



**CDT Comments:
FTC December 2004 P2P File-Sharing Workshop**

November 15, 2004

Office of the Secretary
Room 159-H
600 Pennsylvania Avenue N.W.
Washington, D.C. 20580

Re: P2P File-Sharing Workshop – Comment, P034517

The Center for Democracy and Technology (CDT) applauds the Federal Trade Commission for taking up the difficult but extremely important consumer issues surrounding peer-to-peer file-sharing. We believe there is a constructive role for the Commission to play on these issues, and we appreciate the opportunity to comment for the Commission’s December 2004 workshop.

CDT is a non-profit, public interest organization dedicated to preserving and promoting free expression, consumer privacy, and other democratic values on the Internet. CDT has been active in the policy debate surrounding protection of copyright in the digital age, on the protection of consumer privacy online, and on the problem of so-called “spyware” applications,¹ all of which are implicated by peer-to-peer file-sharing.

Peer-to-peer applications, including file-sharing programs, are powerful programs with great benefits for consumers. At the same time, file-sharing applications have fueled a significant piracy problems and raise real privacy and other concerns for Internet users. The FTC has a role to play in addressing these complex issues and helping to protect consumers, while making sure not to chill what is fundamentally a consumer-friendly and empowering technology.

More specifically, we believe important consumer issues raised by peer-to-peer applications include:

¹ See, e.g., Center for Democracy and Technology, *Mapping the Digital Video Copyright Landscape: Stakeholder Interests and the Internet* (March 2004), available at <<http://www.cdt.org/publications/copyright-matrix.pdf>>. Testimony of Alan Davidson, “Peer-to-Peer File Sharing Privacy and Security,” before the House Committee on Government Reform (May 15, 2003) (“CDT P2P Testimony”). CDT Testimony, FTC Spyware Workshop (April 19, 2004), available at <<http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf>>.

- **Privacy** – Peer-to-peer systems make it possible, and in some cases too easy, for people to share personal files. There is evidence that users of major peer-to-peer networks are inadvertently sharing sensitive documents like their tax returns, inboxes, or electronic check books. More work must be done to help consumers protect their privacy on peer-to-peer systems.
- **Spyware and Adware** – Many file-sharing programs are bundled with other applications that provide the primary source of revenue for peer-to-peer developers. These arrangements are not sufficiently transparent. Consumers deserve notice and real choices about what is installed on their computers
- **Copyright Infringement** – Massive illegal sharing of copyrighted works is a severe problem that drives much of the concern over peer-to-peer applications. In the short-term consumers must become more aware of the legal risks they face if they infringe on file-sharing networks, and peer-to-peer companies have an obligation not to obscure these risks or encourage infringement. In the longer-term, as companies seek to release content in digital form protected by rights management systems, the FTC may also have a role in ensuring that a competitive and transparent market is able to emerge.

We discuss each of these areas in greater detail below.

1. Background

“Peer-to-peer” technology is a broad category that is difficult to define precisely. In many respects, “peer-to-peer” principles are the basis of the Internet communications model. Many of the Internet’s most popular applications—instant messaging, for example—are considered to be “peer-to-peer.” Moreover, peer-to-peer designs appear to be growing only more common. A growing number of new consumer applications—from programs to share photographs among friends, to office collaboration applications—are likely to be peer-to-peer.²

File sharing software has proven to be an incredibly popular application of peer-to-peer design. Millions of people are using peer-to-peer networks today to share text, software, audio, and video files stored on their computers.³ The fundamental principle of peer-to-peer file sharing, helping users communicate directly with minimal central coordination, is consumer-friendly and empowering. This approach allows users to share data with freedom and flexibility while spreading storage and bandwidth costs across a broad user base.

² For more detailed discussion of important and beneficial uses of peer-to-peer networks, see Testimony of Gigi B. Sohn, "Piracy of Intellectual Property on Peer-to-Peer Networks," before the House Judiciary Committee, Subcommittee on Courts, the Internet, and Intellectual Property (September 26, 2002) *available at* <<http://www.house.gov/judiciary/sohn092602.htm>>.

³ A recent study even estimates that traffic from BitTorrent, a file transfer client using peer-to-peer principles, now consumes over a third of all Internet traffic. *See* Adam Pasick, “File-sharing network thrives beneath radar,” *Reuters* (November 3, 2004) *available at* <<http://www.reuters.co.uk/newsArticle.jhtml?type=internetNews&storyID=6705733§ion=news>>

At the same time, the widespread piracy of copyrighted materials over peer-to-peer applications is a severe and recognized problem. Copyrighted songs, video programs, and games have made their way onto file-sharing networks and are distributed illegally over such networks in vast quantities. Such large-scale infringement threatens to undermine the incentives so important to rewarding creators and to promoting the digital distribution of valuable content.

The policy challenge presented by peer-to-peer file-sharing applications is to combat this abuse, and to address other consumer issues associated with such programs, without undermining the great potential of these technologies or chilling the exciting new applications of peer-to-peer design.

2. Privacy

Peer-to-peer file-sharing systems are powerful tools for sharing information with millions of other people around the world. People who install these tools need to be aware of the potentially serious privacy risks that may come from their use or misuse.

Several factors heighten privacy concerns for peer-to-peer networks compared to other means of online publishing. Peer-to-peer applications are used by millions of consumers, typically with far less expertise than the average web publisher. Their powerful search capabilities can make files more widely accessible than other publishing tools. The sharing functions of these systems can be less transparent to users, especially for those unfamiliar with their workings.

Academic studies⁴ as well as CDT's own qualitative research⁵ indicate that at least some file-sharing users are sharing highly sensitive personal documents—such as tax returns, email inboxes, or check registers—on major peer-to-peer networks. These people are making financial information, personal files, and even intimate correspondence easily available to millions of other users around the world.

It is difficult to measure the extent of this problem, and we encourage the FTC to gather more data. Nonetheless, inadvertent sharing of information is a serious issue. Peer-to-peer companies bear a heavy responsibility to make sure consumers are appropriately informed when they make decisions about sharing files and have an obligation to ensure that their products are designed so as to encourage safe behavior. This includes setting defaults appropriately.

Peer-to-peer companies may have bad incentives in this regard. These companies have an interest in encouraging users to make as much content as possible available, as this increases the universe of content available on their network and thus the attractiveness of the network to

⁴ See, e.g., Nathaniel S. Good and Aaron Krekelberg, "Usability and privacy: A study of Kazaa P2P file-sharing" (June 2002) available at <<http://www.hpl.hp.com/shl/papers/kazaa/index.html>>.

⁵ See CDT P2P Testimony. The main problems appear to arise from users either placing too much in their "shared" folders or sharing large numbers of folders or even whole hard-drives.

other potential users. This pressure has, in some instances, led peer-to-peer companies to encourage inappropriate sharing or to minimize the dangers of sharing.

Vigilance for potential abuses, ongoing pressure on peer-to-peer companies to continue to improve their practices, and, above all, continued consumer education such as that already undertaken by the FTC,⁶ are all necessary to combat the problem of inadvertent sharing of personal information over peer-to-peer networks.

3. Spyware and Adware

CDT has commented extensively elsewhere, including before the FTC,⁷ on the epidemic of spyware online. The connection to peer-to-peer applications is only one part of the spyware issue, but there is no doubt that the business practices of some peer-to-peer companies have helped to fuel this problem.

Essentially all commercial peer-to-peer file-sharing services obtain their primary source of revenue from bundling arrangements with other software makers. “Adware” companies are paid by advertisers to deploy software that serves advertisements on user’s computers, typically while they browse the Internet. These companies in-turn pay peer-to-peer developers to have their software included when users install a peer-to-peer application.

CDT has emphasized that there is nothing fundamentally objectionable about ad-support as a business model. But ad-support must be implemented in a way that is transparent to users, that clearly indicates to them the bargain they are making when they download the software, and that respects their choices and privacy preferences.

Perhaps influenced by a desire to gain popularity by minimizing the apparent costs of their software, many peer-to-peer companies have not, to-date, been sufficiently up-front with their users about bundling arrangements. In some cases, the only place where consumers are given notice of the installation of “adware” components is as part of long and dense licensing agreements. Peer-to-peer companies bundling with adware have also all failed to take steps called for by CDT to remedy lack of transparency in the ongoing operation of bundled advertising support components (see Attachment A for one example).

CDT applauds the FTC’s first legal action last month against purveyors of spyware, and we hope that it presages a larger campaign against the deceptive and unfair practices that typify spyware. The FTC’s enforcement role may include actions in cases where end user licensing agreements are clearly used to confuse users or obscure material information about what is being installed. We also see a major role for industry best practices, including the measures described above. Finally, continued efforts must be made to educate Internet users about how to be smart and wary consumers of peer-to-peer software.

⁶ “File-Sharing: A Fair Share? Maybe Not,” *FTC Consumer Alert* (July 2003) available at <<http://www.ftc.gov/bcp/online/pubs/alerts/sharealrt.htm>>

⁷ CDT Comments and Request to Participate: FTC April 2004 Spyware Workshop (March 5, 2004) available at <<http://www.ftc.gov/os/comments/spyware/040305centerfordemocandtech.pdf>>. See generally <http://www.cdt.org/privacy/spyware>.

4. Copyright Infringement

Clearly the single biggest policy problem surrounding peer-to-peer networks is their use in the massive infringing distribution of copyrighted material. Given the decentralized design of peer-to-peer software, this issue is first and foremost about abuse by end users of the powerful capabilities of these programs. Peer-to-peer companies themselves bear responsibility, however, insofar as their applications and accompanying documentation may encourage infringement, and they fail to provide users with adequate warnings about the risk of lawsuits, civil penalties, and even criminal prosecution associated with such illegal file-sharing.

While peer-to-peer file-sharing raises serious concerns for content owners, for many reasons it is not easily susceptible to a quick, simple policy solution.⁸ Rather, CDT has outlined what we believe to be the three crucial elements of a long-term strategy to combat piracy, including large scale infringement by file-sharing.⁹ These are –

- **better enforcement** of existing laws against online infringers, such as the lawsuits that the RIAA and now the MPAA have undertaken;
- **increased education** of users about their rights and responsibilities in online file-sharing; and
- **new distribution models** to lawfully quench the strong demand for valuable content in digital form, based to some extent on use of digital rights management systems to protect content and enable new business models (digital rental, online “jukeboxes,” streaming, etc.).

The FTC has an important role to play particularly on the educational front: helping to raise consumers’ awareness about the legal liabilities they face for illicit file trading, informing them of their rights and obligations in sharing, and helping to ensure that makers of peer-to-peer software do not try to obscure these issues.

The FTC is also likely to have an important role as the market in legitimate online services and digital content grows to offer alternatives to illegal file sharing. Such services will be built around a variety of “digital rights management” technologies. These technologies hold out the promise of fostering an array of different online business models—rental, subscription, sale, and others not yet contemplated—that would not otherwise be possible. If DRM meets its potential, these options will give consumers a diversity of ways to access and interact with digital media.

But DRM also poses unique challenges to consumer education and competition. Such technologies are too-often opaque to users, and may be used to facilitate anti-competitive

⁸ See, e.g., Peter Biddle, *et al.* “The Darknet and the Future of Content Distribution,” presented at the *ACM Workshop on Digital Rights Management* (2002) available at <<http://msl1.mit.edu/ESD10/docs/darknet5.pdf>>.

⁹ For a somewhat more in-depth discussion of our view on this three-pronged approach, see e.g. Center for Democracy and Technology, *Implications of the Broadcast Flag: A Public Interest Primer* (Verison 2.0 (December 2003) at 34-35, available at <<http://www.cdt.org/copyright/broadcastflag.pdf>>.

business models. Part of effectively combating the peer-to-peer problem will mean fostering a robust marketplace in legal alternatives, and the FTC must aid in this goal.

Conclusion

Peer-to-peer technology, including file-sharing technology, has major benefits for consumers and is a growing part of the way people send and receive information online. Illegal file sharing, spyware, and inadvertent sharing of personal information all threaten the potential of these technologies, however. The challenge for companies, policy makers, and enforcement agencies is to find ways to combat these problems without throwing the baby out with the bathwater.

The FTC has several important roles to play in addressing these difficult but crucial consumer issues. Chief among these are educating consumers, continuing to crackdown on spyware activity, and, in the longer term, helping to facilitate the emergence of a flourishing competitive marketplace in viable alternatives to illegal trading. CDT looks forward to a constructive discussion on these issues at the Commission's workshop, and to working with all parties towards solutions to the challenges raised by growing consumer use of peer-to-peer technologies.

Respectfully submitted,

Alan Davidson, Associate Director

Ari Schwartz, Associate Director

Michael Steffen, Policy Analyst

Center for Democracy and Technology

1634 I St., NW

Washington, DC 20006

202-637-9800

<http://www.cdt.org>

Attachment A

Adware companies face a particular hurdle in making their operations and value proposition transparent to users because adware programs typically do not run at the same time as the applications (such as a peer-to-peer sharing programs) they support. Adware programs typically display advertisements while the user is surfing the web, regardless of whether the bundled application is even running. This behavior can obscure the connection between the two applications for users.

As one way to help address this issue, CDT has pushed adware companies—and file-sharing companies they bundle with—to implement co-branding, putting the names and logos of supported applications on all advertisements. Although advertisements would still appear to users out-of-context, separated from the applications they support, co-branding would at least provide an immediately visible indication of the connection to the primary application.

The mock-ups below show some ways that co-branding might be implemented. Some of these examples demonstrate better labeling than others, but they all illustrate the fundamental principle of creating a visible link between advertisements and the programs they support. To date, no adware company of which we are aware co-brands its advertisements.

*Without Co-branding
(Adware Supporting a Single Application):*



With Co-branding:



Without Co-branding
(Adware Supporting a Single Application):



With Co-branding:



*Without Co-branding
(Adware Supporting Multiple Applications):*

Instant Offer - GAIN

Now at Example.com

Save on Widgets.

Buy

GAIN. This ad is brought to you by software from the GAIN Network. It is not brought to you or sponsored by the Web site(s) you are viewing. [More info](#)

With Co-branding:

Instant Offer - GAIN

Now at Example.com

Save on Widgets.

Buy

GAIN. This ad is brought to you by software from the GAIN Network, not the web site you are viewing. It supports the following GAIN partner applications installed on your computer. [More info](#)

Amazon Precision Time Get it at Walmart