Anonymity

During the workshop, it was mentioned on several occasions that P2P companies were actively promoting features intended solely to subvert copyright law enforcement, the primary example of which being "total anonymity". And while total anonymity would make it more difficult for the government or the RIAA/MPAA to track down so-called copyright violators, it is important to realize that anonymity also serves the greater purpose of providing general privacy to users. The same anonymity that makes it difficult for the RIAA to find out what I am searching for and downloading also makes it difficult for my neighbor. It is dangerous to suggest that simply because I want privacy on the internet or in my home, I am scheming to break the law. This basic fact was glossed over in the workshop by various panelists in an attempt to paint P2P companies as agents simply looking for ways to escape law enforcement.

Software to allow more anonymity on the internet is becoming increasingly common and popular. Browsers are allowing users to have better control over identifying cookies stored on their computers. Projects like the EFF's Tor system for anonymous internet communication are becoming more popular for savvy users. Encryption features are being built in to e-mail clients. It is not just P2P companies. And it is not just to break the law.

EFF Tor
http://tor.eff.org/

Browsers with cookie control (partial list)
Internet Explorer, Mozilla, Firefox, Safari, Camino, OmniWeb

E-mail clients with S/Mime or PGP encryption
Outlook, Mac OS X Mail.app, Eudora

Firewalls

It was mentioned several times that P2P software goes out of its way to "poke holes" in firewalls, as though this were an innately mischievous act. These comments either represented attempts to spread fear or demonstrated an egregious misunderstanding of the technology at hand. The purpose of firewalls is to control and deny _unwanted_ network traffic. If I don't want people on the internet to have the ability to print on my printer or attempt to log in to my computer, I can set up a firewall to block these specific network access ports. In the case of people using P2P software, people *want* the software to be able to use the network and subsequently open the appropriate ports on their firewalls. Just as I allow outgoing port 80 connections on my firewall so I can browse the internet, I allow port 6881 connections so I can use BitTorrent to download Linux distributions. It is not mischievous. It is *desired* functionality.

Musician Advocacy

I was severely disappointed with the use of a musician/songwriter (Wood Newton) to one-sidedly spread the propaganda of the RIAA at the workshop. To paraphrase, "We don't refer to them as file-sharing networks, we call it file-stealing". There are already artists earning plenty of money through internet downloading and P2P networks. There are also many, many largely unknown artists who would refer to file-sharing as the best way they have encountered to distribute the music they just want to be heard. The voices of these musicians and artists were not represented. Finally, it was ironic that Mr. Newton's answer to the RIAA giving him only a tiny sliver of the pie made with his song writing was to try to become the middle-men that the RIAA business model has proliferated. Instead, I would suggest that there are other business models out there for artists to capitalize on.

Links to pages of artists' support of P2P:
http://www.eff.org/share/
http://www.moby.com/
http://www.moby.com/cms/viewdiary.asp?Diary_ID=1421&ViewType=Current
http://www.pewinternet.org/pdfs/PIP_Artists.Musicians_Report.pdf

Spyware/Adware/Viruses

Several panelists attributed the phenomenon of spyware and adware to P2P file-sharing and implied that P2P software bundling was the primary source of spyware and adware. However, Jules Polonetsky's slide shows us that computers without file-sharing programs installed on them still had, on average, 82 pieces of spyware/adware. There is clearly large force at work here, and it is not P2P software.

P2P software was also portrayed as a large virus threat without much evidence to support that claim. In contrast, here is a summary of the "most frequent, high-impact types of security incidents currently being reported to the [United States Computer Emergency Readiness Team]":

Santy Worm - a worm compromising web servers exploiting a vulnerability in some versions of phpBB bulletin board software.

W32/Zafi.D - a Zafi variant spread through attachments to e-mails containing a holiday greeting message. This virus does also attempt to spread through P2P sharing networks by copying itself as 'winamp 5.7 new!.exe' or 'ICQ 2005a new!.exe' into certain folders.

W32/Sober Revisited - variants of W32/Sober spread through e-mail attachments.

W32/MyDoom Revisited - variants of W32/MyDoom spread through e-mail attachments, virus-initiated TCP communication, and an exploit of a Microsoft Internet Explorer IFRAME vulnerability.

W32/Bagle Revisited - variants of W32/Bagle spread through e-mail attachments.

Exploit for Microsoft GDI+ JPEG Parser - a vulnerability where a JPEG image is able to execute arbitrary code with the privileges of the user. This vulnerability exists in Microsoft Internet Explorer, Office, Outlook, Outlook Express, and Windows Explorer as well as any program using the GDI+ library to display JPEGs. Displaying an image with the ubiquitous JPEG format can be made to execute arbitrary code on your computer.

W32/Sasser - a worm the exploits a vulnerability in the Windows Local Security Authority Service Server and allows a remote attacker to execute code with SYSTEM privileges.

Exploitation of Outlook Express MHTML cross-domain scripting vulnerability - an exploit of the Outlook Express MHTML handler that allows an attacker to execute arbitrary code with user privileges by convincing the victim to view an HTML document (web page, e-mail).

You will note that only one of eight has any P2P software involvement at all and that it is not the primary vector for propagation. Let us concentrate on the elephant in the room of virus threats and not force blame on P2P software.

US-CERT
http://www.us-cert.gov/current/current_activity.html