Peer-to-Peer File Sharing Privacy and Security

Testimony before the House Committee on Government Reform
Alan Davidson
Associate Director
Center for Democracy and Technology
May 15, 2003

Summary

Mr. Chairman, Mr. Waxman, and Members of the Committee, the Center for Democracy and Technology welcomes this opportunity to testify on the timely issue of privacy and security on popular peer-to-peer file-sharing systems. The use of file-sharing software can raise serious privacy problems, often through mistakes by users that result in the sharing of very sensitive personal information. At the same time file-sharing technology is largely user controlled, oftentimes beneficial, and decidedly hard to regulate. A broad public education effort and better software practices are needed in order to inform people about the risks of file sharing while preserving the benefits of this valuable technology.

CDT is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values on the Internet. Since its creation in 1994, CDT has been heavily involved in the policy debates concerning privacy and computer security online. More recently, in partnership with other consumer groups, CDT has undertaken a project to articulate balanced consumer perspectives on digital copyright issues.[1]

So-called "peer-to-peer file-sharing" systems – like the popular Kazaa, Morpheus, or Grokster applications – are among the most downloaded computer programs today. People who install these powerful tools need to be aware of the potentially serious privacy and security risks that may come from their use or misuse. Key concerns facing file-sharing users include:

- Inadvertent sharing of sensitive personal information – Peer-to-peer systems make it possible, and in some cases too easy, for people to share personal files. There is evidence on major peer-to-peer networks of users sharing very sensitive documents like their tax returns, inboxes, or check registers, certainly in most cases by mistake.
- Spyware and adware – Many file-sharing programs contain "spyware" that communicates information for advertising or other reasons, often without the user's knowledge. Whether in peer-to-peer or other software, consumers deserve notice and real choices about how their computers communicate with third parties.
- Security concerns – File trading introduces risks similar to those faced by Internet users generally. People should take care to only execute files whose source they trust, and they should safeguard their computers when online.

[1] CDT is working in partnership with Public Knowledge and Consumers Union on P2P and related copyright issues, made possible in part by the support of the MacArthur Foundation and the Robert J. Glushko and Pamela Samuelson Foundation.

- Legal risks – File traders who violate copyright laws face obvious legal risks. At the same time, CDT is concerned that at least one provision of current law – the broad subpoena power granted any copyright holder under Section 512(h) of the Digital Millennium Copyright Act – too easily allows the identity of a peer-to-peer participant or any Internet user to be unmasked wrongly or by mistake without their knowledge.

These concerns are exacerbated by the growing use of file-sharing programs by millions of individuals and families, often with little or no training or experience.

With these risks come benefits. Peer-to-peer file sharing can be used for legitimate, non-infringing file distribution. Its underlying technology, not so different from peer-to-peer networks like the World Wide Web, is rapidly evolving and being adopted for many new uses. Regulating this technology without broader ramifications would be difficult, and could have many unintended consequences.

How then do we address these real privacy and security concerns? CDT believes that an active program of education and better software practices is needed. Such a program would:

- Inform people about the risks in file sharing – The public, and particularly the families of file-trading minors, need greater awareness of the potential risks of file sharing. Educational efforts—like the Internet community GetNetWise website—are already including tips for safe peer-to-peer use that should be widely disseminated.
- Seek fair information practices in file-sharing software – Much more should be done to design peer-to-peer software with transparency and better control over shared files. Software producers should reject invasive spyware, adopt fair information practices, and must provide better notice when information is transmitted to third parties.
- Add privacy protections for DMCA subpoenas – Privacy and safety protections for end users should be included in the broad DMCA Section 512(h) subpoena provision in order to require more due process – including notice to the user and other protections– before ISPs are compelled to reveal sensitive personal identity information.
- Prevent invasive "self-help" tactics- In no circumstances should it be legal to damage another person's computer or files based on allegations of wrong-doing, including copyright infringement.

All of this should take place against the broader backdrop of action regarding Internet privacy generally, where the continued growth of privacy technologies and industry self-regulatory efforts along with baseline privacy legislation are necessary to ensure public trust and democratic values.

Congress has a valuable role to play in educating the public about the potential risks of file-sharing systems, in encouraging companies to design more user-friendly systems, and in modifying current legal provisions that create privacy risks. CDT looks forward to working with this Committee and others to further these efforts.

1. The Growing Use of Peer-to-Peer File Sharing Networks

Peer-to-peer (P2P) file sharing networks are an important and rapidly growing new channel for Internet communication. Millions of people are using P2P networks today to share text, software, audio, and video files stored on their computers. By helping users communicate directly with minimal (in some cases no) central coordination, peer-to-peer networks can allow people to share data with far greater freedom and flexibility.

While the P2P file-sharing phenomenon is relatively new, “peer-to-peer” technology underlies the Internet communications model. In many ways, the Internet is the world's largest peer-to-peer network. E-mail, the World Wide Web, and instant messaging are all “peer-to-peer” applications.

The kinds of peer-to-peer networks that are the topic of today’s hearing are the new, highly decentralized systems for sharing information stored on many distributed computers. Napster first brought P2P into the public eye; now largely defunct, its progeny like Kazaa, Morpheus, or Grokster are used by millions today.

Peer-to-peer file sharing networks differ from other Internet applications in that they tend to share data from a large number of end user computers rather than from the more central computers we generally think of as Web servers. A key innovation of peer-to-peer file sharing networks is their sophisticated mechanisms for searching millions of "shared" files to find data among many connected systems. Information on P2P networks tends to be less centrally controlled and more reflective of what end user participants believe is valuable or worth sharing.

File-sharing networks have become remarkably popular in a very short time. The leading peer-to-peer file sharing software, Kazaa Media Desktop, has been downloaded over 200 million times and claims over 60 million users worldwide, and continues to grow in popularity.[2] At any given moment, as many as 4 million users might be participating in the Kazaa network, sharing thousands of terabytes of information. Millions of others regularly use Gnutella, a related open source sharing system.

Peer-to-peer networks have become notorious for fostering piracy of copyrighted materials. A tremendous number of copyrighted songs, video programs, and games have made their way onto file-sharing networks without authorization. While outside of the scope of this hearing, CDT does not condone the widespread infringement of copyright online.

[2] "200m - Hooray!" Sharman Networks press release. March 11, 2003. Available at <http://www.kazaa.com/us/news/201.htm>. Woody, Todd. "The Race to Kill Kazaa." Wired. February 2003. Available at <http://www.wired.com/wired/archive/11.02/kazaa.html>.

Less visibly, peer-to-peer file-sharing technology can support valuable new applications.[3] Some examples include:

- **Data coordination and collaboration**. Peer-to-peer technology is being used by organizations to give workers up-to-the minute data and to facilitate group coordination on large-scale projects. For example, humanitarian groups in Iraq are using peer-to-peer technology to synchronize distribution of aid to the Iraqi people.[4] The fact that peer-to-peer systems require no central servers and minimal centralized coordination makes them ideal for use in environments with little infrastructure.

- **Lawful music sharing.** Peer-to-peer file sharing networks can help users share music lawfully. For example, Furthur Network is a non-commercial, open-source peer-to-peer file-sharing network of live music from bands such as the Grateful Dead, the Allman Brothers, and the Dave Matthews Band.[5] The network is designed so that bands who explicitly authorize the taping and redistribution of their shows can help their fans share recordings of performances from around the globe.

- **Public domain material.** Project Gutenberg seeks to distribute via the Internet thousands of works available in the public domain and other freely available works such as the King James Bible, the works of Shakespeare, and the CIA World Fact Book.[6] Peer-to-peer technology will allow Project Gutenberg and other content publishers to significant diminish the costs associated with making content available to millions of people.

These applications thrive as a result of the flexibility of peer-to-peer architectures. At the same time, with this flexibility has come new risks: infringement of copyrighted works, availability of explicit content, and questions about privacy and security.

Even as new uses are found for P2P file sharing, the underlying technology itself is rapidly evolving. New generations of file-sharing systems will be even more decentralized, support greater anonymity among users, split files among different computers, and rapidly change protocol settings to defy attempts at interdiction.[7] These changes are likely to ease some

[3] Additional details about the importance of peer-to-peer networks are available in Sohn, Gigi B. "Statement of Gigi B. Sohn, President, Public Knowledge. 'Piracy of Intellectual Property on Peer-to-Peer Networks.'" Testimony 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>.

[4] Jones, Mark. "Taking Collaboration to the Masses." *InfoWorld*. April 11, 2003. Available at <http://www.infoworld.com/article/03/04/11/15noise_1.html>.

[5] More information about Furthur Network is available at <http://www.furthurnet.com/>.

[6] More information about Project Gutenberg is available at <http://www.promo.net/pg/>.

[7] Biddle, Peter, Paul England, Marcus Peinado, and Bryan Willman. "The Darknet and the Future of Content Distribution." *2002 ACM Workshop on Digital Rights Management.* Available at <http://crypto.stanford.edu/DRM2002/darknet5.doc>.

concerns (by enhancing privacy and security, for example) and exacerbate others (by defying efforts to regulate P2P use.) As a whole they underscore the difficulty of policy-level efforts to deal with a changing and complex technology.

2. Privacy and Security on Peer-to-Peer File-Sharing Networks

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.

In many respects the problems facing peer-to-peer users are akin to the problems facing any speaker on the Internet. For example, someone who creates a website to share family pictures could inadvertently place sensitive files or pictures they don't wish to share on their site.[8] Many of us have a favorite story about someone who sent an embarrassing email message to a mailing list by mistake.

Several factors heighten privacy concerns for peer-to-peer networks. They 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 activities of these systems can be less transparent to users, especially for those unfamiliar with their workings.

Privacy risks

Peer-to-peer systems make it possible, and in some cases too easy, for people to share personal files. Two academic studies as well as CDT's own qualitative research indicates that as least some file-sharing users are sharing highly sensitive personal documents on major peer-to-peer networks.

For example, a recent study by Good and Krekelberg[9] found dozens of examples of Kazaa users who were sharing sensitive documents like their tax returns, email inboxes, or check registers, certainly in most cases by mistake. In doing so, these people are making financial information, personal files, and even intimate correspondence easily available to millions of users around the world.

It appears that much sharing of personal information is inadvertent and the result of misconfiguration or popular misconceptions about how file sharing works. For example, many file-sharing systems come with a default that files in a "shared" directory will be available to others. Some users may not realize that any files in that shared directory, often

[8] Even professional corporate web site operators have been known to inadvertently share sensitive corporate data on the web. And new web authoring tools, like Apple Computer's .mac initiative, make it even easier for consumers to share files and publish web sites.

[9] Good, Nathaniel S., 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>.

including any files they download, will automatically be shared unless they take steps to avoid sharing.

Some systems have been designed to maximize sharing. For example, many systems default at installation to allow sharing of the shared folder. They may also suggest that users find other directories to share and will assist users in doing so. Many of the most popular file-sharing systems are upgrading their systems to make misconfiguration harder. For example, while early versions of Kazaa appeared to encourage greater sharing a more recent version creates a pop-up screen demanding confirmation before sharing a whole drive (and the software appropriately suggests *not* sharing the drive, though it's default setting remains "Yes".)

Diaries, personal letters, email, and financial records are commonly found on personal computers today and could be shared inadvertently if someone were, for example, to share their whole hard drive. Once available, these sensitive files could be used to commit fraud, invade privacy, or even commit identity theft.

Though such consequences are sobering, it is important to keep the size of the problem in perspective. GAO and FTC studies on identity theft indicate that, in cases where the source of an identity theft is known, Internet or e-commerce sources constitute a very small percentage of identity theft cases.[10] To date CDT knows of no identity theft case that has been attributed to peer-to-peer file sharing problems.

CDT is also not aware of any study of the scope of file sharing privacy problems. Available data seems to indicate that the percentage of peer-to-peer users who inadvertently share sensitive files is very small.[11] This is an important area for future research.

"Spyware" Risks

A troubling privacy and security issue facing peer-to-peer file sharing networks is the use of so-called "spyware" programs."Spyware" is software that, without the user's knowledge, gathers information about an Internet user and sends that information to a third party. A number of popular peer-to-peer file sharing software programs have been found to install spyware onto user's computers, often without the user's knowledge.[12] Once installed, the programs may transmit sensitive information and are often hard to remove.

[10] U.S. General Accounting Office. "Identity Theft: Prevalence and Cost Seem to be Growing." GAO-02-363, March 2002. Available at <http://www.consumer.gov/idtheft/reports/geo-d02363.pdf>. Federal Trade Commission. "Information on Identity Theft for Consumers and Victims From January 2002 Through December 2002." Available at <http://www.consumer.gov/idtheft/reports/CY2002ReportFinal.pdf>.

[11] Most estimates of the number of users sharing sensitive files number in the dozens or hundreds. While this is significant, the total number of users connected to a given P2P file-sharing network may number in the millions. This seems to indicate that the number of people accidentally sharing sensitive files may be considerably less than 1% of all users.

[12] Metz, Cade. "Spyware: It's Lurking On Your Machine." *PC Magazine.* April 22, 2003. Page 85. Available at <http://www.pcmag.com/article2/0,4149,977889,00.asp>.

There are many forms of spyware, and not all are alike. Documented examples of spyware, include:

- "W32.Dlder.Trojan," a "Trojan horse" program capable of tracking the Web sites users visit and relaying that information to a third party. "W32.Dlder.Trojan" has been found in past versions of popular file-sharing programs such as BearShare, LimeWire, and Kazaa.[13]

- "vx2.dll," a spyware program file packaged with certain versions of Audio Galaxy, capable of capturing lists of Web site visited, creating pop-up ads, and even capturing user's input into Web forms and comment boxes -- potentially even sensitive information like credit card numbers or Social Security numbers.[14]

The Fair Information Practices provide a baseline for protection of personal information -- a baseline with which spyware does not comply. The surreptitious manner in which spyware operates denies users any opportunities for notice, consent, access, or other critical abilities. As such, spyware constitutes a significant threat to the privacy of the users of peer-to-peer file sharing networks, and of all Internet users.

Moreover, some spyware conceals itself from users and may even obstruct users' attempts to disable it. This can prevent users from even knowing what software is running on their computer, let alone take corrective action.

CDT believes that the spyware problem demands greater transparency. Users need to be notified whenever a piece of software is installed on their computer, especially one that could diminish the security and stability of their computer and the sensitive information on it. Increased transparency would permit users to make informed decisions about the software they use, and would incentivize software makers to address known flaws in their software. The fair information practices that describe how best to handle personal information can and should be applied as well to the technologies that collect personal information.

Security Risks

Users of P2P file-sharing systems face many of the same security risks as other Internet users. Just as in other applications, P2P users must take care to only run programs from sources that they trust, and should be careful to check for viruses. They should safeguard their computer from attack when online. File sharing adds an extra dimension to these concerns due to the quantity and frequency of files traded, the relatively unsophisticated user base, and the rise of self-help systems to prevent copyright infringement. At this time, P2P

[13] Delio, Michelle. "What They Know Could Hurt You." *Wired News.* January 3, 2002. Available at <http://www.wired.com/news/privacy/0,1848,49430,00.html>.

[14] Benner, Jeffrey. "Spyware, In A Galaxy Near You." *Wired News.* January 24, 2002. Available at <http://www.wired.com/news/technology/0,1282,49960,00.html>.

file-sharing applications are not known to be any less -- or any more -- secure than Internet applications on the market in other areas.

Viruses - Because peer-to-peer file sharing networks enable files to be transferred among millions of computers -- most of which are owned and operated by total strangers -- there is an ever-present risk that files downloaded from a peer-to-peer file sharing network could carry various kinds of malicious software like viruses and "worms."

It is, of course, possible to receive a dangerous file in numerous ways, such as over the Web or by e-mail. The best protection against viruses continues to be the use of up-to-date anti-virus software. 100% protection can never be achieved, but users should be aware that to download files without adequate protection opens them up to substantial risks.

Online Attacks **-** When peer-to-peer networks identify shared files to millions of users, they also identify the location of a user's computer, and could even target that computer's IP address (Internet Protocol address) with attempts to gain access. This is not a risk unique to peer-to-peer file sharing networks; <u>all</u> Internet communications involve an exchange of IP addresses. But because peer-to-peer file sharing networks search millions of computers, they can provide access to millions of IP addresses.

“Self-Help” Attacks – A new form of security threat may be growing for peer-to-peer users in the rise of “self-help” techniques by copyright holders concerned about infringement on file-trading networks. More benign versions flood P2P networks with bogus copies of copyrighted works in order to fool people into downloading or storing them. Such practices are considered legal because they do not disrupt the technical operation of a person's computer or networks.

Some companies are reportedly pursuing more invasive forms of self-help. The *New York Times* recently reported that companies were investigating systems that invade the computer of a suspected copyright infringer and delete files, slow network access, or even do more permanent damage.[15] Such practices are most likely illegal today, but amendments to our computer crime statutes have been proposed to allow some of them in the future.

CDT is concerned that invasive self-help measures create privacy and security risks for users. Innocent users might find their computers attacked by mistake, perhaps due to a confusingly named files. A person’s computer might stop working without them ever know why. Even infringers might not warrant the costly effects of damaging self-help measures.

More generally, the overall security of these networks and of the Internet itself would be harmed by the sanctioned development of attack tools that might be used for inappropriate purposes. Instead, we strongly believe that copyright infringement should be punished in accordance with current law, with due process afforded.

[15] Sorkin, Andrew Ross. "Software Bullet is Sought to Kill Music Piracy." *The New York Times*. May 4, 2003. Available at <http://www.nytimes.com/2003/05/04/business/04MUSI.html?ex=1053001791&ei=1&en=8d9f2b1d372d373>.

Legal risks

File traders who violate copyright laws risk lawsuits, civil penalties, and even criminal prosecution. These actions typically begin with efforts to identify individuals and can result in the disclosure of personal information. Peer to peer users should always be aware of the legal penalties for copyright infringement and should share legally, and responsibly.

At the same time, CDT is concerned that at least one provision of current law– the broad subpoena power granted any copyright holder under Section 512(h) of the Digital Millennium Copyright Act–too easily allows the identity of a peer-to-peer participant or any Internet user to be unmasked wrongly or by mistake, without their knowledge.

CDT strongly sympathizes with the need of copyright holders to identify potential infringers in order to enforce their legal rights online and curb the increasing piracy of digital content. At the same time, the unique subpoena provision in DMCA Section 512(h) and the interpretation of that provision in the recent Federal court rulings in *RIAA v. Verizon* raises important privacy concerns. In that case, Verizon, a prominent ISP, challenged the recording industry's attempt to gain identifying information about Verizon customers through a 512(h) subpoena. The court permitted the subpoena, and its broad interpretation of section 512(h) has raised serious concerns about the privacy of Internet users who are thought -- even mistakenly -- to be sharing copyrighted content.

Section 512(h) would permit any copyright holder – possibly millions of organizations and individuals – to compel an ISP to disclose the identity of an Internet user based on an allegation of copyright infringement. This disclosure of personally identifying information would take place without requiring any notice to the end user that his or her identity had been unmasked, and without extensive legal review or judicial oversight as to the likely truth of the allegations. An ISP could now be compelled to disclose the identity of any user of its networks – such as someone downloading a web page – who is alleged to be a copyright infringer, not just those who host materials at an ISP. Although we recognize the importance of fighting massive copyright infringement online, we are concerned that personal identifying data about users will be revealed without their knowledge due to misuse, abuse, or mistake, casting a chill on their privacy and security.

Recent events illustrate the extent to which mistakes can be made in seeking action against alleged infringers. This week the RIAA formally apologized for a letter sent to Penn State University threatening legal action over a music file created by PSU Professor Emeritus Peter Usher that was apparently confused with the copyrighted work of the recording artist Usher.[16] Had such a mistake been made in the context of a 512(h) subpoena, the end user

[16] McCullagh, Declan. "RIAA apologizes for threatening letter." *CNet News.com*, May 12, 2003. Available at <http://news.com.com/2100-1025_3-1001095.html>. Recent reports have shown that the Usher incident is just one of a number of mistaken notices sent by content companies. See McCullagh, Declan. "RIAA apologizes for erroneous letters." *CNet News.com*, May 13, 2003. Available at <http://news.com.com/2100-1025-1001319.html>. Also, in a submission before the court in *RIAA v. Verizon*, ISP UUNET assembled a list of notices it had received since January 2001. Among those notices were numerous files mistakenly associated with recording artist George Harrison, including pictures such as "Portrait of mrs harrison williams 1943.jpg"

could easily have had sensitive identity information released without his or her knowledge.

Effective copyright enforcement need not come at the expense of individual privacy. CDT believes that a better balance can and should be struck. For example, providing end users with notice when their identity is revealed would go a long way toward preventing abuse by giving those with the greatest interest in correcting mistakes an opportunity to contest release of their information. Courts could be required to exercise greater oversight. Sanctions could be put in place for misuse. Reporting requirements could be established to ensure that provisions were not being used in ways beyond what Congress intended. ISPs could be compensated for the efforts required to identify users, in part to provide a check against repeated and inappropriate use.

Many of these suggestions -- particularly a notice requirement -- could simultaneously protect user privacy while advancing intellectual property protection online. We believe that resolving this issue will ultimately be a policy question for Congress to decide if the courts continue to uphold a broad interpretation of the provision.

3. Suggested Approaches for Dealing with Peer-to-Peer Privacy and Security

Regulating peer-to-peer file-sharing technologies directly is likely to be difficult and undesirable. The systems we tend to think of as “peer-to-peer” share many characteristics with other Internet technologies like instant messaging, network file transfer protocols, and even email or web browsing. The rapid evolution of these systems—from central control towards decentralized systems with encrypted data, anonymous clients, rotating ports, and split files – will continue to make it hard to isolate peer-to-peer traffic. The technology itself is oftentimes beneficial and the source of innovation.

In many ways file sharing is inherently user-controlled. Users decide which directories to share and what files to download. For that reason the most critical privacy protections for peer-to-peer are best addressed through user education about how to protect themselves and how to choose applications that respect their privacy. In only a few key areas – where developers fail to obey fair information practices, or where the law already has created privacy risks – might legal changes be needed.

We believe several key steps should be taken to protect privacy and security without jeopardizing the benefits of this important new technology.

Inform Users About Privacy and Security Concerns in Peer-to-Peer File Sharing - Users need to better understand the basic operation and potential risks of peer-to-peer systems. Based on these and other concerns, CDT has developed a set of Tips for Safe Sharing attached at Appendix I. These and sets of tips like it are among the types of resources that should be shared widely with peer-to-peer users.

and with the movie *Harry Potter and the Sorcerer's Stone*, including a text file entitled "harry potter book report.rtf."

Raising public awareness is a critical first step. CDT, along with over forty-five other Internet industry companies and public interest groups, has helped create a family information portal called GetNetWise (see *http://www.getnetwise.org*). Established in 1999, GNW is a comprehensive collection of tools for families seeking to protect their children online. Its web site is linked to by over 80,000 other sites, including major Web companies like Yahoo!, MSN, and AOL, public interest organizations like CDT and the National Center for Missing and Exploited Children schools, individual Internet users, and the offices of numerous members of Congress. Now there is an effort underway to expand GetNetWise's offerings into other areas of Internet privacy and security. New resources are currently being developed describing how families can protect themselves when using peer-to-peer file sharing networks. (A copy of GetNetWise's peer-to-peer resource pages is attached as Appendix II.)

With such a broad base of support, GetNetWise's offerings can help catalyze discussion among the industry, public interest, and lawmakers about privacy and security throughout the Internet. CDT hopes that members of Congress will continue to view GetNetWise as a valuable tool to educate American Internet users about the risks that exist online, and how to protect oneself against them.

Expect fair information practices in file-sharing software - The developers of file-sharing software could do much more to make it easier to use, with greater transparency and better control over shared files. The Kazaa usability study, for example, notes how difficult it can be to determine what files are shared. Pop-up warnings about sharing drives, default settings that favor privacy, limits on tools that assist in sharing more files, and simpler user interfaces generally should be standard features for powerful file-sharing software.

More importantly, like others who might collect personal information peer-to-peer software producers should adopt fair information practices,[17] particularly regarding any use of adware or spyware. Better notice at a minimum should be provided – including privacy policies and machine-readable notices like P3P, the Platform for Privacy Preferences[18]. Meaningful choice about collection of information, access to information stored, and other fair information practices should be followed as well.

We recognize that a diverse and young marketplace, including small companies and open source developers, may not be equipped to deal with such practices. But unless such practices are adopted through industry standard setting groups that are open to consumer participation, users will feel the need for more regulatory approaches.

Add privacy protections for DMCA subpoenas – As noted above, the broad DMCA Section 512(h) subpoena provision allows the sensitive identity of Internet users to be unmasked by any copyright holder, without the knowledge of the user, and with little oversight. Privacy

[17] For example, the OECD Guidelines for the privacy of personal records are generally cited as a baseline of fair information practices. Available at <http://www.cdt.org/privacy/guide/basic/oecdguidelines.html>.

[18] More information about P3P is available at <http://www.w3.org/P3P/>.

and safety protections should be attached to this authority to prevent misuse, abuse, or mistake. In many areas of electronic surveillance and privacy Congress has struck a balance to support enforcement while protecting privacy. This example need not be different. Numerous due process tools are at our disposal – including notice to the end user when their privacy is being invaded, additional judicial scrutiny, reporting and audit requirements, cost reimbursement to ISPs (as a check on misuse), and other protections.

Such tools can and should be put to use in a way that simultaneously protects users and advances the cause of intellectual property protection. In particular, attaching a notice requirement to the 512(h) subpoena provision of DMCA would both help protect the anonymity of innocent users and serve as a warning to those who would engage in copyright infringement. Privacy need not come at the expense of enforcement.

Prevent invasive "self-help" tactics- Under no circumstances should it be made legal to damage another person's computer or files based on mere allegations of wrong-doing, including copyright infringement. Efforts to amend the computer crime, anti-hacking, or electronic privacy laws to allow for invasive self-help measures without adequate due process should be resisted.

Continue the broader push for Internet privacy protections – All of these efforts take place in the context of a broader debate about protecting privacy in a digital age where more personal information is in the hands of third parties, particularly online. The application of fair information practices remains a touchstone of privacy online, although not always a sufficient one. CDT continues to believe that a three-part package of technology protection measures (like encryption, anonymizers, or P3P), self-regulation (like the adoption of notice, choice and other practices by companies), and where needed, narrowly tailored and technology-neutral baseline privacy legislation.

4. Conclusion

History is replete with examples of technological change that sparked fear and social concern. The automobile, the telephone, email itself, were all greeted by skepticism and concern about the very real dislocations and social changes they caused. Some issues turned out to be serious; others hyperbolic; in each instance people adapted, policy responses were crafted as needed, and concerns were dealt with while preserving innovation and societal benefits.[19]

Peer-to-peer file sharing is likely facing such a moment of dislocation. The concerns it raises are very real. Preserving the potential benefits of the innovation and open, decentralized communication model that P2P is part of will be important as well.

Solving the problems of peer-to-peer privacy and security will ultimately require the cooperation of the Internet industry, lawmakers, and the public interest sector in order to be

[19] See, e.g., Standage, Tom. *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers*. New York: Berkley, 1998.

effective. By fostering dialogue and promoting public awareness, Congress can help guide this process as well as raise the public profile of these important issues. Additionally, continued dialogue will help illuminate the path forward and will help users and policymakers avoid the pitfalls of premature regulation. CDT looks forward to participating in the effort to promote safe, secure use of these valuable tools.

House Rule XI, Clause 2(g)(4) Disclosure: Neither Alan Davidson nor CDT has received any federal grant, contract, or subcontract in the current or preceding two fiscal years.

Appendix I: CDT's Tips for Safe File Sharing

To aid in the education effort, CDT has assembled its own list of tips to help users keep their file sharing safe.

1. **Know what files you're sharing.** Sharing files makes them accessible to millions of people. Be sure you know what you're sharing. Many applications automatically share files you've downloaded. Others make it too easy to share parts of your hard drive that might contain personal information. Monitor what files your computer is sharing, particularly if several people use your computer.
2. **Be careful with files you download.** Downloaded files can be a source of viruses or other damaging software. As with any files you download, be sure you sufficiently trust their source before using them. Make sure that your computer is protected with up-to-date anti-virus software.
3. **Use the security tools.** Many tools to protect privacy and security on peer-to-peer networks are already available, and more are being developed. These include network firewalls, spyware-removal tools, and newer, more secure file sharing clients.
4. **Share lawfully.** Unlawful sharing of copyrighted works can result in serious legal liability. Peer-to-peer users should know whether they are infringing copyrights in their activities and should keep their file sharing legal at all times.
5. **Look out for spyware.** Some file-sharing programs collect information about your computer use and may transmit it to third parties. Try to be aware of what information your software is collecting, and avoid programs that collect more information about you than you want. If you think you may have downloaded spyware and you want to remove it, consider using one of the Net's many anti-spyware tools. An informed marketplace, cautious about using tools that collect too much personal information without obeying fair information practices, is likely to be the most powerful force to counteract bad practices.
6. **Talk to your family.** Just as they have many important benefits, peer-to-peer file sharing networks also may carry real dangers. Families should be particularly aware of the risks facing children who use these networks.

For other tips for protecting privacy and security online, see CDT's privacy resource guide at <http://www.cdt.org/privacy>.

Appendix II: GetNetWise Resources on File Sharing

GetNetWise.org, a comprehensive online resource for families seeking to keep children safe online, has recently developed a resource to help answer questions about online file sharing. (See attached).

GetNetWise

You're One Click Away...

About... Security

GetNetWise About...

Tips Tools Take Action Press Glossary Questions Join Us

Home / Security / Tips / Sharing / File-sharing Risks

File-sharing Risks

GetNetWiseTV: Anne Collier on File-sharing Risks

Peer-to-peer or file-sharing programs allow you to share your files with others on the Internet -- and vice versa. File-sharing is a new and interesting technology that shows promise for future applications. However, just like you shouldn't open email attachments from people you don't trust, you should be wary about downloading files from them as well. You never know what you or your kids may find on the hard drives of random strangers on the Internet. [How file-sharing works]

The best tip for file-sharing is to stop and think before downloading files through these networks. Here are more tips to keep your and your kids' file-sharing safe, secure and legal. Some of the risks associated with using file-sharing programs include:

Kids' Access to Pornography

Many file-sharing programs allow children to access inappropriate audio and video clips -- most of a sexually explicit nature. Kids searching for popular music files may sometimes inadvertently pull up sexually explicit files that use the same keywords. For older children, parents should be concerned about their access to other people's video libraries that may contain inappropriate videos. If you're concerned about these things, make sure to check your computer for file-sharing programs. See a list of some file-sharing programs. Some parental-control tools on the market do not restrict access to file-sharing technologies. Check the GetNetWise Tools for Families database to search for tools that restrict access to file-sharing or peer-to-peer networks.

Copyright Law

Many of the files available on file-sharing networks, such as many movies, songs, and video games, are copyrighted by the owner. That means that the law protects the owner's right to copy and distribute their content. What does the copyright mean to you? It means that downloading copyrighted music, movies and software using these file-sharing programs without the copyright owner's permission could put you in serious legal trouble. Peer-to-peer users should be aware that they may not be anonymous while using these networks. Copyright holders have located peer-to-peer copyright infringers and have sued them. So, make sure that you or your family does not infringe copyright while using filesharing networks. Be smart, and keep your file-sharing legal.

Dewie Explains the Risks and Threats to Cyberspace

Learn more about...

Viruses

Firewalls

E-Mail Filters

Sharing

Teaching Kids about Security

Computer Security

Sharing files with people you don't trust is a matter of hygiene -- and you should keep your computer as clean as possible. Using file-sharing networks creates a risk that viruses or other malignant code could be spread to your computer over the network. Computer security experts are starting to see viruses and malignant code (spyware) spread through file-sharing services. Viruses may damage your computer or interfere with your files; spyware may track your online activities and send that information to third parties. Spyware has been spotted in many places on file-sharing networks -- including packaged with the file-sharing clients themselves.

Privacy

If mis-configured, some file-sharing programs may expose the entirety of your hard drive to all other users of the file-sharing software. If you keep sensitive information on your computer, like your tax return information and online bank account data, check to make sure that you are not inadvertently making this available to thousands of strangers on the Internet.

Privacy Policy Contact GetNetWise.org Tell-a-Friend Get the GNW Newsletter

GetNetWise

You're One Click Away...

About... Security

GetNetWise About...

Tips Tools Take Action Press Glossary Questions Join Us

Home / Security / Tips / Sharing / Files / Tips

File-sharing Tips

The best tip for file-sharing is to stop and think before downloading files through these networks. It's best to keep your and your kids' file-sharing safe, secure and legal. Here are more tips:

- **Don't download files from people you don't trust** -- Just like you shouldn't open e-mail attachments from people you don't trust, you should be wary about downloading files from them as well.
- **Keep your file-sharing legal** -- Downloading copyrighted music, movies and software using these file-sharing programs without the copyright owner's permission could put you in serious legal trouble. Peer-to-peer users should be aware that they may not be anonymous while using these networks. Copyright holders have located peer-to-peer copyright infringers and have sued them. There are a growing number of online music and movie services where you can stream, download or purchase digital files with the copyright owners' permission. Using these services is one way to ensure that you will avoid unwanted lawsuits.
- **Watch out for "spy-ware"** -- Some file-sharing programs embed "spy-ware" programs when you install them on your computer. These programs can run in the background and create unwanted pop-up advertisements and some even monitor your online behavior.
- **Use and update your anti-virus software** -- Computer experts are starting to see viruses being spread through file-sharing networks. Be careful what you download and always make sure your anti-virus software is running and frequently updated.
- **Secure your sensitive computer information** -- If you keep sensitive information on your computer like your tax return information and online bank account data, check to make sure that you are not inadvertently making this available to thousands of strangers on the Internet.
- **Parents, talk to your kids** -- Parents should beware that file-sharing networks contain inappropriate audio and video clips -- many of a sexually explicit nature.

Dewie Explains the Risks and Threats to Cyberspace

Learn more about...

Viruses

Firewalls

E-Mail Filters

Sharing

Teaching Kids about Security

Privacy Policy Contact GetNetWise.org Tell-a-Friend Get the GNW Newsletter