies are at least as good as IE6's settings.

What's most interesting about Firefox is what it's not. It's not an "Internet suite" like Netscape. It's a browser, period. You want a mail client? There's a Thunderbird extension (if you don't use Outlook/Outlook Express). Want to edit Web pages from within your browser? An extension is in beta. Firefox itself is small (less than 7 megabytes), fast, very standards-compliant, and clean.

I like it. So do lots of other people. The logs for Cites & Insights [http://cites.boisestate.edu/] for the first 2 months of 2005 show Firefox with 13.6 percent of the traffic: the first time anything other than Internet Explorer has ever been higher than 5 percent. (Safari accounts for 1.6 percent.) I've heard that Firefox has passed the 10 percent mark at many other sites. Firefox comes from the Mozilla Foundation, so you should find the Firefox code in Netscape 7.x—but I'd suggest going directly to Firefox [www.mozilla.org/products/firefox].

SHOULD MICROSOFT CARE?

Some industry analysts claim that Microsoft will stomp out Firefox with the next release of Internet Explorer—but some industry analysts can't stand the idea of more than one successful product in any category. I suspect a lot of us (maybe 15 percent, maybe more) are nervous enough about Microsoft hegemony that we'll stick with first-rate competitors when there's no downside. It's going to take a lot for Internet Explorer 7 to win me back—and I like Microsoft products such as Word.

I don't understand why Microsoft should care. Microsoft earns the same revenue from Internet Explorer as the Mozilla Foundation does from Firefox: None. Both are free. Every Windows PC will continue to have IE—there's no way around that. This probably means IE will always have more than half of the browser market: Many, probably most, PC users have better things to do than find and download superior browsers. Apparently, most PC users can't even take the time to add firewalls and antivirus software; something as minor as a better browser doesn't begin to compare.

Microsoft should want some visible, successful competition. It claims not to be a monopoly. Firefox helps to show that it's not. But I'm not privy to Microsoft's thinking.

A CLEANER INTERNET EXPLORER?

Thanks to Firefox, I suspect, the next IE will be leaner, cleaner, faster, and more secure. I wouldn't be surprised to see tabs and RSS autosensing. IE will be more like Firefox.

IE will continue to have the advantages of tight coupling. If I click on a comma-separated-values (.CSV) file in Firefox, I get a text display of the values; in IE, Excel pops up automatically, displaying the .CSV values as a spreadsheet. That's one example; there are others. I'm guessing the tight coupling will also mean IE will continue to be more vulnerable to attack; I hope I'm wrong.

COEXISTENCE AND COMPETITION

Competition and coexistence are good things. Open competition is even better. Intel-based personal computers, with Windows' relatively open architecture, have provided a marvelously open platform for hardware and software development of all varieties, with several winners in some categories.

Word dominates the text-handling field right now, but that hasn't always been the case. I was seduced by Word back in 1988, when I had to use WordPerfect for some projects (and hated it) and used PC-Write and The FinalWord II when I had a choice. To me, Word just made sense as a writer's tool, at a time when WordPerfect owned the market.

On the other hand, I tried Microsoft Publisher and found it lacking, and it doesn't dominate the desktop layout market by any means. Microsoft doesn't always win—and when Microsoft does win, it isn't entirely because of bundling. Microsoft doesn't even enter most specialized software fields, and that's probably a good thing.

Firefox can coexist with IE; competing applications frequently coexist with market leaders. While Windows may not be as purely open a software platform as UNIX/Linux, the PC platform itself is remarkably open.

THE THREAT TO OPEN ARCHITECTURE

This could change. One leading threat to the open nature of personal computing goes by an unlikely name: the broadcast flag. The other current set of threats consists of various anti-peer-to-peer legislation and court cases.

Sure, personal computers compute—behind the scenes for almost every task, up front when you're using a spreadsheet, tax program, or accounting software. But what PCs do more than anything else is copy. If you read this column online then choose to print it, consider the number of copies involved:

When you click on the appropriate link, you're copying the text (in HTML form) from the Web site to your PC's memory.

That same click instructs your computer to copy the text from the PC's memory to your display, transforming HTML to screen layout along the way.

If you save the file for further use, you're copying it from PC memory to the hard disk—and when you display it or print it, you're making two more copies (to RAM and to the screen or printer).

The Internet is also a magnificent copying machine; otherwise, you couldn't get the text so easily. The whole architecture of the Internet promotes copies. You could say that copying files from one machine to another—and determining which file on which machine should go to what location on what other machine—is really all the Internet does.

Copying mechanisms are so fundamental to personal computing that you don't even think of them as copying. Hardline copyright people—those who believe that the holder of a copyright should be able to control all use of the material under copyright—see it differently. They see a system for making copies, which is inherently a system well-adapted to making copies that infringe copyright.

Peer-to-peer (P2P) copying is the most dramatic example of this situ-

ation. P2P copying is not illegal. There's nothing illegal about offering a file to be copied (uploaded), and there's nothing illegal about copying such a file (downloading). But Big Media and its supporters consistently demonize P2P systems on the basis that the systems are fundamentally no more than tools for infringing copyright.

Attempts to legislate P2P out of existence get a lot of attention. Such attempts can only work by locking down the architecture of the Internet—making it a more closed architecture—or by restricting the abilities of the PCs that connect to it (making them closed and controlled architectures).

THE BROADCAST FLAG

Although the U.S. Congress has been remarkably willing to bend balanced copyright so that it favors copyright holders and Big Media at the expense of citizens, it has—so far—been unwilling to lock down personal computing and Internet architectures to prevent copying.

So Big Media went a different route: regulatory agencies, specifically the Federal Communications Commission (FCC). The opening salvo is the broadcast flag, a rule adopted by the FCC and scheduled to take full effect as this issue appears (July 2005). The broadcast flag is a tiny bit of data at the beginning of a digital TV broadcast that can assert limitations on how, how often, and for what period one or more copies of the broadcast can be made, retained, and used.

The FCC rule, if it stands, means that any receiver capable of receiving digital TV and made on or after July 1, 2005, must recognize and obey the broadcast flag. That's bad enough: It inherently restricts fair use rights that have always been implicit in over-the-air broadcast materials. However, it's worse: To "obey" the broadcast flag, the digital receiver must assure that the next device in the chain—for example, a digital video recorder, DVD recorder, PC-based recorder, or in-house wireless network—also obeys the flag. And, of course, that device must assure that any other device in a real or possible chain obeys the flag.

There's the threat to open PC architecture. Every device capable of copying or storing digital TV signals (which means almost everything in a PC except speakers, keyboard, power supply, and mouse) must be certified as meeting broadcast flag requirements, if any digital broadcast is ever to enter the PC. That gives the FCC control over most aspects of personal computers—and DVR, DVD recorders, or whatever.

Here's a trivial example: You won't be able to play back a DVD burned on a flag-compliant system and containing a broadcast that has a flag on any existing DVD player—because none of those players can be flag-compliant. But the overall effects of locking down digital processing streams capable of video bandwidth are much more devastating.

It's not just video. The RIAA is already demanding a similar broadcast flag for in-band high-resolution audio broadcasts. The MPAA has made it clear that it wants to close the "analog hole"—the procedure by which you can convert a protected digital medium to its usable analog form (video stream or audio), redigitize it with some loss in quality, and wind up with an unprotected digital recording.

There is no way to close the analog hole without locking down the open architecture of the personal computer. It doesn't require much analysis to recognize this. A fully "copyright-protective" computer architecture could only work by preventing any use of files that aren't certified as carrying explicit copyright permissions. What isn't explicitly permitted would be forbidden: That's the only way to close the analog hole.

The American Library Association (ALA) and eight other groups (including SLA and the Electronic Frontier Foundation) sued to overturn the broadcast flag, claiming that the FCC exceeded its authority and that the flag is an unworkable solution for a nonexistent problem. As I write this, the oral arguments were just heard in a district court. By the time you read this, the decision may have come down—and with luck, it will prevent the broadcast flag from taking effect.

That won't be the end of the story. Those who want absolute control over the creations they own have made it clear that they'll continue to seek absolute protection. That absolute protection can only come by locking down PC architecture. I've discussed the broadcast flags and similar threats to balanced copyright and open technical architectures at some length in *Cites & Insights*; the annual indexes will guide you to appropriate articles.

Walt Crawford *[wcc@notes.rlg.org] is senior analyst at RLG.*

Comments? E-mail letters to the editor to marydee@xmission.com.

Broadcast Flag Defeated

On May 6, 2005, the U.S. Court of Appeals for the District of Columbia circuit ruled unanimously that the FCC exceeded its authority in establishing the broadcast flag. "We grant the petition for review, and reverse and vacate the *Flag Order* insofar as it requires demodulator products manufactured on or after July 1, 2005, to recognize and give effect to the broadcast flag." The American Library Association and its co-petitioners won.

Consumer and balanced-copyright groups were jubilant, although some noted that the fight will now return to Congress. A few pessimists assumed that Congress would ram through legislation to enforce the broadcast flag almost immediately—but that seems unlikely. Consumer organizations, electronics and computer manufacturers, library associations, and a whole range of others have become much more aware of the dangers of copyright extremism than they were when the Digital Millennium Copyright Act passed in 1998.

ALA and its allies cited three grounds for striking down the broadcast flag order. The court chose to rule on just one of the three—leaving the other two open in the unlikely case an appeal is successful. For now, design innovation continues to be an open field.