Filesharing Programs
and
"Technological Features to Induce Users to Share"

A Report to the United States Patent and Trademark Office

from the Office of International Relations

Prepared by

Thomas D. Sydnor II

John Knight

Lee A. Hollaar

v 1.1
November, 2006

Foreword

by Jon W. Dudas,
Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office (USPTO)

This report originated when one of its authors showed me data on the behavior of filesharing programs that was being compiled for use in a law review article. Because the data seemed to have potentially important implications, I asked the authors to present it in the form of a report to USPTO. Having reviewed the resulting report, I conclude that this data should be made known to the public.

This report analyzes five popular filesharing programs to determine whether they have contained, or do contain, "features" that can cause users of these programs to share files inadvertently. It concludes that these programs have deployed at least five such "features," and that distributors of these programs continued to deploy such features after their propensity to cause users to share files inadvertently was, or should have been, known. It concludes that further investigation would be warranted to determine whether any distributors who deployed these features intended for them to trick users into sharing files unintentionally.

I requested this report because I believe that it raises important questions about why individual users of these filesharing programs continue to infringe copyrights. This report also reveals that these filesharing programs threaten more than just the copyrights that have made the United States the world's leading creator and exporter of expression and innovation: They also pose a real and documented threat to the security of personal, corporate, and governmental data.

For the Federal Government, this threat became manifest during 2005, when the Department of Homeland Security warned all Federal Agencies that government employees or contractors who had installed filesharing programs on their home or work computers had repeatedly compromised national and military security by "sharing" files containing sensitive or classified data. These users probably did intend to use these programs to download popular music, movies, software or games. But it seems highly unlikely that any of them intended to compromise national or military security for the sake of "free music."

A decade ago, the idea that copyright infringement could become a threat to national security would have seemed implausible. Now, it is a sad reality. It is important to ask how and why this happened. This report attempts to provide some answers and to encourage further research into questions that it can raise, but not answer.

The unanswered questions raised by this report implicate diverse competencies: Some might be best addressed by consumer-protection advocates or agencies, others by computer-science researchers. By releasing this report, I hope that USPTO will

encourage others to bring their expertise to bear on some of the questions that this report leaves open. Examples of such questions might include the following:

- What is the overall prevalence of inadvertent sharing? It may be possible to estimate the number of users who have recursively shared "C:\" or their "My Documents" folder, but estimating the number of users inadvertently sharing downloaded files or their "My Music" folder might be much more difficult.

- How can users of filesharing programs who do not want to upload files *effectively* avoid the sort of coerced-sharing features discussed in this report?

- What are the best options for owners of home computers who want to avoid the security and liability risks associated with filesharing programs?

Finally, I reviewed this report as both a father who manages a home computer and the director of a Federal Agency that must protect the security of valuable electronic files and data. It leads me to believe that I owe a debt of thanks not only to my colleagues at the Department of Homeland Security, but also to two groups of persons.

First, I would like to thank all of the computer-science researchers who have studied filesharing networks. They have done what scientists are supposed to do: Observed carefully and reported what they found—both the good and the bad. Their reports bring to the debate about filesharing objectivity and dispassion that has otherwise been lacking.

I would also like to thank the researchers, reporters, agencies, private citizens, and information-security firms who worked for years to call attention to the persistent and recurring problem of inadvertent sharing. Special thanks are owned the unnamed Samaritan interviewed by CBS News, to the creator of the website *See What You Share,* and to Dr. Howard Schmidt and the employees of Tiversa, Inc.

Table of Contents

I. **Executive Summary.**

For years, computer-science researchers, Federal Agencies, concerned private citizens, IT-security companies, public-interest groups, news reporters, and others have also reported that users of popular filesharing programs have been sharing files unintentionally. More recently, in *MGM Studios, Inc. v. Grokster, Ltd.*, the Supreme Court found "unmistakable" and "unequivocal" evidence that distributors of two popular filesharing programs intended to induce users of their programs to infringe copyrights. The findings in *Grokster* suggest that persistent reports of inadvertent sharing could signal the effects of duping schemes, a known means of inducement.

In a duping scheme, an entity that intends to use others as a means to achieve an illegal end tricks other people into inadvertently or unintentionally performing a potentially illegal act. In the context of filesharing, duping schemes could be particularly effective. Duping that caused infringing files to be shared inadvertently by young, new or unsophisticated users could still make millions of files available for downloading. Indeed, new users of filesharing programs tend to download many more files than established users, so duping that targeted new users could add a disproportionately large number of files to the network. Duping schemes that targeted young or unsophisticated users would also ensure that attempts to enforce copyrights against those infringers who upload hundreds or thousands of infringing files would tend to target young or sympathetic users.

This report reviews public data about the behavior of five popular filesharing programs; it focuses on the programs BearShare, eDonkey, KaZaA, LimeWire, and Morpheus. It seeks to answer two questions. *First*, have distributors of these filesharing programs deployed features that had a known or obvious propensity to trick users into uploading infringing files inadvertently? *Second*, if so, do the circumstances surrounding the deployment of such features suggest the need for further investigation to determine whether any particular distributor *intended* for such features to act as duping schemes—as "technological features to induce users to share."

This report concludes that the distributors of these five filesharing programs have repeatedly deployed features that had a known propensity to trick users into uploading infringing files inadvertently. Distributors deployed at least five such features:

- **Redistribution features**: All five programs analyzed have deployed a feature that will, by default, cause users of the program to upload (or "share") all files that they download. These features create a counter-intuitive link between downloading files for personal use and distributing files to strangers, and they have often been implemented in ways that could make their effects less obvious to new users. Since 2003, lawsuits against users of filesharing programs have made it more important for users to understand the effects of redistribution features. During this period, some programs tended to disclose less information about their redistribution features.

- **Share-folder and Search-Wizard Features**: All five programs analyzed have deployed share-folder or search-wizard features. These features are uniquely dangerous: They can cause users to share inadvertently not only infringing files, but also sensitive personal files like tax returns, financial records, and documents containing private or even classified data. Published research identified these features as causes of inadvertent sharing by mid-2002. By mid-2003, the distributors of the programs analyzed here had agreed to discontinue use of these features, and concerned legislators had warned that their continued use would compromise national security because government employees using these programs would inadvertently share files containing sensitive or classified data.

  Nevertheless, the distributors of BearShare, eDonkey, LimeWire and Morpheus programs kept deploying search-wizard or share-folder features, and the distributors of KaZaA eliminated these features in a way that would tend to perpetuate inadvertent sharing previously caused by such features. By late spring of 2005, the Department of Homeland Security reported that government employees using filesharing programs had repeatedly compromised national and military security by "sharing" files containing sensitive or classified data.

  - **Share-folder features**: All five of the programs analyzed have deployed a feature that lets users store downloaded files in a folder other than the specially created folder that stores downloaded files by default—but does so through an interface that does not warn users that all files stored in the selected folder will be shared. In most cases, the sharing caused by this feature will be recursive: The program will share not only the files stored in the folder selected to store downloaded files, but also all files stored in any of its subfolders.

  - **Search-wizard features**: At least three of the programs analyzed have deployed a feature that will search users' hard drives and "recommend" that users share folders that contain certain "triggering" file types, which usually include document files, audio files, audiovisual files, and image files. Some search-wizard features activate automatically; others require the user to trigger them. Some are activated during a program's installation-and-setup process; others are an option that a user can activate after the program is installed and running. Some will select identified folders for sharing; others "recommend," but do not select, identified folders for sharing. All search-wizard features discussed will cause recursive sharing of identified or selected folders.

- **Partial-uninstall features**: At least four of the programs analyzed have deployed partial-uninstall features: If users uninstall one of these programs from their computers, the process will leave behind a file that will cause any subsequent installation of any version of the same program to share all folders shared by the "uninstalled" copy of the program. Whenever a computer is used by more than one person, this feature ensures that users cannot know which files and folders these programs will share by default.

- **Coerced-sharing features**: Four of the programs analyzed have deployed features that make it far more difficult for users to disable sharing of the folder used to store downloaded files. This folder may be the default download folder created by the filesharing program or an existing folder selected to store downloaded files through a share-folder feature. In each case, the feature can provide misleading feedback indicating—incorrectly—that the user has disabled sharing of the download folder. But in each case, an obscure mechanism appears to allow sophisticated users to avoid the coerced-sharing feature and stop sharing the download folder.

All five of these features can cause users to share infringing files inadvertently. Redistribution and coerced-sharing features can cause users to share *downloaded* files inadvertently: As *Grokster* noted, these files are usually infringing. Share-folder, search-wizard, and partial-uninstall features can cause users to inadvertently share *existing* files on their computers: The design of these features ensures that the files shared may tend to include users' collections of media files, like audio files copied from purchased CDs.

All five programs analyzed in this report have deployed most or all of these features during at least some portion of the period from 2003 to 2006. In many cases, versions of these features actually became more aggressive after their propensity to cause inadvertent sharing was, or should have been, known to reasonable distributors of filesharing programs. For example, the distributors of BearShare, eDonkey, LimeWire and Morpheus began or continued to deploy poorly disclosed redistribution features, share-folder features, search-wizard features and/or coerced-sharing features even after these distributors drafted a *Code of Conduct* that should have precluded use of any such features. Some distributors even responded to reports of inadvertent sharing by releasing new versions of their programs that seemed improved, but actually *perpetuated* inadvertent sharing caused by features previously deployed. Consequently, this report concludes that the totality of the circumstances surrounding the deployment of such features justify further investigation to determine whether particular distributors *intended* for such features to act as duping schemes.

This report does not, however, draw conclusions about the intent of any particular distributor that deployed some or all of these features in its filesharing program. This report analyzes public data, and it is possible that nonpublic data now controlled by a particular distributor might show that it deployed these features mistakenly, negligently, or recklessly. This limitation on the scope of this report's conclusions is a precautionary measure: It does not imply that a court obligated to draw conclusions about the intent of a particular distributor could not find that the data discussed herein provides "unmistakable" or "unequivocal" evidence of intent to induce copyright infringement within the meaning of *MGM Studios, Inc. v. Grokster*, 125 S. Ct. 2764 (2005).

II. **Background.**

A combination of two factors suggested the need for the analysis conducted in this report. *First*, on June 27, 2005, in *MGM Studios, Inc. v. Grokster, Ltd.*, the Supreme Court of the United States found "unequivocal" and "unmistakable" evidence that the distributors of the Grokster and Morpheus filesharing programs intended to induce users of their programs to infringe copyrights. Duping schemes are a known means to induce others to perform illegal acts.

Second, in the context of filesharing, duping schemes would, by definition, cause users of filesharing programs to share infringing files unintentionally. For years, researchers, governments, the media, and users themselves have been reporting that users of some filesharing programs end up "sharing" files unintentionally.

Together, these two factors suggest a need to investigate to determine whether distributors of filesharing programs may have used duping schemes to induce users of their programs to upload, or "share" infringing files unintentionally.

A. Policy and practical considerations show the need to consider whether distributors may have designed filesharing programs to dupe new or vulnerable users into "sharing" infringing files.

The inducement doctrine reaffirmed by the *Grokster* Court has long been a basis for imposing secondary civil liability for many forms of wrongful conduct, including copyright, patent, and trademark infringement. As a result, inducement cases and laws provide courts, rightsholders and technologists with "diagnostic tools" that can identify conduct that may indicate intent to induce others to break the law.

For example, in cases involving alleged infringements of intellectual-property rights, courts have called inducement the civil analog of the criminal-law doctrine of aiding and abetting. By analogy, the two-part structure of the criminal aiding-and-abetting statute, (Section 2 of the United States Criminal Code), suggests that there are two means for a culpable entity to induce others to commit illegal acts:

- **Section 2(a) Inducement (Persuasion):** An entity might seek to persuade or encourage third parties to break the law *intentionally*. In the context of filesharing, a distributor engaged in 2(a)-type inducement might say something like this: "Separating the download of the data and the keys may help protect file sharers from lawsuits, making it more difficult for courts to say exactly which party is responsible for copyright infringement…."[1]

- **Section 2(b) Inducement (Duping Schemes):** An entity might also seek to dupe or trick third parties into breaking the law *unintentionally or unwittingly.* Justice Story's classic example of duping involves a murderer who has food poisoned and delivered by a child who does not intend to harm the intended victim.[2] In the context of filesharing, "duping schemes" might be executed by features in

filesharing programs that trick some users into sharing files that they did not intend to make available to others.

The difference between inducement-by-persuasion and duping turns on whether the person induced to perform a potentially illegal act *intended* to break the law—not on the use of deceit. For example, inducement-by-persuasion might well involve deceit: An inducer might misrepresent the odds of getting caught in order to persuade another person to perform an illegal act intentionally. The *Grokster* decision focused on evidence suggesting that distributors of filesharing programs encouraged users of their programs to infringe copyrights intentionally. The Court did not consider the possibility of duping.

After *Grokster*, it becomes important to consider the possibility of duping. In any context, duping schemes can be particularly destructive to the rule of law:

- Duping schemes can conceal their authors: Violations of the law occur, but they seem to result from the mistakes or negligence of third parties.

- Duping schemes can also endanger unwitting participants: Persons duped may risk civil liability or even criminal prosecution.

- Duping schemes can also shield the culpable: A duping scheme also encourages culpable parties to break the law intentionally; if culpable lawbreakers are caught, they can avoid or minimize the consequences of their acts by posing as dupes.

While duping schemes might seem appealing, they have remained rare in practice. Ordinarily, it would be unlikely that distributors of a product would have incentives to dupe its users into breaking the law. And even if distributors had such incentives, two factors would usually deter a resort to duping.

First, consumers usually have very powerful remedies against the distributors of any product that causes any sort of foreseeable harm. The vast information markets that surround almost all popular consumer products would also be likely to detect and reveal any wrongdoing—and thus ensure that the remedies available to consumers would be brought to bear.

Second, duping schemes could reveal themselves if they affect too many users of a product: If most people who use a product end up breaking the law unintentionally, it will become obvious that the product—and its designers—have contributed to this result. Duping would thus have to be calibrated to cause only a relatively small subset of users to break the law. Consequently, duping should occur only if some disproportionate benefit could be gained by tricking only a relatively small percentage of users into breaking the law.

Filesharing presents an unusual context in which these practical obstacles to duping diminish. In practice, popular filesharing programs are used mostly to download and upload infringing copies of copyrighted music, movies, games, images, and software. For example, in *Grokster*, unrebutted evidence indicated that 90% of the files available

on filesharing networks consisted of infringing files. Upon remand, the district court in *Grokster* found that undisputed evidence showed that "[a]lmost 97% of the files actually requested for downloading were infringing or highly likely to be infringing."[3]

When almost all users of a product use it to break the law almost all of the time, the protections against duping provided by consumer-protection and tort laws recede. As a practical matter, persons who use a filesharing program to download infringing files cannot call their state attorney general or the Federal Trade Commission and report the following complaint: "I installed this program so I could download popular music without paying for it, but the program caused me to share the infringing files that I downloaded, and that got me sued." The user who did this might well be confessing to a federal crime. Nor would this user be a sympathetic tort plaintiff.

This situation also seems to deter information markets: For example, because virtually everyone who uses a popular filesharing program appears to use it almost exclusively to download infringing files, a mazagine or website seeking to do a meaningful review of filesharing programs would have to assess their relative efficacy as a means of copyright piracy. Perhaps for this reason, filesharing programs have become one of the most widely used, let least discussed and reviewed, computer programs on the market.

Filesharing also presents the unusual case in disproportionate benefits could be gained by tricking only new, unsophisticated or young users of filesharing programs into sharing infringing files:

- Filesharing programs are very widely used. Duping could thus cause many millions of files to be uploaded even if it affected only a small fraction of users.

- New users of filesharing programs download many more files than existing users.[4] Duping that affected only new and unsophisticated users would thus be disproportionately effective at adding files to a network.

- Many users of filesharing programs are young teenagers or preteen children.[5] Children are the classic targets of duping.

Taken together, these three factors suggest that schemes to dupe young, new, or unsophisticated users of filesharing programs into sharing infringing files unintentionally could help populate networks with infringing files even if they affected only a small percentage of users.

An additional factor could then allow duping schemes to have a uniquely malign effect: Were a distributor to design its filesharing program to dupe otherwise-sympathetic users into "sharing" many infringing files unintentionally, the distributor responsible would not be the one to punish these users for their credulity. As a result, duping schemes might tend to vilify—not their authors—but copyright holders and copyright laws. Copyright holders trying to deter infringement might sue the most egregious infringing users of filesharing programs—those few who upload hundreds or thousands of infringing files.

Duping schemes could ensure that such lawsuits would actually tend to target a program's youngest and most sympathetic users.

Such a situation would raise important policy concerns. Historically, copyrights have generally been enforced against *distributors* or *commercial users* of protected works, but not against ordinary consumers. This long practice ensured that copyrighted works could be enjoyed by everyone—from toddlers to seniors—without the need for any detailed knowledge of copyright law.[6]

Filesharing became the exception to this practice because many programs were designed to ensure that infringing use of filesharing networks could not be halted by sending takedown notices to the distributors of the programs that create them, or even by suing those distributors into bankruptcy. After the *Napster* litigation, distributors were told that such designs could help *them* avoid liability: "The key here is to let go of any control you may have over your users—no remote kill switch, contractual termination rights or similar mechanisms."[7] Thus, even if rightsholders successfully sue the distributors of these programs, they still confront a lose-lose-lose decision: They must either (1) try to deter infringement by suing the consumers who use these programs, (2) try to deter infringement by paying off the architects of filesharing piracy, or (3) accept ongoing, pervasive infringement that could eventually waive their rights to prevent unauthorized reproduction or distribution of their works.

In *Grokster*, the Supreme Court noted, "[T]he ease of copying songs or movies using software like Grokster's and Napster's is fostering disdain for copyright protection." Network architecture that forces copyright holders to waive their rights, payoff pirates, or sue consumers may inevitably foster further disdain for copyright protection—for the system of private property rights in expressive works that the Framers of the Constitution thought indispensable to the growth of private expression in a democratic republic.

Indeed, after some copyright holders sued users uploading many hundreds or thousands of infringing files, defenders of filesharing objected that such users tend to be poor, unsophisticated, or children. For example, in its 2005 report, *RIAA v. The People*, the Electronic Frontier Foundation (EFF) described the users uploading many hundreds of infringing files as follows: "The[y] were not commercial copyright pirates. They were children, grandparents, [and] single mothers…." EFF then cited numerous individual cases involving users who were (1) unaware that sharing infringing files was illegal, (2) unaware that they were uploading infringing files that they had downloaded, (3) poor, (4) unsophisticated, (5) children or young teenagers, or (6) some or all of the above.[8]

The cases cited by EFF involve defendants who seem sympathetic *because* circumstances strongly suggest that they never intended to turn their home computers into online distribution centers for pirated goods. Another EFF lawyer condemned enforcement against such users as a "reign of terror" against "defenseless people" who probably did not intend to break the law—"any real pirate would never leave the meta-data and would be using someone else's Internet access."[9] But such condemnations just beg a more fundamental question: *Why* do children, grandparents, and poor single mothers end up sharing hundreds or thousands of infringing files inadvertently?

Distributors of filesharing programs have also argued that the prevalence of children among high-volume uploaders of infringing files makes it wrong for copyright holders to enforce their rights. For example, one high-volume uploader of over 800 infringing audio files turned out to be a 12-year-old female honor student receiving public assistance. The distributors of the BearShare, Morpheus, and eDonkey programs responded to this tragic situation in the press release *Peer-to-Peer Trade Group to RIAA Bullies: Come Out and Fight Us If You Want, But Leave the Little Guys Alone*:

> [I]t's time for the RIAA's winged monkeys to fly back to the castle and leave the Munchkins alone.…
>
> They're playing the Wicked Witch of the West, using $150,000-per-song lawsuits to frighten the little people.…
>
> Like the Cowardly Lion, the record industry bullies should come out and fight us if they want, but leave the little guys alone.[10]

Such rhetoric heightens the need to investigate. Distributors of filesharing programs created an unprecedented, avoidable, and tragic conflict between artists and their fans. These distributors then denounced the enforcement lawsuits against users that their own choices had made nearly inevitable. But declarations of sympathy for the fate of the "little guys" would ring very hollow if authored by distributors deploying "features" that could tend to cause "the Munchkins" to become high-volume uploaders of infringing files.

These policy considerations show why it is important to consider the possibility of duping. They are also reinforced by practical considerations. By definition, duping schemes would cause users of filesharing programs to "share" (or "upload") infringing files *unintentionally*. For years, an expanding set of public reports has asserted that users of filesharing software do "share" files unintentionally.

Since at least 2002, such reports have come from computer-science researchers, congressional hearings, agencies, consumer groups, scholars, security companies, news media, and users of filesharing programs. These reports have arisen from sources on both sides of the filesharing debate and sources largely unconcerned with that debate. While these reports do not—and cannot—describe the full scope of the problem, they show that unintentional sharing of files has recurred regularly. In the aftermath of *Grokster*, the potential implications of such reports become clear enough to warrant investigation.

B. This report investigates whether popular filesharing programs contain features that their distributors knew or should have known could cause users to upload files inadvertently.

Appendix A provides more detail about the factors that shaped the scope of this report, and it defines some of the terms used. Consequently, this section will simply outline the

scope of the issues that this report addresses. This report reviews only publicly available data, and it seeks to answer two questions.

First: Do popular search-and-download filesharing programs contain—or have they contained—features that can cause users to share files unintentionally? This report will focus on five such programs: KaZaA, LimeWire, BearShare, eDonkey, and Morpheus.[11] It will examine how the sharing-related features of these programs operate, and how their operation did or did not change from 2002 through 2006.

Second: Do the circumstances surrounding the use of any such features suggest a need to further investigate whether any particular distributor that deployed such a feature *intended* for it to dupe users into sharing files inadvertently? This report does not purport to determine whether any particular distributor intended to dupe users by deploying a feature with a known or obvious propensity to cause inexperienced users to share files inadvertently. To be sure, intent might be inferred from unrebutted public data showing that a particular distributor deployed a feature that had a known propensity to cause users to share files inadvertently. But even in such a case, a distributor might possess nonpublic data that would tend to show that the feature at issue was actually deployed innocently, negligently, or recklessly.

It is important to note that a report that seeks to answer the two questions described above will not answer many other important questions. Filesharing programs raise an array of public-policy and public-safety concerns, and only a few of them will be addressed in detail in this report.

This report focuses on features that could mislead users into *sharing files* inadvertently: It does not discuss features that might dupe users into performing other actions. For example, by default, most filesharing programs make a user's computer eligible to serve as a "supernode" or "ultrapeer." It seems highly unlikely that most users realize that this means that they have "agreed" to house—on their computers—search-index servers much like those that subjected Napster, Inc. to billion-dollar secondary liability or those that subjected operators of Direct Connect "hubs" to criminal prosecution and conviction.[12] Nevertheless, housing a search-index server does not cause users to share their own files inadvertently, so the issue will not be discussed further here.

This report also focuses on features that could indicate intent to dupe users into sharing files *inadvertently or unintentionally*: It does not discuss features in popular filesharing programs that encourage users to sharing infringing files *intentionally*. Many potential examples of such features exist:

- Versions of the KaZaA filesharing program contained a "Participation Level" feature that creates strong incentives for users to share files that other users want to download. As *Grokster* notes, such files strongly tend to be infringing.

- Professor Strahilevitz argues that filesharing programs encourage new or unsophisticated users to share files through "charismatic code" that "presents each member of a community with a distorted picture of his fellow community

> members by magnifying cooperative behavior and masking uncooperative behavior." Deceit gives this code its "charisma": "While there is nothing terribly persuasive about telling a lie per se, the genius of Gnutella is the way in which it makes that lie look like a reality to its users."[13]

Under *Grokster,* such features might be relevant to an analysis of inducement-by-persuasion. Nevertheless, features that encourage users to *intentionally* share infringing files do not suggest duping, so they are not a focus of this report.

Finally, this report does not assess *all* security risks associated with filesharing programs. At least two types of security risks fall outside of its scope. First, filesharing programs themselves may contain bugs or flaws that hackers can exploit to compromise computers or networks. Second, filesharing programs can download mislabeled files that contain malicious code that can compromise computers and networks. These vulnerabilities are significant, but neither is a focus of this report.

III. **An Analysis of Potential "Technological Features To Induce Users to Share" in Five Popular Filesharing Programs.**

A potential link between filesharing programs and duping schemes first appears in the 2000 study *Free Riding on Gnutella,* one of the most widely cited scientific studies of post-*Napster* filesharing networks.[14] In 2000, early filesharing programs based upon the Gnutella protocol had similar uploading and downloading capabilities: A user had to make a conscious decision and act affirmatively in order to download or upload any particular file.[15]

Researchers from Xerox PARC Labs studied the resulting network in August of 2000 and concluded that Gnutella-based networks would not be robust, efficient or scalable because so few users chose to share files: 66% shared no files at all, so 1% of all users provided 47% of all responses to queries for files. The Gnutella network, though entirely decentralized in its architecture, thus remained highly centralized in fact.

Free Riding on Gnutella and subsequent research also noted that these low levels of sharing were no accident: Design characteristics like anonymity, indiscriminate sharing, large user-bases, dynamic membership, cheap pseudonyms, and lack of central administration made filesharing networks suitable for infringing use, but these features also discouraged users from sharing files.[16] Indeed, they ensured that few users would possess *any* files that they could safely and legally distribute over filesharing networks.

For example, many parents will *want* to share digital photos of their children with family and friends. But "sharing" such photos over a filesharing network would be ineffective and dangerous. LimeWire has explained why it could be ineffective: "Here's modern p2p's dirty little secret: It's actually horrible at [locating] rare stuff."[17] It would be dangerous because the anonymity, cheap pseudonyms, and indiscriminate sharing that make these networks an attractive venue for infringement also attracted "unstoppable" pedophiles who share violent child pornography, and, reportedly, inadvertently shared

data about particular children.[18] In short, if users of filesharing programs were not sharing files, the distributors of these programs had their own design decisions to blame.

From their analysis, the authors of *Free Riding* drew the following conclusions:

- The Gnutella network faced "possible collapse" if developers of Gnutella-based programs continued to rely on "voluntary cooperation between users."

- Developers of Gnutella-based programs could rely, instead, on "technological features to induce users to share." [19]

The study noted at least two such "features." One was the redistribution feature used by Napster, Inc. that would cause users to upload files downloaded from the network. Another was the forced-sharing feature used by FreeNet that compels each user to store and share files.

The phrase "technological features to induce users to share" is inherently interesting in a post-*Grokster* world. In itself, it might not suggest duping: Distributors could "induce" users to share noninfringing files or to share infringing files intentionally. But this phrase does suggest duping when reliance upon "technological features to induce users to share" is presented as an alternative to reliance upon "voluntary cooperation between users." Consider, for example, the most widely deployed "technological feature" cited by *Free Riding on Gnutella*: A redistribution feature that will, by default, cause users to upload (or "share") all files that they download.

A. Redistribution features can cause users to share infringing downloads unintentionally.

After *Free Riding on Gnutella* was published, the redistribution features it recommended became nearly ubiquitous in filesharing programs. Some distributors reportedly implemented such features in response to its findings.[20] By 2002, the Gnutella protocol required compliant filesharing programs to contain a redistribution feature.

Research suggests dramatic results: By mid-2001, another study of the Gnutella network revealed that only 25% of studied users shared no files.[21] A smaller 2001 study of users of versions of the KaZaA and Morpheus filesharing programs that contained redistribution features showed that only 32% of those users shared no files: "At least part of this increased sharing, relative to Gnutella, surely stemmed from the defaults built into these systems."[22]

Today, almost all popular filesharing programs contain a redistribution feature. Most programs implement this feature by storing downloaded files in a folder that is shared by default. As *Free Riding on Gnutella* predicted, distributors of filesharing programs assert that these redistribution features are essential. In a 2004 letter to six Senators, the distributors of KaZaA asserted that disabling KaZaA's redistribution feature would

"cripple" the KaZaA network. In an internal email, Altnet asserted that "p2p exists because of this feature."[23]

Obscure or poorly disclosed redistribution features that tend to cause new or unsophisticated users to share downloaded files inadvertently could assist filesharing networks in two ways. First, they could help networks scale by ensuring that popular downloads are widely shared. Second, they would ensure that more users would share files with the same hash value: This would facilitate "swarming" downloads in which users download pieces of the same file simultaneously from multiple sources.[24]

Commentators have repeatedly concluded that redistribution features cause users to "share" downloaded files unintentionally. For example, in 2003, Professor Strahilevitz concluded that these features cause "unsophisticated or ambivalent users to make their files available for others to download."[25]

Similarly, in 2004, a neutral *amicus* brief to a Federal court from five professors of intellectual-property law from Harvard Law School's Berkman Center for the Internet and Society concluded that "only the most sophisticated" high-volume uploaders of infringing files intend to share *any* files: "Many users may not be aware that redistribution is automatically enabled by default." These scholars warned that distributors create "technological barriers" to ensure that "disabling file-sharing … can be [a] very difficult, and perhaps impossible, task for all but the most expert computer users."[26]

Professor Sag drew similar conclusions: "[P]eer-to-peer networks are programmed to create strong incentives to upload…. In part, this is achieved by burying the pro-sharing default so that it takes some user sophistication to figure out how to turn it off."[27]

These conclusions accord with reports from users of filesharing programs. Beginning in mid 2003, some copyright holders began suing users of filesharing programs alleged to be uploading many hundreds of infringing files. Sued users soon reported that they did not know that they were "sharing" the files that they had downloaded. The pro-filesharing website *p2pnet.net* characterizes their complaints as follows:

> It seems most of the RIAA's victims, including young children, used KaZaA.… They also say Sharman failed to make it clear that the folder in which KaZaA downloads were stored needed to be disabled so other people couldn't tap into it. But even if they had known, figuring out how to disable the folder was beyond them, say victims, especially children.[28]

While several of these sources explain why users might have difficulty disabling redistribution features, none explains why users might overlook redistribution features. But *Free Riding on Gnutella* shows that most users of filesharing programs do not want to share files; they only want to download files shared by others. For two reasons, users who only want to download can overlook a program's redistribution feature.

First, users who only intend to download files have no incentive to explore the sharing-related interfaces of their filesharing programs. Filesharing programs typically disclose their redistribution features in these sharing-related interfaces.

Second, redistribution features link the acts of downloading and uploading in a way that can be profoundly counterintuitive to consumers generally or even to experienced computer users. Ordinarily, the act of acquiring a book, CD, or DVD for personal use does not cause a consumer to distribute that work to others. One user who lost her life savings in a lawsuit stressed this point:

> I never willingly shared files with other users.… [T]he music I downloaded was for home, personal use. … As far as I was concerned copyright infringement was what the people in Chinatown hawking bootlegged and fake CDs on the streetcorner were doing. …[29]

This user understood that distributing unauthorized copies of protected works constitutes infringement, but she did not understand that the redistribution feature in her filesharing program ensured that she was doing just that.

Redistribution features could even confuse experienced computer users: Most programs do not cause their users to automatically redistribute saved or downloaded files. For example, using an Internet browser to visit websites or download files does not cause the user to begin acting as a server for each visited website or to begin making each downloaded file available to strangers.

By late 2003, distributors of filesharing programs knew or had reason to know that disclosing redistribution features only in sharing-related interfaces could cause users to share downloaded files inadvertently. Many distributors pledged to improve their disclosures. For example, by October of 2003, the distributors of eDonkey, BearShare, LimeWire, and Morpheus had drafted and published a *Code of Conduct* that required their programs to "conspicuously require the user to confirm the folder(s) containing the file material that the user wishes to make available to other users before making such material available.…"[30]

This conspicuous-confirmation requirement permits redistribution features—if they "conspicuously require the user to confirm" that he or she wishes to share downloaded files. Although the distributors of BearShare, eDonkey, LimeWire, and Morpheus all pledged to comply with this *Code* and repeatedly represented that they had done so, studied versions of their programs did not "conspicuously" require users to confirm that they wished to share downloaded files.[31] Indeed, disclosure of redistribution features often *decreased* after the *Code* was drafted.

Three basic patterns of disclosure emerge. The first is nondisclosure: A program might provide new or download-only users with no information that would suggest that a redistribution feature exists. For example, studied versions of eDonkey, like version 1.4.3, provide no information about sharing on their main interface—by default or otherwise—nor do they disclose their redistribution feature during their installation-and-

setup processes.[32] eDonkey 1.4.3 did not "conspicuously require the user to confirm" that she wished to share downloaded files by default.

But nondisclosure is better than a potentially misleading disclosure: A program containing a redistribution feature could suggest that redistribution was disabled by default. Here, for example, is an interface that appears during the installation-and-setup process in a 2003 version of Morpheus:

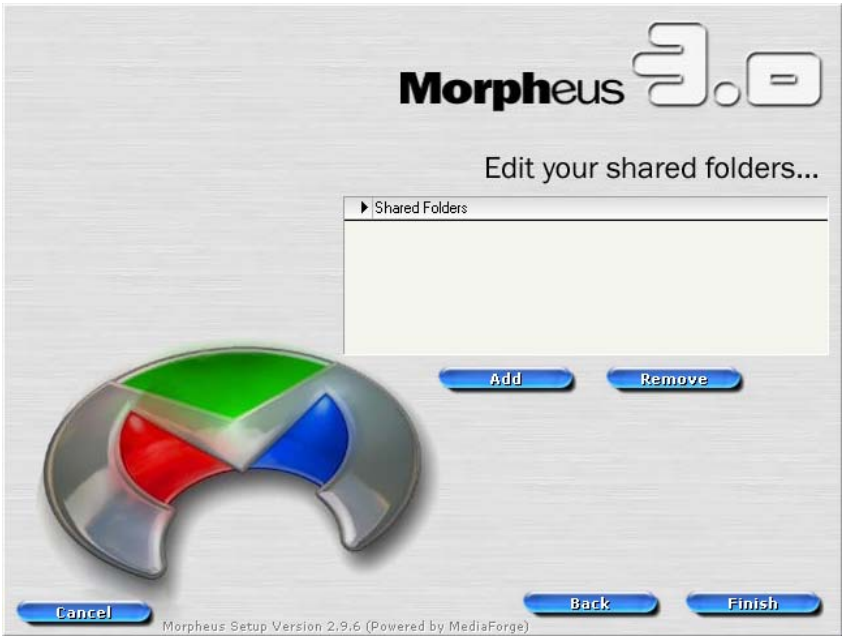

Figure 1: Morpheus 3.0.36

This version of Morpheus appears to lack a redistribution feature. Big black text tells the user, "Edit your shared folders", and the list below is empty by default. But appearances can deceive: This version of Morpheus has a redistribution feature—downloaded files are stored in a specially created "Downloads" folder that will be shared by default. Consequently, the information provided could be affirmatively misleading. Nor has this interface improved materially in the more recent versions of Morpheus.

Finally, other disclosures decreased over time. Information can be disclosed in ways that make it too ambiguous to be useful. For example, in THE HITCHHIKER'S GUIDE TO THE GALAXY, aliens create a supercomputer called Deep Thought to calculate the meaning of life, the universe, and everything. After calculating for ages, Deep Thought discloses that the answer to the meaning of life, the universe and everthing is "42." Just "42." This disclosure does not really illuminate the meaning of life.

Fortunately, real-world filesharing programs have provided main-interface disclosures about sharing more useful than the information provided by the fictional computer Deep Thought. One of the best of these displays appears in 2003 and 2004 versions of LimeWire. This display appeared at the bottom left of the main interface:

Figure 2: LimeWire 4.0.7

This display is not perfect: It does not clearly inform the user that *they* are the one sharing these files. Users migrating from KaZaA might find this ambiguity particularly confusing because the lower left of the KaZaA main interface provides information about files shared by *other* users of the KaZaA program. Nor does this display reveal how the user might disable the sharing disclosed. Nevertheless, this display could provide useful information to some users and with minor modifications, it might have been even more informative.

Given that this best-of-class display could have easily become even more useful and informative, one might wonder whether it has changed over time. It has. In early 2006, this display looked like this:

Figure 3: LimeWire 4.10.9

"42." Just "42." In other words, this user is sharing 42 files. LimeWire's once-useful display became a real-world implementation of Deep Thought.

In summary, some programs disclosed less information about their redistribution features after the filing of copyright-enforcement lawsuits made this information more important to users. This suggests that redistribution feature can cause new or unsophisticated users to share downloaded files inadvertently. But as potential duping schemes, redistribution features would have two weaknesses.

First, redistribution features are not really that difficult to detect or disable. While the deployment of redistribution features may have radically increased users' propensity to share files in 2001, their effects soon faded: For example, a study using data collected in mid-2002 reported that 42% of studied Gnutella users shared no files.[33]

Second, redistribution features cannot add new content to a network. In particular, they cannot cause users to inadvertently share the large collections of *existing* media files stored on their computers, (such as those copied from purchased CDs).[34]

Consequently, a distributor might deploy other "technological features to induce users to share" that would compensate for these inherent weaknesses of redistribution features. It thus becomes important to determine whether popular filesharing programs have contained, or do contain, features that could cause users to inadvertently share *existing* files already stored on their computers.

All five programs examined have contained such features. Many still do.

B. Search-wizard and share-folder features can cause users to infringe copyrights—or jeopardize their own financial or personal safety—by sharing existing files inadvertently.

In mid-2002, computer-science researchers from HP Labs showed that distributors of filesharing programs had deployed two features that could cause users to inadvertently share existing files stored on their computers:

- **Search-wizard features**: Search wizards may activate automatically, or they may be activated by the user. When activated, these features scan portions of a user's hard drive and then identify folders that contain "triggering" file types, which usually include audio files, audiovisual files, and document files. A list of identified folders is then displayed. Some search wizards merely recommend sharing of listed folders—these folders will be shared only if the user checks an associated checkbox. Others will automatically select all listed folders for sharing. Search wizards were often included in filesharing programs' installation-and-setup processes; they may also be accessed from menus within the programs.

- **Share-folder features**: By default, most filesharing programs store downloaded files in a folder created by the program during installation. A share-folder feature lets the user select a different folder to store downloaded files. But it does so through an interface that does not clearly warn the user that the selected folder, and usually its subfolders, will be "shared" with other users.[35]

These search-wizard and share-folder features usually cause *recursive sharing*: They will "share" not only the files stored in a folder selected by a search-wizard or share-folder feature, but also files stored *in any subfolder* of the selected folder. In short, a recursive-sharing search-wizard or share-folder feature treats a user's instruction to store files in, or share, one folder as an authorization to share that folder and many other folders and files.

The inadvertent sharing of *existing* folders and files can have dangerous effects. Like inadvertent sharing of downloaded files, inadvertent sharing of existing files can make a user a high-volume uploader of infringing files. For example, a user might try to store downloaded files in his "My Documents" or "My Music" folder because these folders probably contain no existing files, only subfolders. Recursive sharing would then cause this user to "share" the thousands of audio files copied from purchased CDs stored in subfolders of "My Music."

But inadvertent sharing of existing files can also have other effects—thanks to a post-*Napster* change in the design of most filesharing programs. Napster, Inc.'s filesharing program shared only audio files. After the *Napster* litigation, distributors of filesharing programs were advised to bolster their capacity-for-substantial-noninfringing-use defense by redesigning their programs to share almost *all* types of files by default: "[I]f you're developing a file-sharing system or distributed search engine, support all file types, not just MP3 or Divx files."[36] Such advice was widely followed: KaZaA, LimeWire, BearShare, eDonkey, and Morpheus now share almost all types of files by default.

This changed behavior makes inadvertent sharing of existing files very dangerous. Most computers now store files containing highly sensitive information.[37] These files may contain sensitive personal information—credit card data, financial information, tax returns, scans of legal or medical records, digital photographs, personal correspondence, business documents, or other similar files. They may also contain sensitive information owned by an employer or another user of the computer. Inadvertent sharing of such files could result in identity theft, disclosure of trade secrets, economic espionage, or worse.[38]

Because inadvertent sharing of existing files and folders can have such serious consequences, it is critical to note how this problem was called to the attention of distributors of filesharing programs, how they responded, and what happened afterwards.

In the June 2002 study *Usability and Privacy: A Study of KaZaA P2P File-Sharing*, researchers Nathaniel Good and Aaron Krekelberg showed that users of the KaZaA filesharing program were sharing so many sensitive personal files that identity thieves had begun data-mining the KaZaA network for inadvertently shared credit-card data.[39]

To determine why users were sharing files inadvertently, *Usability and Privacy* developed four usability guidelines for responsible developers of filesharing programs and conducted a user study. The users studied were adults, and almost all of them were relatively sophisticated: All were regular computer users; all "were given a short tutorial on file sharing, and the concept of a shared folder"; and 83% had previously used filesharing programs.

Based upon the usability guidelines and the user study, *Usability and Privacy* concluded that KaZaA was unsafe. Its user interface was "weighted too heavily in favor of sharing files." *Usability and Privacy* revealed two features in the KaZaA interface that could cause users to share existing files inadvertently. These were the KaZaA share-folder and search-wizard features.[40]

The KaZaA share-folder feature was accessed from the program's "Options" menu. It would present the user with the following interface:

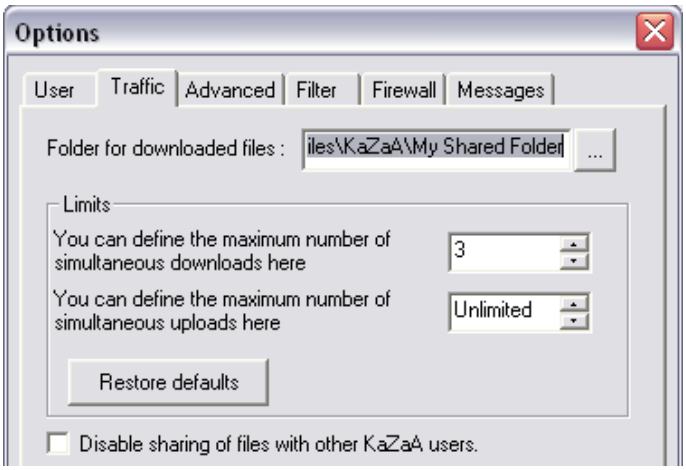

Figure 4: KaZaA 1.7.1

Usability and Privacy summarized the problems with the KaZaA share-folder feature: "The word "folder" is singular, implying one folder, and does not hint that all folders below it will be recursively shared with others." Worse still, "the name 'download folder' implies that it will be used to store files that are downloaded and has nothing to do with sharing. It does not mention that this folder (and the folders and files underneath) will also be shared with others…." Indeed, the KaZaA share-folder feature gave users only one obscure hint that the "download folder" might be shared: A checkbox near the bottom of the interface was labeled "Disable sharing of files with other KaZaA users."

The KaZaA search-wizard feature had changed over time. In versions before 1.7.1, the wizard could be accessed during the program's installation-and-setup process, (when the user would be most unfamiliar with the program), and from the "Options" menu within the installed program. In versions 1.7 to 2.4, the wizard could only be accessed from the "Options" menu within the program. It was inactive by default, but if activated by the user, it would produce a results screen like this one:

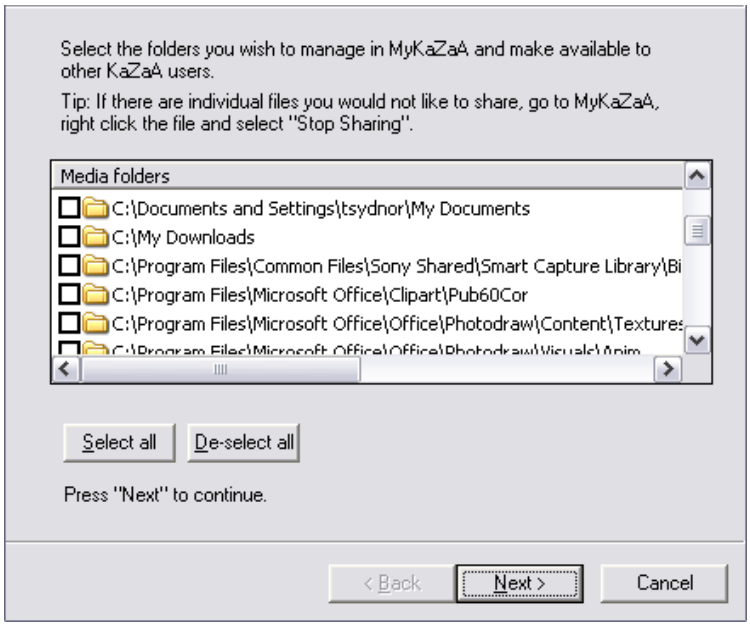

Figure 5: KaZaA 1.7.1

The results screen shown above shows the KaZaA search wizard "recommending" that the user share his "My Documents" folder. Note that "My Documents" will be shared only if the user checks the checkbox to the left of the folder path. But the user is not warned that "My Documents" will be shared recursively, and this information is essential if the user is to react intelligently to the absurd "recommendation" to share "My Documents."

Usability and Privacy cited many other problems with the results screen, including the following: (1) "it does not say what files in the 'My Documents' folder will be shared," (2) it "relies on the user's knowledge of what is capable of being shared by a file sharing program," and (3) "[i]t presumes that users have perfect knowledge of what kinds of files (and sub-directories with further files) are contained in these folders and that these

contents will be recursively shared." The study also confirmed that these presumptions did not correlate with reality: It noted, "Novice users are 'notoriously bad' at navigating hierarchical file structures," and it revealed that 75% of the users studied "believed that only multimedia files such as music, video and pictures could be shared."

Usability and Privacy concluded that "file sharing software is safe and usable if users … are clearly made aware of what files are being offered for others to download [and] do not make dangerous errors that can lead to unintentionally sharing private files…" It concluded that KaZaA failed to satisfy these standards. It warned that "lessons learned from KaZaA are applicable to designers working with other P2P systems," and that "the potential violation of user privacy and the current abuses that we noted" meant that eliminating features that were causing inadvertent sharing of existing files "should be a top priority for file sharing applications.…"

Because inadvertent sharing of existing files had such dangerous consequences, *Usability and Privacy* prompted two congressional hearings. During a hearing before the House Committee on Government Reform, staff investigators confirmed that thousands of users of filesharing programs were inadvertently sharing data files for popular finance-management software that could contain account numbers and detailed records about a user's finances.[41] During a hearing before the Senate Committee on the Judiciary, legislators repeatedly warned distributors that unless they eliminated features that caused users to share existing files inadvertently, their programs would compromise national security:

- "[I]n government agencies, employee use of P2P networks could … disclose sensitive government data to the enemies of this country."

- "[I]f the user is a government employee … sensitive government information could be made available to those unfriendly to the United States."

- "For government users, the situation is far worse. Not only personally sensitive information can be stolen, but information vital to the functioning of government, as well. Confidential memos, Defense Department information, law enforcement records, all could be available to any Internet user with some free software and the desire to go looking."[42]

In the aftermath of *Usability and Privacy* and the hearings, distributors of various filesharing programs were differently situated as to the problems identified. One needed only to refrain from adding features that had been shown to cause users to share existing files inadvertently. *Usability and Privacy* had noted that inadvertent sharing of sensitive files was less common on the Gnutella network. The design of the Gnutella-based program LimeWire may explain why: From at least the beginning of 2002 through June 2003, LimeWire contained neither a search-wizard nor a share-folder feature.

But most distributors of popular filesharing programs had deployed share-folder or search-wizard features. During the hearings, the distributors of KaZaA assured legislators, "[W]e welcome intelligent research like that done by Good and Krekelberg

and we always incorporate it into our product development plans."[43] They promised that the forthcoming release of KaZaA 2.5 would redress the identified problems.

After the hearings, other distributors claimed that they too had moved swiftly to redress inadvertent sharing of existing files. For example, on September 29, 2003, the distributors of Morpheus, BearShare, LimeWire, and eDonkey published a *Code of Conduct* that imposed the following obligations:

- "[Our] software and associated user instructions shall conspicuously require the user to confirm the folder(s) containing the file material that the user wishes to make available to other users before making such material available, and"

- "[Our] software and associated user instructions … shall be designed to reasonably prevent the inadvertent designation of the content of the user's … principal data repository … as material available to other users."[44]

On its face, the *Code* bars the use of KaZaA-like share-folder and search-wizard features on two separate grounds: Those features did not "conspicuously" require users to confirm that they wished to share all the folders that these features would actually share, and they were not designed "to reasonably prevent" sharing of a user's principal data repository. More importantly, the *Code*'s generally worded obligations also prohibit virtually any other feature that might cause inadvertent sharing—including, for example, a poorly disclosed redistribution feature.

Consequently, by September 29, 2003, the distributors of *all* of the programs studied in this report had declared that they would end the use of KaZaA-like share-folder or search-wizard features. These declarations also seemed credible: *Usability and Privacy* and the 2003 hearings had not treated misleading search-wizard and share-folder features as potential duping schemes. To the contrary, they were treated as mistakes in interface design that responsible distributors should correct.

Indeed, by mid 2004, distributors were claiming that they had responded so thoroughly that the problem of inadvertent sharing of existing files had become a mere "urban myth." On June 23, 2004, the distributors of Morpheus, BearShare, and eDonkey testified to a Senate Subcommittee that they had created "safeguards" that would "render the feared 'broadcast' of personal data to 'millions of others of Internet users' … wholly without foundation." They testified, "[A]s far as [we] are concerned, allegations that it is easy for a user to inadvertently 'publish' sensitive materials like … tax information through our software is literally the equivalent of an urban myth…."[45]

This same attitude also appears in the response that the distributors of BearShare, eDonkey, and Morpheus offered to a frequently-asked question about whether use of a filesharing program increases a user's risk of identity theft: "Absolutely nothing about peer-to-peer software itself … increases the odds that a user's personal information can or will be accessed by some unknown person."[46]

On January 18, 2005, the distributors of Morpheus, BearShare, and eDonkey submitted the following written statement to the Federal Trade Commission:

> *Myth*: "Thousands" of people's personal data—such as health, tax, and other financial material—has been and is inadvertently made available through P2P software programs, which make such breaches of personal security easy and whose developers don't seem to care.
>
> FACT: As [we] testified before Sen. Smith last June, these allegations are among the most egregiously false claims about [our] software. They appear, however, to have the inexplicable staying power of "an urban myth, no more accurate—though easily as persistent—as reports of alligators in New York's storm drains."
>
> In fact, users of our … software must affirmatively create and populate "shared" document folders and are subject to multiple cautions about the importance of not affirmatively placing sensitive material in them. Moreover only files downloaded with our … programs are "routed to such shared folders…. No existing information on a users' [sic] hard drive can "migrate" to those shared folders on its own.[47]

These, and similar, representations certainly made it appear that distributors of filesharing programs had moved quickly, responsibly, and effectively to redress the problem of inadvertent sharing of sensitive files.

But then, from 2004 to the present, inadvertent sharing of sensitive files began to recur:

- CBS Marketwatch reported that BearShare users were again inadvertently sharing "tax returns" and "private medical files and private bank statements." A BearShare spokesman said, "As I understand it, a new version will be coming out literally in a matter of days that will seek to close any possible vulnerabilities of this."[48]

- The website *See What You Share* reported that criminals were again mining filesharing networks for inadvertently shared data. It reported that identity thieves were searching for inadvertently shared financial data. It also reported that pedophiles were searching filesharing networks for hard-core child pornography—and for inadvertently shared data about particular children.[49]

- The security company Blue Security reported that inadvertent sharing had become so widespread that spammers were "systematically" data-mining filesharing networks to find inadvertently shared email addresses. Blue Security found "hundreds of incidents where files containing email addresses were made accessible to any Internet user." These incidents involved "[m]any files [that] contained sensitive personal and business information, for example: a list of professors teaching in a well known university, email addresses of pro-gay

marriage supporters and a complete customer list of a certain Internet store, along with customer contact information."[50]

Recently, Howard Schmidt, former White House cybersecurity advisor and co-author of the National Cyber-Security Policy, warned that inadvertent sharing has become pervasive, affecting both corporations and individuals. He found corporations sharing internal audit reports, human-resource records, internal litigation documents, and security manuals: "I've seen thousands of documents containing internal administrative passwords which are now being shared throughout the world." He warned, "The risk is that [criminals] are now searching for corporate information—P2P search strings [we've identified] show that they're actively seeking those documents." The problem also affected individuals: "In one case of this sort, a criminal searched for and found 117,000 medical-record passwords—just by knowing how to search in a P2P app on the Web." He also warned that "one woman's credit-card information was found in such disparate places as Troy, Mich., Tobago, Slovenia, and a dozen other places. Why? We found that the 'shared' folder in her music-downloading application was in fact making readily available her entire 'My Documents' folder to that app's entire P2P audience, 24 hours per day." Inadvertent sharing had thus become "a major part of the current identity theft problem."[51]

The Department of Homeland Security (DHS) also reported another consequence of continued inadvertent sharing of sensitive files—one both foreseeable and foreseen. In a bulletin sent to all Federal Agencies and all state and local agencies involved in homeland security, DHS warned that government employees or contractors using filesharing programs had repeatedly compromised national and military security:

- "There are documented incidents of P2P file sharing where Department of Defense (DoD) sensitive documents have been found on non-US computers with no protection against hostile intelligence services."

- "[T]here is a military investigation … in which classified material has been wrongfully disclosed using P2P."

- "Multiple organizations have ongoing investigations into disclosure of sensitive or classified material due to P2P."

- "These applications represent a vulnerability that cannot be afforded without a strong justification."[52]

Given that distributors had been warned that this would happen unless they eliminated features that could cause users to share existing files inadvertently, the DHS bulletin raises a question: Did distributors of popular filesharing programs actually eliminate and halt the effects of dangerous search-wizard and share-folder features like those condemned in *Usability and Privacy*?

The answer to this question is "No": None of the distributors of the five programs analyzed here did so. Indeed, except for the distributors of KaZaA, these distributors

either began or continued to deploy either search-wizard or share-folder features, or both, in studied versions of their programs released during 2004 and 2005. In many cases, 2004 and 2005 versions of these features were actually *more dangerous* than the search-wizard and share-folder features condemned in *Usability and Privacy* and the 2003 congressional hearings.

And as these features migrated from FastTrack to other networks, so too did the problem of inadvertent sharing of sensitive files. In 2002, when FastTrack-based programs like KaZaA were deploying search-wizard and share-folder features, a survey by the authors of *Usability and Privacy* found more inadvertent sharing on the FastTrack network than the Gnutella network.

In 2004, when KaZaA had eliminated such features prospectively and many Gnutella-based programs had deployed them, another informal survey found more inadvertent sharing on the Gnutella network.[53] An informal survey of relative levels of inadvertent sharing conducted for this report also indicated that inadvertent sharing of personal files is most prevalent on Gnutella, the network used by the programs deploying the most aggressive search-wizard and share-folder features in 2005.

1. Share-folder features were widely deployed after their potential to cause inadvertent sharing was known.

During 2004, 2005, and 2006, the distributors of BearShare, eDonkey, LimeWire, and Morpheus deployed share-folder features in studied versions of their programs. In BearShare, Morpheus, and LimeWire, these share-folder features would cause recursive sharing. Often, these features were more problematic than the KaZaA share-folder feature condemned in *Usability and Privacy*. For example, the Options Menu of a 2004 version of LimeWire contains two sub-menus: One is titled "Saving" and the other "Sharing." The "Saving" menu displays the LimeWire share-folder feature:

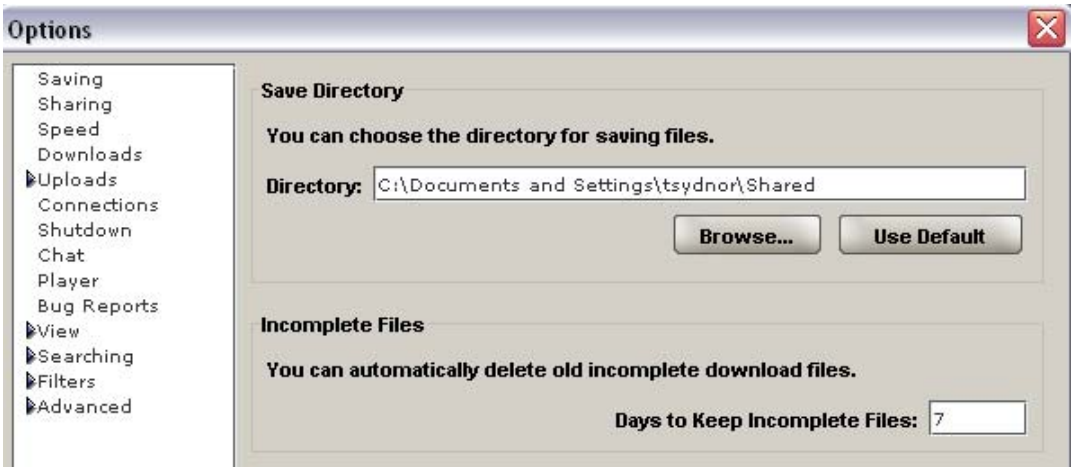

Figure 6: LimeWire 4.0.7

In short, the user is told that this is a "Save Directory"—and left to figure out that in LimeWire, "save" means "share recursively." This is actually worse than the KaZaA share-folder feature: The user receives not even a hint that a folder selected as the "Save Directory" will be shared—much less shared recursively. Nor is the LimeWire share-folder feature unique.

The following screenshot shows the "Downloads" tab on the BearShare Setup menu. Note that there is a separate tab called "Uploads":

Figure 7

Again, the user gets no hint that selecting a folder to store downloaded files in the "Downloads" menu will recursively share all files in that folder and all files in all of its subfolders. Nor would the BearShare *User's Guide* help; it had only this to say about the "Downloads" menu: "Here is where you indicate where files will go when you download them. The default directories are entered for you, but you can change them by clicking 'Browse' and entering a new location for your downloads." Consequently neither the program nor its user instructions "conspicuously require the user to confirm the folder(s) containing the file material that the user wishes to make available to other users before making such material available…."[54] A user does not "conspicuously confirm" that he or she wishes to share a particular folder by selecting it to store downloaded files through a menu that reveals neither that the selected folder will be shared nor that all of its subfolders will be shared recursively.

The LimeWire and BearShare share-folder features were also more dangerous than the KaZaA share-folder feature for a second reason. Unlike KaZaA, LimeWire and BearShare incorporated share-folder features into their setup processes—a decision that could increase the threat that these features pose to new users.

Share-folder features like these can have particularly devastating effects when a filesharing programs is used on a computer connected to a governmental, corporate, or home network. For example, on some networks, using a share-folder feature to store downloaded files in "Documents and Settings" can recursively share the files of *all other users* of the network in question.

Moreover, the share-folder features in some recent versions of LimeWire, BearShare, eDonkey, and Morpheus are actually worse than they appear because they encode a behavior not discussed in *Usability and Privacy*. For example, imagine that a LimeWire user designates "My Music" as her "Save Directory" because this folder contains no existing files, only subfolders. Later, this user discovers that the recursive sharing thus enabled has caused her to share thousands of audio files copied from purchased CDs.

Realizing that she has now become a copyright-enforcement target, the user re-opens the "Saving" menu and sees that LimeWire provides a way to correct her mistake: There is a "Use default" button below and to the right of the "Save Directory":

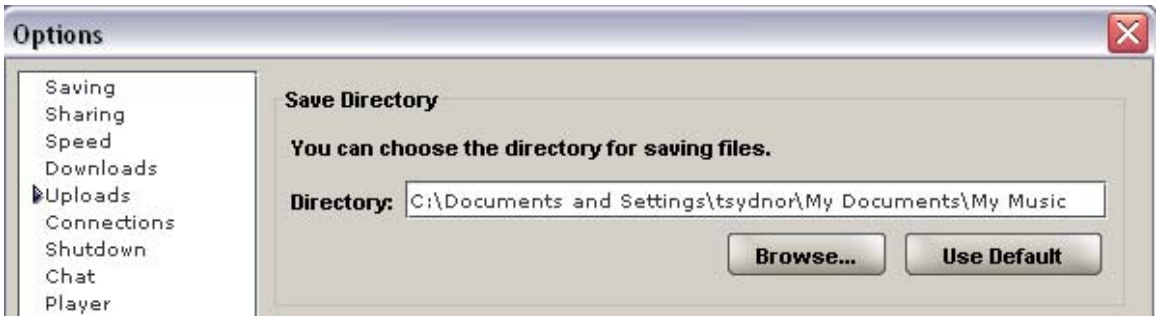

Figure 8: LimeWire 4.0.7

She clicks the "Use default" button and is relieved to see that the "Save Directory" is instantly reset to the empty default "Shared" folder created by LimeWire:

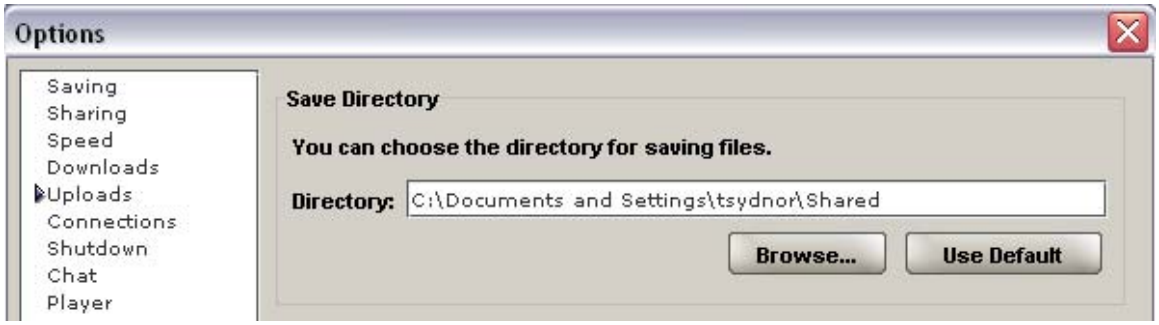

Figure 9: LimeWire 4.0.7

A user viewing the interface shown in Figure 9 might think, "Problem solved!" But nothing has changed: LimeWire is still sharing all files stored in the user's "My Music" folder and all of its subfolders. Share-folder features like those used by LimeWire, BearShare, Morpheus, and eDonkey exhibit a behavior that can be called "librarying": A folder "shared" through the share-folder feature will remain shared *even if the share-folder feature is reset to its "default" setting or used to select a different folder to store downloaded files.* A "librarying" share-folder feature is a one-way ratchet: Successive uses of it can only cause users to share *more* files and folders—never less.

It is difficult to justify the behavior of librarying share-folder features: Even were a distributor to assume that users would instinctively know that any folder used to store downloads will *always* be shared by default, then this justification for sharing would end once a folder ceased to be used as the download folder.

Moreover, undisclosed share-folder features would be obviously problematic even if they had not been specifically condemned in *Usability and Privacy*. If a distributor gains access to existing files on a user's computer by failing to disclose that any folder used to stored downloaded files will be shared—or by failing to disclose that such sharing will be recursive—then the user has really not authorized anyone to access or download those files. It is illegal to gain unauthorized access to data on someone else's computer or to exceed the scope of authorized access to such data.[55]

The LimeWire share-folder feature is particularly inexplicable. For example, in 2004, LimeWire purported to explain why distributors of filesharing programs had failed to resolve the problem of inadvertent sharing of existing files:

> We have been looking at addressing the accidental sharing issue for a while. Certainly, more can be done.…
>
> That being said, these are file sharing applications. The main goal of a file sharing application is to make it easy for users to share files. Users need to be aware of what they are doing.…
>
> Given that file sharing is still a relatively new type of application, it makes sense that the developers have not worked out all of the security issues. We are still focused on improving the P2P protocol.[56]

In short, LimeWire claimed that it was too busy helping others download whatever files users did happen to "share" to ensure that users shared only those files that they *intended* to share. Even ignoring the odd priorities thus revealed, this claim still flounders on an awkward fact: Researchers, Congress, *and LimeWire itself* had "worked out" the rather obvious "security issues" raised by share-folder features.

By 2004, *Usability and Privacy* and two congressional hearings had already "worked out" the security issues raised by share-folder features. But LimeWire's distributors had already "worked out" those issues for themselves. In 2001 and 2002, LimeWire would

twice display the following question and warning after a user selected a new folder to store downloaded files:

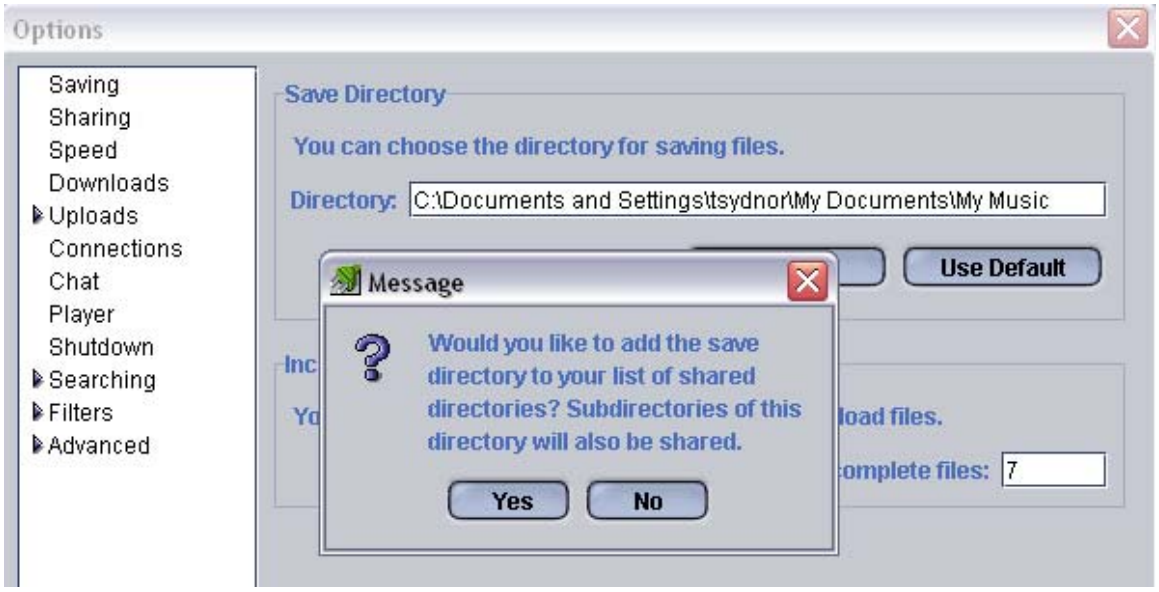

Figure 10: LimeWire 2.0.4

This dialog box shows that LimeWire's distributors needed neither published research nor Congress to inform them that users might not want to share an existing folder used to store downloaded files *and* that users must be warned that such a folder would be shared—and shared recursively—in order to make an informed decision about whether to share it at all. Only after *Usability and Privacy* was published—and its findings highlighted in congressional hearings—did the distributors of LimeWire modify the LimeWire program, remove its warnings, automate sharing of the download folder, and create the undisclosed, recursive-sharing, librarying share-folder feature discussed previously.

2. Search-wizard features continued to be widely deployed after their potential to cause inadvertent sharing had been identified.

In addition to share-folder features, distributors of popular file-sharing programs also continued, or began, to deploy search-wizard features in the aftermath of *Usability and Privacy* and the two congressional hearings.

For example, LimeWire began to deploy a search-wizard during 2003. Like the more aggressive wizard in pre-1.7.1 versions of KaZaA, it was incorporated into LimeWire's installation and setup process:

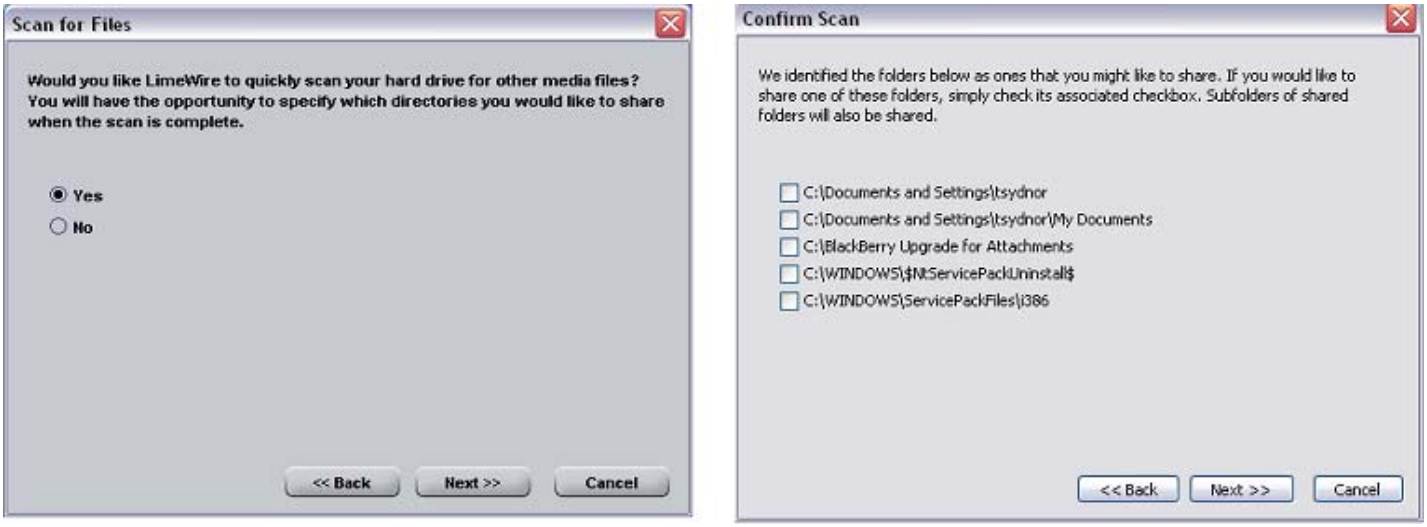

Figure 11: LimeWire 4.10.9

In one way, this is an improved search-wizard: The results screen states that selected folders will be shared recursively. But the user is only told that the wizard will scan for "media files"—not that it will share all files in any folder selected for sharing. Moreover, the notice of recursive sharing reaffirms a more fundamental defect identified by *Usability and Privacy*: Arguably, search-wizard features might assist those users who are "notoriously bad" at conceptualizing folder structures—those do not really know where in their folder hierarchy various files are stored. But to respond intelligently to a wizard's recommendations, a user must have "perfect knowledge" of all the files stored in all the subfolders of any folder identified for potential sharing and which of those types of files will be shared by default. Consequently, the users who, in theory, might benefit from a search wizard will lack, in practice, the near-perfect knowledge of file and folder locations and relationships needed to respond properly to the recommendations of a recursive-sharing search wizard. It may thus be nearly impossible to adequately disclose a search-wizard or share-folder feature that causes recursive sharing.

Like share-folder features, search-wizard features sometimes became even more aggressive than those condemned in *Usability and Privacy*. For example, here is the results screen from the search wizard used in a 2005 version of BearShare:

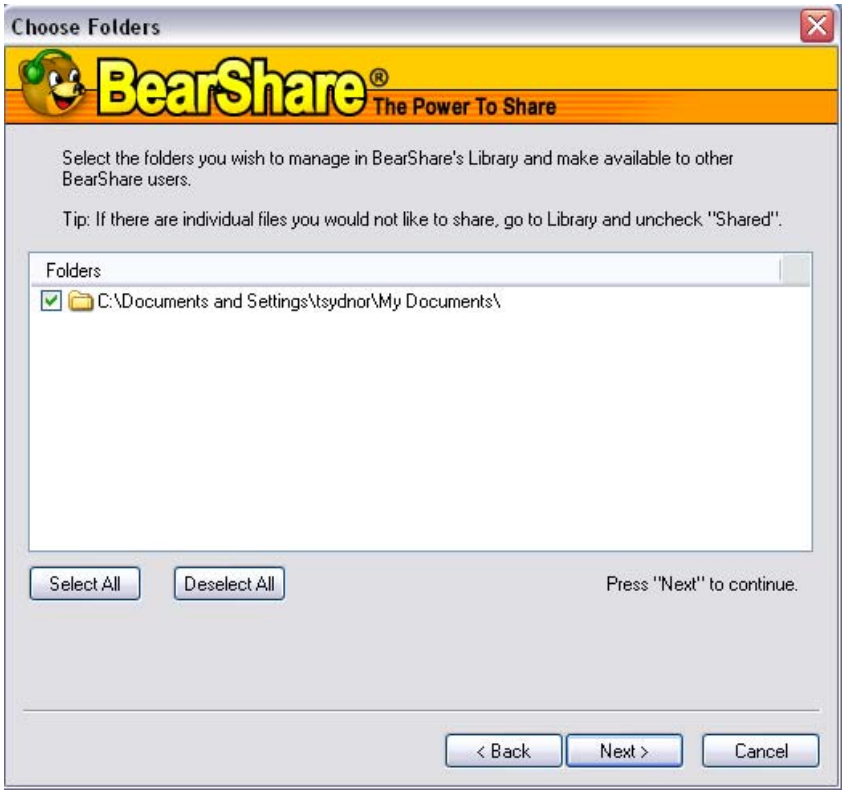

Figure 12: BearShare 4.7.0.76

Like the more aggressive version of the KaZaA search wizard, the BearShare search wizard appears during the installation-and-setup process—when users will be least familiar with the program's behavior and its implications. But unlike the KaZaA search-wizard, the BearShare wizard *selects* for sharing all folders that it identifies: Once the wizard is triggered, every folder listed by the wizard will be shared—and shared recursively—unless the user acts affirmatively to prevent this. And as Figure 12 shows, this search wizard will select for recursive sharing the user's "My Documents" folder.

Public data provides no clear answer about whether Morpheus began or continued to deploy a search-wizard feature after mid-2003. In June of 2004, the distributors of Morpheus testified to a Senate Subcommittee that they had moved decisively to prevent users from inadvertently sharing existing files:

> [A]t no time and under no circumstances is … any existing file on a user's computer[] automatically made available to other Morpheus users. Rather, all the software does by default upon installation is create two empty folders….
>
> One folder, the 'Shared Folder' is intended to accept files manually inserted by users that they wish to share. The other 'Download Folder' is where files that our users download using our software will reside…
>
> Thus, functionally speaking, only files downloaded to or intentionally placed in a user's "Shared Folder" will be available to other P2P software

> users. These safeguards render the feared "broadcast" of personal data … wholly without foundation.

Unfortunately, this testimony fails to respond *at all* to the concerns raised in *Usability and Privacy* and the congressional hearings. Nor does it reveal whether the distributors of Morpheus were abiding by the *Code of Conduct* that they had drafted: If this testimony accurately described how the then-current version of Morpheus behaved, it could still have contained share-folder and search-wizard feature more aggressive than those condemned in *Usability and Privacy*.

The quoted testimony is unresponsive because it proceeds from a false premise: It claims that concerns about the "'broadcast' of personal data" are "wholly without foundation" unless a filesharing program "automatically" shares users' existing files and folders. This is wrong: The KaZaA search-wizard and share-folder feature did not activate "automatically," but both were problematic. *Usability and Privacy* had noted that while a "default setup [of KaZaA] where file sharing is disabled" is "relatively safe," "user modification of various settings" was not safe.

But if this testimony was otherwise accurate, then it would, at least, show that the then-current version of Morpheus did not contain, in its setup process, a search-wizard feature that was active by default and that would share identified folders by default. But if so, then this state of affairs may have changed. The following screenshot shows the result of a default installation of an early-2005 version of Morpheus.

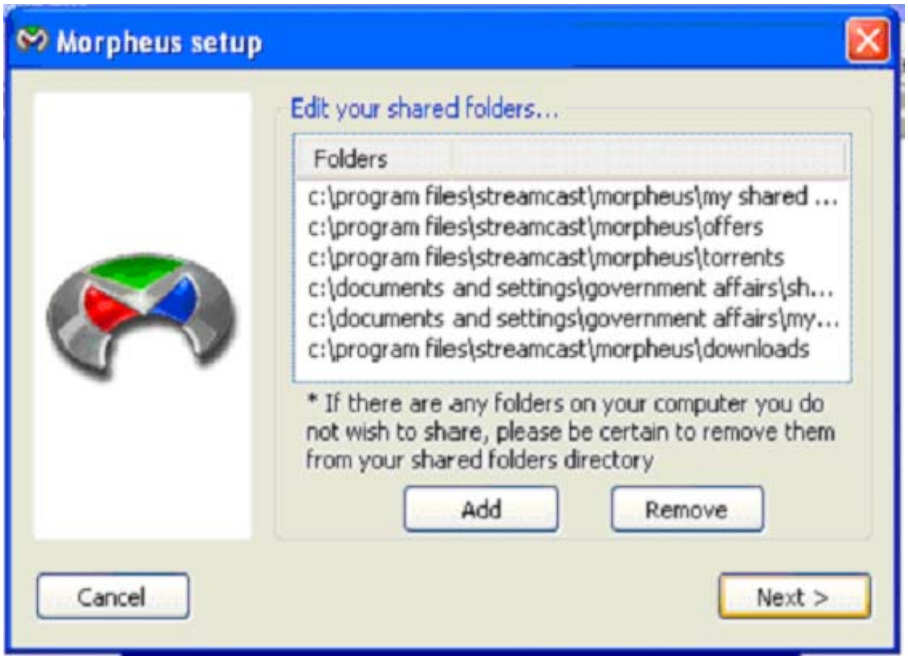

Figure 13: Morpheus 4.7.1.326

This screenshot shows Morpheus sharing *six* folders automatically. Four of these folders appear to be specially created by the Morpheus program. Two of these folders appear to be existing folders, and one appears to be "My Documents"—though this version, like

others, truncates folder pathnames in a way that makes it difficult to be sure which folder is being shared. In short, this screenshot *may* show that one or more 2005 versions of Morpheus incorporated a search wizard feature—one that would activate by default and share identified folders by default.

Nothing more definite can be said about the meaning of this screenshot. The 4 and 5-series versions of Morpheus install in a way that prevents the replication of the experiment that produced this screenshot.[57] Consequently, it is possible that this version of Morpheus actually contained a different "feature" that can produce effects akin to those of a fully automatic search-wizard feature. The following hypothetical illustrates the potential consequences of this "feature" in a multiple-user environment like a private home or a college dormitory. The hypothetical uses BearShare because older versions of this program are more readily available.

Suppose that a man who owns an Internet-connected home computer hosts a party for his relatives. During the party, a bored 13-year-old nephew leaves the gathering and installs BearShare onto his uncle's computer to download some files. To make downloaded files easy to find, the boy sets the download folder to "My Documents," a folder that contains no existing files, only subfolders. As he is downloading, the boy realizes that he has—somehow—begun sharing thousands of files from his uncle's computer. He exits BearShare and immediately uninstalls the program. Shaken, he returns to the party, believing that he has corrected his mistake.

Much later, his uncle reads a report that declares filesharing programs to be "technologies of freedom" and "technologies of innovation."[58] Intrigued, he downloads and installs BearShare. The installation and setup process would reveal no information about sharing. Nevertheless, were this user to find the tiny "Folders" button on the Library interface of BearShare and drill down into the folder tree, he would find that BearShare had automatically and recursively shared the following folders:

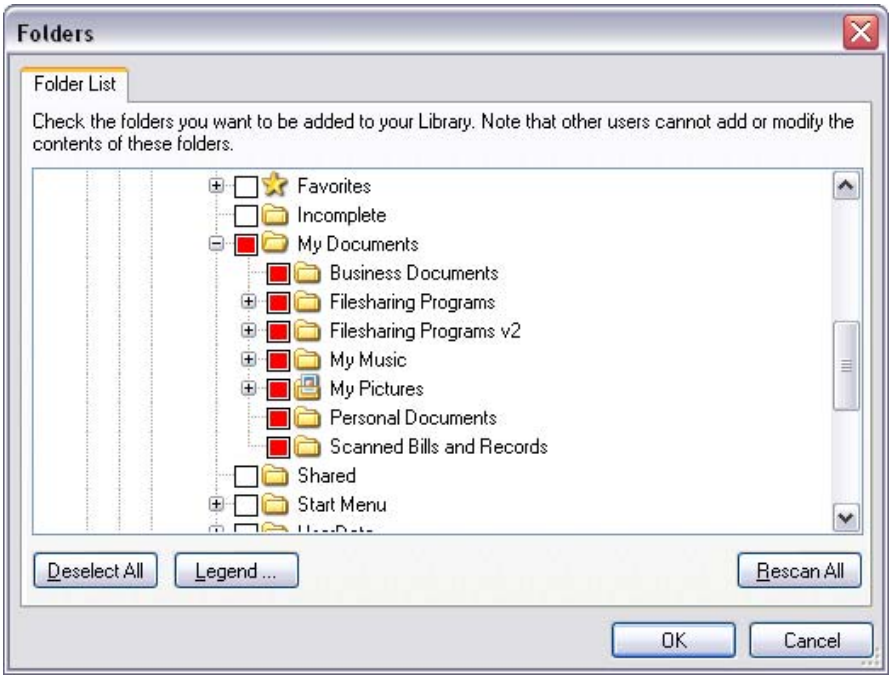

Figure 14: BearShare 4.7.0.76

This happened because versions of BearShare—like some versions of LimeWire, KaZaA, and other programs —contain what could be called a "partial-uninstall" feature: If a user tries to uninstall one of these programs, the process will leave behind a file that records the folders shared by the uninstalled program. If anyone ever installs any subsequent version of the same program, the new installation will automatically begin recursively sharing all the folders that were shared by the uninstalled copy of the program. Predictably, a partial-uninstall feature violates yet another provision of the *Code of Conduct* drafted by the distributors of BearShare, eDonkey, LimeWire, and Morpheus: "A method by which a Member's software (and any other software installed with it) *readily may be uninstalled* by the user shall be provided to users."

Nor is this a technical violation: A partial-uninstall "feature" ensures that programs like BearShare or Morpheus can automatically, and by default, recursively share existing files and folders on a user's computer.[59] As *Usability and Privacy* noted, most home computers are used by more than one person. A partial-uninstall "feature" ensures that someone installing a filesharing program on such a computer cannot be sure *what* files and folders the program will share automatically. Therefore, unless you are installing a filesharing program with this feature on a brand-new computer—or on a computer to which no other person has ever had access—then statements like the following may not be accurate:

> [A]t no time and under no circumstances is … any existing file on a user's computer[] automatically made available to other … users. Rather, all the software does by default upon installation is create two empty folders….

3. "Fixing" the effects of share-folder and search-wizard features—by perpetuating them.

One more behavior relating to search-wizard and share-folder features bears note. These features have repeatedly caused users to share existing, sensitive or infringing files inadvertently. When distributors who deployed such features were "caught" causing their users to share sensitive files inadvertently, they responded by claiming that new versions of their programs would correct inadvertent sharing caused by previous versions:

- KaZaA (2003): "[W]e changed a lot of the settings so that users wouldn't be inadvertently sharing files."[60]

- LimeWire (2004): "The LimeWire installation is a little dangerous for people who don't pay attention, and we'll have to address this issue in future releases …."[61]

- BearShare (2005): "[A] new version will be coming out literally in a matter of days that will seek to close any possible vulnerabilities of this."[62]

In two out of three of these cases, the promised improvements were not delivered. For example, the installation-and-setup process in LimeWire 4.10.9 seems unimproved from 2004 versions. BearShare kept its librarying, recursive-sharing share-folder feature in its program but removed the search wizard from its setup process. By contrast, KaZaA 2.5 did eliminate previously deployed search-wizard or share-folder features.

But even in the cases of KaZaA and BearShare, only *new* users of these programs—those who had never before installed any previous version of these programs on their computer—would have benefited from these changes. In the case of KaZaA, that benefit was probably material. In the case of BearShare, it appears marginal.

But the vast installed base of e*xisting* users of these programs—those upgrading from the prior versions of KaZaA or BearShare that contained features that *had* caused inadvertent sharing—*did not* benefit from these changes: Existing users never had their filesharing preferences reset or rechecked. In effect, distributors who responded to incidents of inadvertent sharing by changing share-folder or search-wizard features created an appearance of improvement that actually *perpetuated* inadvertent sharing caused by previous, (and concededly defective), versions of their programs.

The distributors of BearShare may have further "perpetuated" these effects with bad advice that could *increase* users' risk of sharing files inadvertently. After converting inadvertent sharing of tax returns from an "urban myth" to a grim reality, BearShare's distributors published *An Important Word from BearShare about Keeping Your Private Files Private* and an *Important Privacy Notice for Users of BearShare Version 4.7.2 and Earlier*.[63] Readers of the *Important Word* and the *Important Privacy Notice* were told two myths about inadvertent sharing:

- ***Myth*: In BearShare, you can inadvertently share existing files only during the installation-and-setup process.** "After BearShare is installed, non-

downloaded files not specifically saved to the ['My Downloads'] folder will not be accessible to other BearShare users.… [A]fter the installation process is complete, the only non-downloaded files that can be shared with others through BearShare are files that you deliberately move or copy to the shared folder."

- **FACT: BearShare's share-folder feature ensures that users can inadvertently share "non-downloaded" files from within the program.** Before and after version 4.7.2, BearShare contained an undisclosed, recursive-sharing, librarying share-folder feature accessible from within the installed program. So "non-downloaded" files "can be shared with others through BearShare" *without* being "deliberately move[d] or cop[ied] to the shared folder."

- ***Myth*: To tell whether you are sharing existing sensitive files as a result of the search wizards in BearShare version 4.7.2 and lower, just check your "My Downloads" folder**: "During the installation process, BearShare will ask you whether you wish BearShare to include files already on your computer in a new shared folder [called 'My Downloads']. (This [search-wizard] option is presented on the 'Select Drives' screen.)… If you do not check any of the boxes next to the listed drives, no information on your computer at the time of installation will be included in your shared folder. HOWEVER, checking one or more listed drives *will* 'populate' your shared folder with existing files from the source(s) you have checked. If you checked one or more drives upon installation, or if you're not sure whether this was done, PLEASE CHECK THE CONTENTS OF YOUR SHARED FOLDER NOW TO BE CERTAIN THAT IT DOES NOT CONTAIN ANY FILES THAT YOU DO NOT WISH TO SHARE; PARTICULARLY FILES CONTAINING SENSITIVE PERSONAL INFORMATION…."

- **FACT: pre-4.7.2 BearShare search-wizards did not "populate" a user's "My Downloads" folder by copying existing files and folders into it.** In studied pre-4.7.2 versions of BearShare, search wizards shared existing files from their existing locations—they did not "include" those files in the user's "My Downloads" folder. As a result, a user recursively sharing his "My Documents" folder could check his "My Downloads" folder and find *no* sharing of *any* sensitive files. BearShare's distributors thus told users to look for inadvertent sharing of existing files in the one place in which it would almost *never* be found.

Each of these claims from the *Important Word* and the *Important Privacy Notice* is inaccurate. Neither could have been made by someone who understood how pre- and post-4.7.2 versions of BearShare actually worked.

BearShare's *Important Word* and *Important Privacy Notice* merely highlight a question that echoes through the short, ugly history of share-folder and search-wizard features: *Why?* Why did distributors keep deploying these obviously dangerous features after their propensity to harm users was repeatedly identified?

Public data cannot answer this question: It cannot reveal why the distributors of BearShare, eDonkey, LimeWire, and Morpheus began or continued to deploy dangerous

share-folder and search-wizard features during 2003, 2004, and 2005. But by doing so, they made a mockery of their own *Code of Conduct.* They also undermined the accuracy of their representations to Congress, Federal agencies, state attorneys general and the public. They eviscerated claims that responsible distributors of filesharing programs can self-regulate. And they may have helped achieve the previously inconceivable result of converting copyright piracy into a threat to national security.

But public data does reveal that while implementations of search-wizard and share-folder features recurred and worsened, the distributors deploying these features were again confronting an old problem—one that had recurred and worsened: Users of their programs no longer wanted to share files. Indeed, by mid-2004, users' desire to share files had declined so precipitously that researchers again concluded that the Gnutella network was on the verge of "collapse."

4. Free Riding on Gnutella Revisited: The Bell Tolls?

By mid-2004, distributors of popular filesharing programs were still deploying an array of features that had been shown to cause users to share files inadvertently. Inadequately disclosed redistribution features were common. Share-folder features were deployed in BearShare, eDonkey, Morpheus, and LimeWire. Search-wizard features were deployed in BearShare and LimeWire, and, it is unclear whether such a feature was, or would be, deployed in Morpheus. But by this time, two things had changed.

First, high-profile, well-publicized copyright-enforcement lawsuits had heightened public awareness of the consequences of sharing infringing files. Users thus had stronger incentives to avoid or limit the sharing of infringing files, particularly audio files.

Second, concerned users of filesharing programs could now find what distributors of filesharing programs had not provided: Detailed, program-specific, step-by-step, screenshot-illustrated instructions on how to disable sharing caused by redistribution, share-folder, and search-wizard features.[64] These instructions on how and why to disable sharing were provided by public interest groups, universities, and ISPs. EFF argues that these stop-sharing campaigns blunted the deterrent effects of copyright-enforcement lawsuits against users:

> To the extent file sharers are worried about the RIAA lawsuits, many are simply opting to continue downloading while refraining from uploading (this is known as "leeching" in the lexicon of the P2P world). Because the RIAA lawsuit campaign has, thus far, only targeted uploaders, leechers can continue downloading, evidently without risk.[65]

But if culpable users had stopped uploading the infringing files that they were downloading, this would suggest that sharing was decreasing. It would also suggest that distributors of filesharing programs using duping schemes to populate their networks with infringing files needed to evolve those schemes to counter this trend.

Coincidentally, in May of 2004, a team of computer-science researchers replicated much of the analysis performed in the 2000 study *Free Riding on Gnutella.*

In *Free Riding on Gnutella Revisited, The Bell Tolls,* the researchers reported that users' propensity to share files had decreased sharply: "Our results indicate that 85 percent of peers share no files."[66] Moreover, users who did share files still rarely shared popular files: The data presented showed that 1% of users now returned 50% of all responses to search queries.

Revisited also confirmed that "a significant volume of queries target copyrighted materials and that a similar proportion of responses refer to copyrighted files." It thus proposed that a "positive feedback loop" was discouraged sharing: Copyright enforcement discouraged sharing; this made those still sharing more vulnerable; and this increased vulnerability further discouraged sharing. *Revisited* thus concluded that if levels of sharing remained low and enforcement continued, "the logical conclusion of both trends will be the Gnutella network's collapse."

Revisited also proposed an answer to a longstanding question: *Free-Riding on Gnutella* had identified at least two "technological features to induce users to share"—a redistribution feature and a "forced sharing" feature that would compel users to share files. But while redistribution features became ubiquitous, forced-sharing features remained very rare. *Revisited* proposed that users' increasing desire to "leech" prevented distributors from deploying features that "enforced sharing of downloaded files": Distributors who deployed such features would quickly see 85% of their revenue-generating (but "leeching") users defect to other programs.[67]

For example, distributors could have encouraged sharing by deploying redistribution features that users *could not* disable. But such features—particularly if their effects were obvious and disclosed—would impose equal burdens upon both new and sophisticated users: Both groups could avoid sharing only by incurring the tedium and risks of copying downloaded files to a non-shared folder and then deleting them from the download folder. These burdens and risks might cause culpable "leechers" to defect.

But if sophisticated, culpable users would defect unless they could leech, then a distributor could make it more difficult for new or unsophisticated users to stop sharing files while ensuring that more sophisticated users could do so. Such a distributor might deploy what could be called a "coerced-sharing" feature: This type of feature would be neither obvious nor fully disclosed. It would make it difficult to disable sharing of the download folder while providing potentially misleading feedback suggesting, incorrectly, that sharing of the download folder could be easily disabled. Nevertheless, such a feature would provide a mechanism—an obscure, nonintuitive mechanism—that would let sophisticated users disable sharing of the download folder.[68] Of course, this sort of coerced-sharing feature would blatantly violate the conspicuous-confirmation requirement imposed by the *Code of Conduct* drafted by the distributors of BearShare, eDonkey, LimeWire, and Morpheus.

C. Recently, filesharing programs have deployed potentially misleading coerced-sharing features that make it difficult, but possible, for users to stop sharing downloaded files.

By mid 2005, BearShare, eDonkey, LimeWire, and Morpheus contained a coerced-sharing feature.[69] In each case, the feature could mislead new or unsophisticated users into believing that they had disabled sharing of the download folder. And in each case, there appears to be a mechanism—an obscure, nonintuitive, mechanism—that would let sophisticated users stop sharing the download folder.[70] Often, these coerced-sharing features appear to be recent additions to programs that once let users stop sharing their download folder.

For example, before mid-2005, version of Morpheus let users stop sharing the folder used to store downloaded files. More recent versions of Morpheus make it difficult for users to stop sharing the download folder, though some Morpheus users may think otherwise.

Recall the Morpheus 3.0.36 setup screen presented above in Figure 1. Three years later, the analogous setup screen in a 2006 version of Morpheus looked like this:

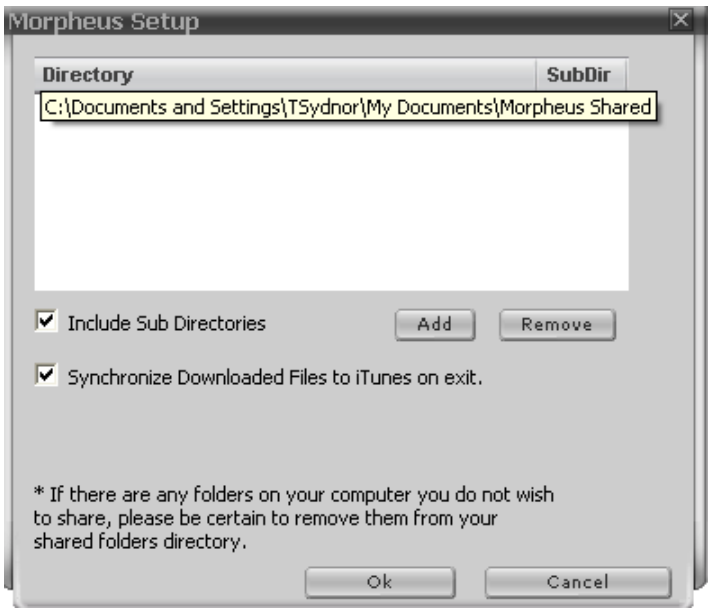

Figure 15: Morpheus 5.1.2

Note that the "edit your shared files" instruction has now vanished: The user must read to the end of the small, asterisked text at the bottom to find out what this interface is. Only one folder is listed, "Morpheus Shared." This folder will never store *any* files unless the user manually copies or moves files into it. But a few users might know—and others might guess—that the default download folder, "Downloads" is actually a subfolder of the "Morpheus Shared" folder displayed in the shared-folder list. Such users might also note that the "Include Sub Directories" checkbox is checked by default, and then select "Morpheus Shared" and click the "Remove" button to disable sharing. If they do, Morpheus would provide the following feedback on the consequences of their acts:

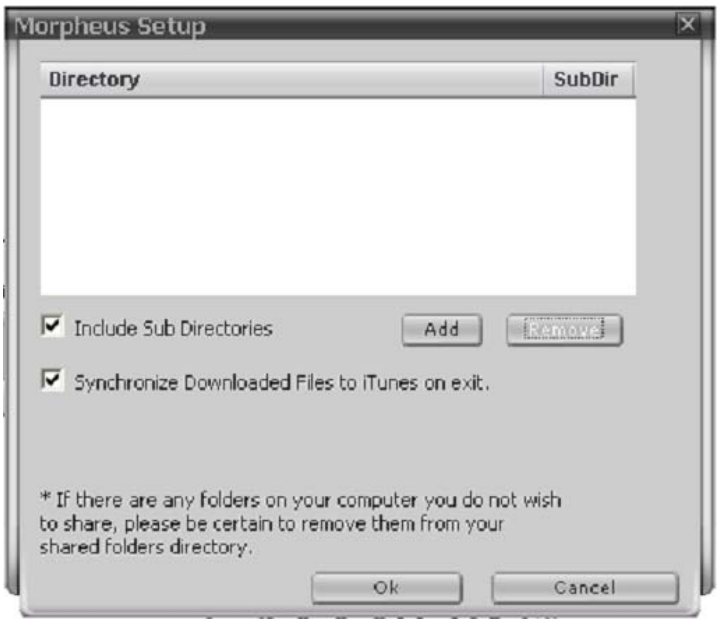

Figure 16: Morpheus 5.1.2

Users could reasonably conclude that this once-populated, now-empty "shared folders directory" indicates that they are not sharing *any* folders. But that is wrong: Morpheus is still sharing the download folder. Nor will the share/unshare interface within the program disable sharing of the download folder: Morpheus now has a coerced-sharing feature. This feature upends the *Code's* conspicuous-confirmation requirement: If users "conspicuously confirm" that they *do not* want to share the download folder, the program shares it anyway.

Users installing BearShare can also receive misleading feedback. During setup, BearShare presents users with a "Folder List" screen and the instruction "Check the folders that you want to add to your Library":

Figure 17: BearShare 5.2.3.7

If users correctly guess that “add to your Library” means “share”—and open the “Legends” submenu or guess correctly—then users will realize that BearShare’s “Folder List” outlines a folder’s checkbox in grey if neither it nor any of its subfolders will be shared, but it outlines a folder’s checkbox in red if it contains a shared subfolder. Such users might then realize that BearShare shares at least one folder by default. Users might then try to halt this sharing by clicking the “Deselect All” button. If so, this is what users will see:

Figure 18: BearShare 5.2.3.7

If the information reported conformed to BearShare's feedback rules, then Figure 18 would show that BearShare is not sharing *any* folder on the user's computer. But Figure 18 actually shows that BearShare violates its feedback rules: It is still sharing the downloads folder. In fact, clicking the "Deselect All" button during a default installation of BearShare has only one effect: It causes red checkbox outlines to turn grey. Nor will BearShare's internal share/unshared interface let users stop sharing the download folder: BearShare has a coerced-sharing feature.

Many programs also provide potentially misleading feedback about sharing of the download folder from within the program itself. For example, attempts to disable sharing from within Morpheus or BearShare can produce much the same misleading feedback as attempts to disable sharing during installation and setup.

BearShare will also inform users that they have stopped sharing *files* that they are still sharing. For example, Figure 19, below, shows the "Uploads" menu in a 2005 version of BearShare that is sharing 145 files from "My Downloads," a folder included in the user's "Library." In the upper right of the Uploads menu is a checkbox labeled "Share files from library." That box is checked by default. A user who wants to stop sharing downloaded files has now "unchecked" it, and BearShare has popped up a dialog box:

Figure 19: BearShare 4.7.0.76

In many programs, attempts to take certain actions will produce a dialog box that reminds the user that if they take action *X*, that will have effect *Y*, and then asks, "Would you like to continue?" Here, BearShare notes, "Only when users share files is it possible for everyone to find the files that they want to download. Please share." BearShare then asks, "Would you like to continue …. Sharing?"

So the user could only complete the action that she indicated that she wanted to take by selecting the counterintuitive answer "No." If she answers "Yes," she will continue sharing. And what happens if BearShare asks the user "Would you like to continue sharing?" and the user answers "No"?

The user will continue sharing. To be sure, the main interface will show that the user has "Unshared" all previously shared files, but if the user opens the Library view in BearShare and right-clicks upon individual files, she will learn that those "Unshared" files are actually still being shared.

eDonkey can also confuse. eDonkey does not provide any misleading feedback about the user's ability to disable redistribution during installation and setup because that process never discloses eDonkey's redistribution feature. Within the program itself, eDonkey lets users share and "unshare" various folders through a graphical share/unshared interface. In this interface, eDonkey identifies "shared" folders with a bright-green, checked circle that looks like this:

Figure 20

Using this information about the behavior of the eDonkey share/unshare interface, try to find the shared folder in the following screenshot:

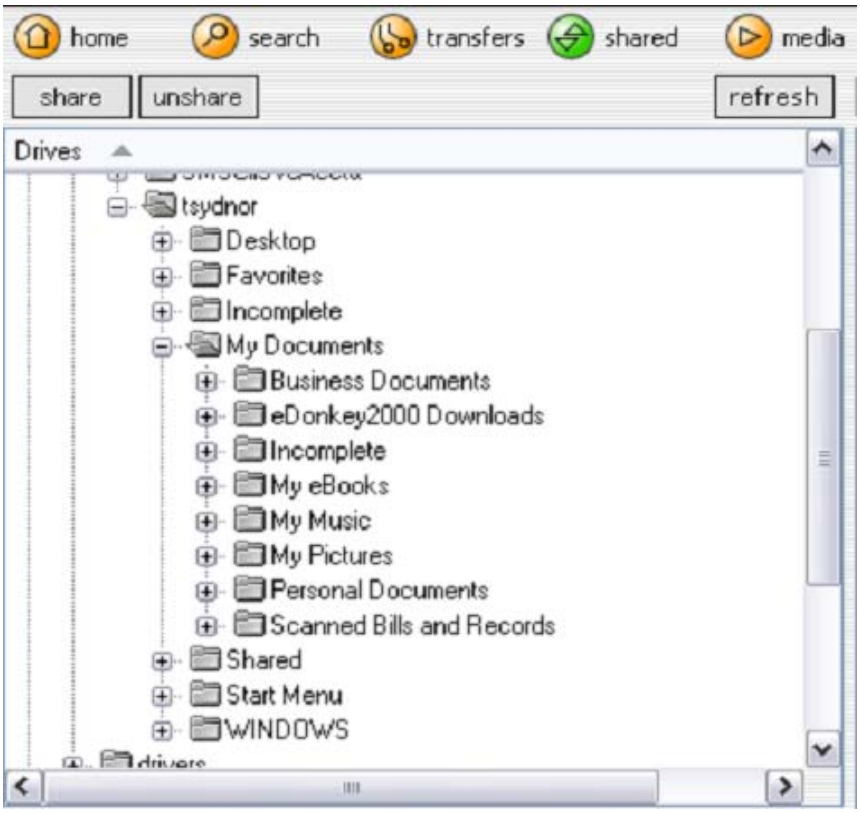

Figure 21: eDonkey 1.4.3

The task is challenging because the shared folder looks like it is not being shared. The shared folder is the default download folder, "eDonkey 2000 Downloads." It looks like a non-shared folder because the user tried to stop sharing this folder by selecting it and clicking the "unshare" button at the top of the graphic interface shown in Figure 21. The user's actions did make the checked green circle disappear, but eDonkey kept on sharing the download folder. Indeed, there is no obvious way for a user to disable sharing of the download folder in any eDonkey interface: eDonkey has a coerced-sharing feature.

This behavior might be the result of a bug that somehow remained undetected, for years. But, as shown below, the design of eDonkey itself may suggest otherwise:

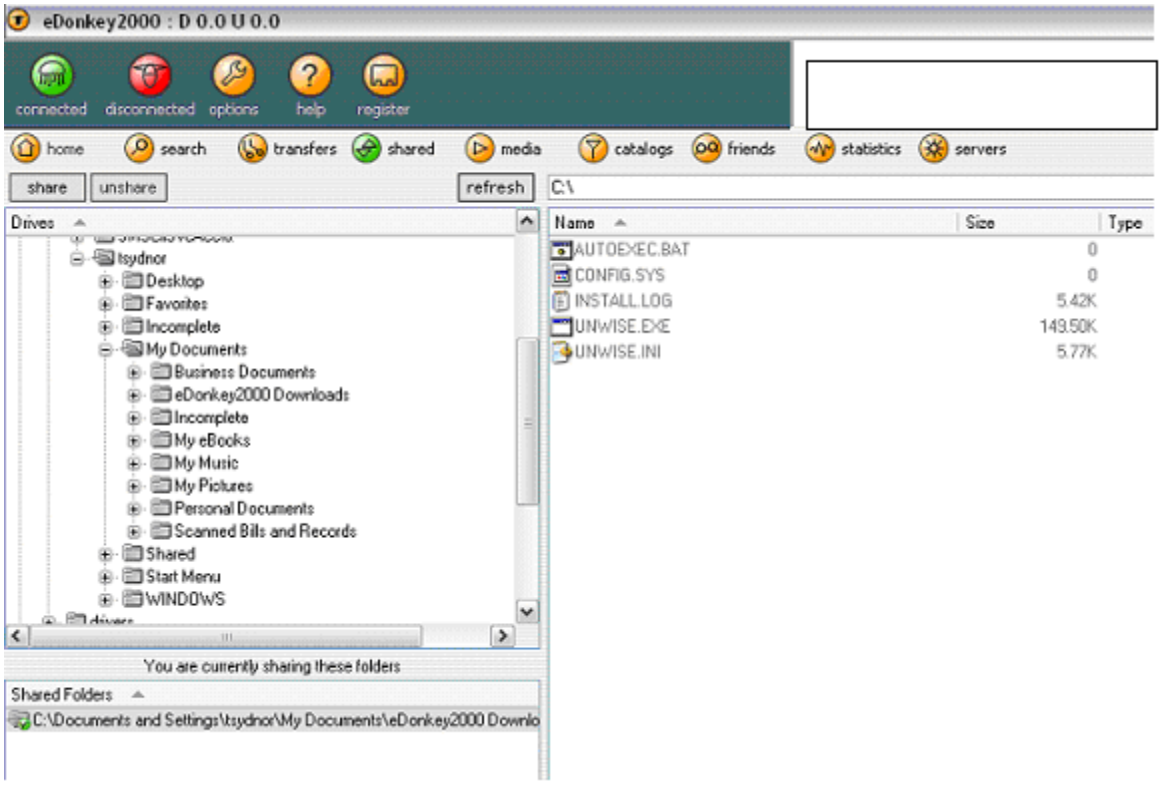

Figure 22: eDonkey 1.4.3

This screen shot shows a larger portion of the eDonkey screenshot shown in Figure 21. This larger view shows several things. Note that eDonkey actually has two share/unshare interfaces. The graphical share/unshared interface occupies most of the screen, but below it, there is a text-based share/unshare interface.

Here, these two interfaces provide conflicting accounts of whether the download folder is being shared: The large graphic interface says “no,” and the small, text-based interface says “yes.” But readers of this report know what the user would have to guess: The text-based interface is the one delivering accurate information. Indeed, if a user right-clicks the download folder in the text-based interface, an “unshare” button will appear, but it will be grayed-out and inactive, suggesting (incorrectly) that eDonkey will not let users disable sharing of the download folder. Nevertheless, the text-based interface shows that eDonkey can provide users with correct information about whether the download folder is shared.

And there is something else odd about the graphic interface. It is always updated instantly whenever a user shares or unshares a folder. If a user selects “My Documents” and clicks “share,” checked green circles appear. If a user selects the same folder and clicks “unshare,” checked green circles disappear. No matter which folder a user shares or unshares, the changes appear immediately and are implemented immediately. So why, in the upper right of the graphic interface, is there a button labeled “refresh”?

Usually, that “refresh” button is worse than useless: It does not affect the information displayed, but clicking it collapses the portion of the folder tree being viewed, so most

users probably learn not to click it. Indeed, analysis identified only one circumstance in which clicking the "refresh" button will affect the graphic interface.

If the user has selected the download folder and clicked "unshare," the folder will still be shared, but the green, checked circle that signals sharing will disappear, and it will not re-appear. But if a user has seemingly "unshared" the download folder, then clicking "refresh" will—after the user re-expands the collapsed folder tree—make the green circle reappear on the download folder, indicating that it is being shared.

So the behavior of the graphic interface may not be a bug: Someone who did understand its potentially misleading behavior may have worked hard to create this inconvenient, obscure Rube-Goldberg-like refresh-button to make the graphic interface report accurate information about the actual status of an "unshared" download folder.

Programs like Morpheus, BearShare, and eDonkey also reveal another problem that arises when distributors implement coerced-sharing features that thwart attempts to stop sharing the download folder: Such features can also thwart attempts to correct the effects of share-folder features. For example, Figure 14 shows a default installation of BearShare automatically sharing a user's "My Documents" folder because a previous installation of a prior version of the program had done so.

But another problem is less evident in this screenshot: Neither the "Downloads" nor the "Folders" menu in BearShare will halt this behavior. BearShare's "Downloads" sub-menu contains an undisclosed, librarying share-folder feature: It will *never* halt the sharing of *any* currently shared folder. Nor will BearShare's share/unshare interface let a user stop sharing the download folder or any of its subfolders. Users must figure out for themselves that they must (1) access the BearShare share/unshare interface by finding the tiny button labeled "Folders," on the "Library" view, (2) open the "Legends" submenu on the share/unshare interface to discover that solid red squares indicate that a folder is the download folder or a subfolder of the download folder, (3) exit from the share/unshare interface, (4) open the BearShare Setup menu; (5) open its "Downloads" submenu; (6) use the "Downloads" submenu to select a *different* folder to store downloads, (7) exit the BearShare setup menu, (8) re-open the BearShare share/unshare interface from the "Library" view, and (9) disable sharing of "My Documents" and its various subfolders.

Not all programs have made it difficult for users to stop sharing the download folder. For example, recent versions of LimeWire still let users disable sharing of the "Save Directory" using the same method that disabled sharing in previous versions. LimeWire also seems to have implemented some other useful changes. In version 4.9 and above, LimeWire improved—somewhat—its librarying, recursive-sharing share-folder feature.[71]

But when LimeWire 4.9 improved the share-folder feature, it also implemented a new "Individually-Shared-File" (ISF) feature. This ISF feature lets a user share a particular file *without* sharing the folder in which it is stored. The *LimeWire User Manual* describes ISF as a user-controlled, user-activated feature: "To share a file individually, right-click on a folder and select 'Share New File.'" The *Manual* thus portrays the ISF feature as one that gives users unprecedented control over their sharing.

But the *Manual* omits a key detail: By default, LimeWire itself will designate every file that a user downloads as an Individually Shared File. The ISF feature thus ensures that disabling sharing of the download *folder* no longer disables sharing of downloaded *files*. In versions of LimeWire after 4.8.1, users who want to stop sharing downloaded files must now disable sharing of the download folder, disable the ISF feature, and then disable the sharing of each downloaded file previously tagged by LimeWire as an ISF. In effect, ISF is a coerced-sharing feature that acts like a "backup" redistribution feature: In LimeWire 4.9 and above, users who once knew how to disable sharing of downloaded files at the folder level will now keep right on sharing….

In summary, four of the five programs studied here have deployed non-obvious, potentially misleading coerced-sharing features that can, however, be circumvented by sophisticated users who want to avoid the tedium and risk inherent in a copy-and-delete strategy. Such features appeared first in eDonkey and BearShare and were adopted later by Morpheus and LimeWire—during the period when the efficacy of redistribution, share-folder, and search-wizard features appears to have been waning. These coerced-sharing features also have another effect: They render useless—or worse—almost all of those detailed, program-specific, step-by-step, screenshot-illustrated instructions that once described how to disable sharing.

D. Next steps: Are search-wizard features poised to return?

While this report has focused on the behavior of five popular filesharing programs, it has revealed patterns of behaviors that change over time: Coerced-sharing features are popular today, but users will eventually discover what they do and how to disable them. As that happens, new "technological features" that can "induce users to share" may arise.

In late 2004, the authors of *Usability and Privacy* testified to the Federal Trade Commission about the problem of inadvertent sharing and criticized a less-well-known filesharing program, WarezP2P, for its aggressive search-wizard feature.[72] A more recent version of WarezP2P still contains an aggressive search-wizard feature. It is triggered automatically when the program is installed. It does not disclose that identified folders will be shared recursively. It will, like the BearShare wizard, share all folders it identifies unless the user acts affirmatively to prevent this. Nevertheless, the following screenshot of the WarezP2P search-wizard's results screen shows that it differs from previous wizards in one respect:

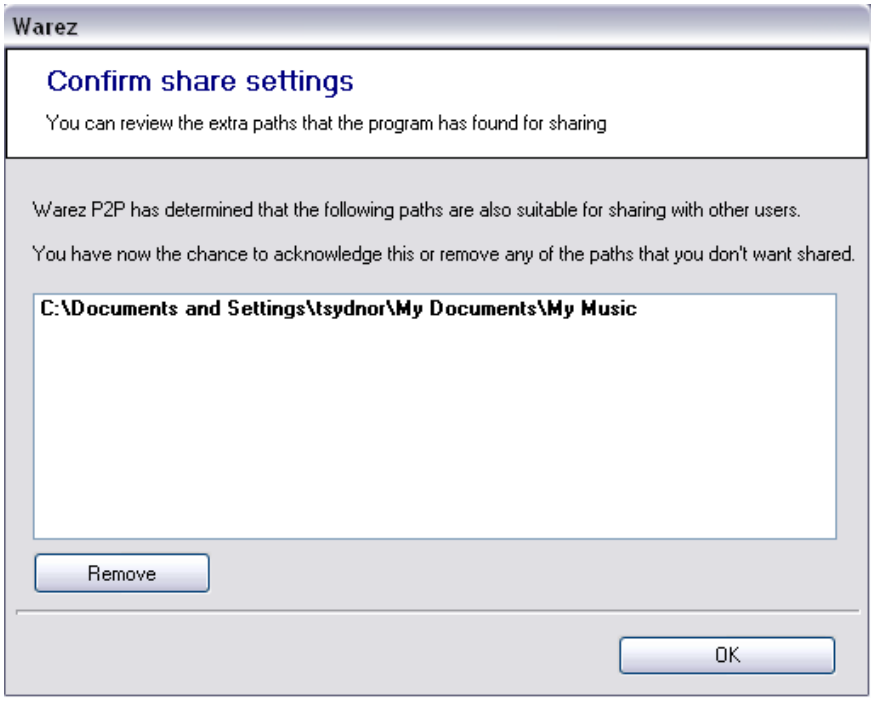

Figure 23: Warez P2P 2.9.5.3040

The WarezP2P wizard now appears to specifically target folders containing audio files: In the screenshot shown above, it has targeted for recursive sharing a "My Music" folder containing hundreds of copyrighted audio files. One long-time user of Gnutella-based filesharing programs has reported that such features are now common, apparently among the less-popular client programs: "Gnutella applications frequently share the 'My Music' directory on Windows computers by default…."[73]

Search-wizards that target folders containing specific types of media files might reduce these features' tendency to cause users to share existing *sensitive* files while preserving their tendency to cause users to upload existing *infringing* files. This sort of "targeted" search-wizard feature could become the next of the "technological features to induce users to share" to be widely deployed.

IV. **Conclusions and Implications.**

Public data on the behavior of filesharing programs reveals an array of "features" that could cause users to share files inadvertently. Some are obviously problematic: No wonder users upload files unintentionally if the interface that lets them select a folder to store downloaded files does not disclose that any folder selected will be shared, and shared recursively. Such circumstances make it relatively easy to answer the questions that this report seeks to address.

A. Conclusions.

This report seeks to answer two questions. First: Are there now, or have there been, features in popular filesharing programs that can cause users to share files unintentionally? Second: Do the totality of the circumstances suggest the need for further investigation to determine whether any particular distributor that deployed such a feature *intended* for it to dupe young or unsophisticated users into sharing files inadvertently?

The public data examined show that the answer to the first question is "Yes": There are now, and there have been, features in popular filesharing programs that can cause users to share files unintentionally. These programs have contained, and some still do contain, features that *could* act like duping schemes—like "technological features" that "induce users to share" infringing files unintentionally.

The public data examined also show that the answer to the second question is "Yes": The circumstances surrounding the behavior and deployment of "technological features" that can "induce users to share" infringing files unintentionally do justify further investigation to determine whether distributors *intended* for these features to dupe young or unsophisticated users into sharing files inadvertently.

Distributors have confronted new and unsophisticated users with an ever-changing array of redistribution, share-folder, search-wizard, partial-uninstall, and coerced-sharing features. These features were often implemented in ways that tended to obscure their effects. Some of these features have been implemented in ways that could confuse even experienced users; others in ways that are nearly inexplicable. Too often, implementations of these features became more aggressive after their potential effects on users were, or should have been, known to reasonable distributors of filesharing programs.

Such conduct suggests the possibility of duping. The available data on users' propensity to share files also suggests a potential motive: When sharing or uploading was a clearly voluntary behavior, few users chose to share files. Later, lawsuits against infringing users of filesharing programs appear to have decreased users' already-limited propensity to share files voluntarily. Under such circumstances, it may be impossible to base a successful filesharing network entirely upon "voluntary cooperation among users": Technological features that "induce users to share" files unintentionally may be indispensable.

The ugly history of share-folder and search-wizard features further suggests that duping or another form of inducement may be critical to a viable filesharing network. Absent some pressing need, it is difficult to imagine why distributors of filesharing programs would have continued or begun to deploy search-wizard or share-folder features after mid-2003. These features were deployed while the *Grokster* litigation and various legislative proposals on filesharing piracy focused increasing attention on the distributors of these programs. They were deployed while distributors were telling Congress and federal agencies that inadvertent sharing was a mere "urban myth." They were deployed

while some distributors repeatedly informed agencies and Congress that they were complying with the following self-imposed obligation:

> [Our] software and associated user instructions shall conspicuously require the user to confirm the folder(s) containing the file material that the user wishes to make available to other users before making such material available, and shall be designed to reasonably prevent the inadvertent designation of the contents of the user's entire hard drive (or other principal data repository) as material available to other users.

Indeed, these share-folder and search-wizard features were deployed even after the predicted compromises of personal, national, and military security occurred or recurred. Distributors could, in theory, possess data that would suggest that their actions were the result of mistake or neglect. But these distributors were also making repeated representations about how promptly and responsibly they had responded to the problem of inadvertent sharing of sensitive files. It would be surprising if they had consistently failed to correlate their rhetoric against the reality of how their programs worked. For example, it is possible that the authors of BearShare's *Important Word* and *Important Privacy Notice* simply did not know how their program actually operated. But if BearShare's distributors did know that they were misrepresenting how their program operated, then they probably had a good reason to do so.

For these reasons, further investigation by entities that could require complete disclosure of non-public information about the behavior and evolution of filesharing programs may be warranted. Such efforts could show definitively whether the distributors of programs that deployed the features discussed in this report intended for these features to act as duping schemes—as "technological features to induce users to share."

Definitive answers to questions about the intent underlying the actions of distributors of particular filesharing programs might clarify whether particular distributors would be subject to civil inducement liability under *Grokster*. They would also have broader significance.

For example, a showing that features in filesharing programs were (or were not) intended to dupe users into sharing files unintentionally would show whether user education could resolve the problem of inadvertent filesharing. Granted, user education might be ineffective even if such features were mere errors in interface design: Consumers Union once warned that "[t]here may be no educating around a design flaw."[74]

But there can be *no* "educating around" a duping scheme: As users become "educated" about a scheme, the scheme should evolve and turn users' "education" against them. If the "features" discussed in this report were deployed as duping schemes, then for users of filesharing programs, only one thing is certain: There is worse yet to come.

Answers to questions about duping could also clarify the validity of claims that the networks created by filesharing programs show that properly designed code can inspire large groups of people to cooperate even when it would be irrational for any individual

member of the group to do so: Some even suggest that filesharing reflects the emergence of a fundamental change in human nature—the evolution of *Homo swappus*.

But this view of filesharing presumes that users share intentionally: "The fundamental premise of peer-to-peer systems is that individual peers voluntarily contribute resources to the system."[75] As Professor Wu has noted, those who advocate this view of filesharing might see the cartoon-bear mascot of BearShare as a fitting symbol of their cause:

> "There is little on the screen to suggest that a user is engaging in a morally ambiguous operation or is committing an act of theft. The friendly bear in BearShare is an icon of charismatic code."

Figure 24: "The Friendly Face of the BearShare Community"[76]

But the friendly face of this cartoon bear once concealed some ugly code. In some 4-series versions of BearShare, that smiling bear deployed an increasingly less-obvious redistribution feature, an undisclosed, librarying, recursive-sharing share-folder feature, an aggressive search-wizard feature, a potentially dangerous partial-uninstall feature, and a potentially misleading coerced-sharing feature that sophisticated users can avoid. These features may have been deployed to trick the young and the unwary into uploading infringing files that culpable, revenue-generating leechers could download with little risk to themselves.

If so, then BearShare would hardly reflect a step forward in human evolution. To the contrary, it would seem to reflect a regression to the law of the jungle—a return to a system that preys upon the young and the naive.

Until questions about duping are resolved, potential users of 4-and-5-series versions of BearShare should beware the smiling "icon of charismatic code": In these versions, that happy little cartoon bear has teeth. And he will bite.

B. Implications.

This report does not purport to draw conclusions about whether any given distributor of a particular filesharing program *intended* to deploy "technological features" in order to "induce users to share" files inadvertently. Nevertheless, for some groups of persons, significant implications follow from the conclusions drawn regardless of whether or how questions about any individual distributor's intent are ultimately resolved.

Government and Corporate IT-Security Managers: For anyone concerned about protecting the security of sensitive data or the security of computer networks, questions about whether features that can cause users to share files unintentionally were *intended* to

do so are largely irrelevant. In either case—and as DHS has acknowledged—filesharing programs present a tripartite threat to the security of data and networks.

- Filesharing programs can cause inadvertent sharing that can compromise entire networks: In networked environments, the effects of the "features" discussed above can be particularly devastating. For example, on some networks, a user who tries to store downloaded files in a folder like "Documents and Settings" can end up "sharing" all files created by all users of the network. Even home use of filesharing programs can compromise government or corporate networks: *Usability and Privacy* notes that if a home computer has a VPN connection to a corporate or governmental network, a user can inadvertently "share" the portion of the network available through the VPN connection.

- Filesharing programs can infect computers or networks with malicious code: To avoid vicarious liability for pervasive infringing uses of their programs, distributors of filesharing programs stopped registering or uniquely identifying individual users of their programs. Distributors knew that this would encourage distributors of malicious code to use popular downloads as a means to compromise computers and networks: "*As you would expect*, when files often come from anonymous and uncertified sources, the risk of that file containing a virus greatly increases."[77] As a result, research by the security company TruSecure found that 45% of popular downloaded files concealed malicious code.[78]

- Filesharing programs can contain vulnerabilities that hackers can exploit to steal sensitive data: DHS warns that filesharing programs "can result in network intrusions and the theft of sensitive data.… [F]ederal government organizations have discovered the presence of P2P software on compromised systems while investigating cyber intrusions." McGill University warns that some filesharing programs are developed by "ragtag teams following ad hoc plans, resulting in barely functional, extremely buggy clients that are prone to security breaches."[79]

All three of these risks increase because filesharing programs—unlike most others—often appear to be designed to go where they are not wanted and to evade the security measures that could exclude them. As one security expert warns, "Many of the finest computer minds in the world are continuously working to make the P2P programs evade the best detection schemes available."[80]

There will almost never be a legitimate business or governmental justification for employee use of filesharing programs. Nevertheless, preventing employees from using these programs on corporate or government networks can be both difficult and expensive.[81]

Owners of Home Computers: People who store any type of sensitive data on their home computers—particularly computers to which children, teenagers, or college students might have access—confront circumstances similar to those faced by

governmental or corporate IT managers. Unfortunately, owners of home computers face two additional challenges.

First, owners of home computers will almost always lack the resources available to governmental or corporate IT managers. Second, home computers are often used by multiple persons, and the person who best understands which files are sensitive and where they are stored may not be the person who installs and runs a filesharing program. Indeed, whenever employees do work at home, government or corporate IT managers may find that these complications affect their interests as well.

The critical challenge will be assessing the options available to owners of home computers (or persons who contract with Internet-access providers) who want to prevent filesharing programs from being installed or used on their computers and networks. While software firewalls or routers can be configured so that only one person can grant Internet access to a program, this solution may prove impractical for most roommates or families. The Federal Trade Commission has done some initial investigation into other filesharing-detection-or-prevention options available to owners of home computers. Further research and reporting by consumer-protection advocates might be useful.

Users of Filesharing Programs: For users of filesharing programs, it is, again, largely irrelevant whether particular features in those programs were intended to—or simply can—cause some users to share infringing files inadvertently. In either case, many of the same implications follow.

The research on uploading rates among users of filesharing programs suggests that users' propensity to share files is affected, but not dictated, by the design of filesharing programs. The more than 100% increase in sharing reported between 2000 and 2001 strongly suggests that program design can significantly affect users' propensity to upload files. But the 500% plunge in sharing rates—to 15% of the user population— by 2004 strongly suggests that users can, over time, overcome the effects of design. But the rise of coerced-sharing features suggests that as users overcome the effects of design, users' past experiences can be turned against them.

This suggests that users are neither unaffected nor enslaved by the design of filesharing programs. This may refute claims that distributors of filesharing programs do not "facilitate the exchange of files between users" or that users alone "select which files to share."[82] But it also seems to refute Professor Lessig's claim that a "fundamental principle of bovinity" ensures that "it is as likely that the majority of people would resist [imperfect controls imposed through code] as it is that cows would resist wire fences."[83] His "bovine account" of human nature asserts that most people are no more than witless cows. But, given time, information, and incentives, most users did resist some of the "technological barriers" to disabling sharing that filesharing programs tended to create.

Unfortunately, while users of filesharing programs may have proven to be, over time, more competent—more human—than some thought, for users, the implications of features in filesharing programs that can cause users to share files inadvertently are almost universally bad.

First, until distributors of filesharing programs eliminate all features in their programs that can cause users to share files unintentionally—and stop adding new ones—filesharing programs will be dangerous, use-at-your-own-risk propositions. While this report identifies some potential problems, the precautions taken to avoid confusing imperfect interface design with duping ensure that this report does not purport to identify all features in filesharing programs that could cause users to share files unintentionally: It is not a guide to "safe sharing."

Second, for now, users of filesharing programs who want to avoid inadvertent sharing are on their own. As *Usability and Privacy* noted, filesharing programs themselves often do a "poor job" of helping users avoid inadvertent sharing. The users' guides and manuals for these programs are also often unhelpful, and some could be affirmatively misleading. Nor can users rely on the informal user forums associated with most programs: Posting questions on these forums about halting or restricting sharing may produce hostile "flame" responses, but little useful guidance. While users can search the Internet for instructions on disabling sharing in various programs, most are now dated, and some are inaccurate. Again, consumer-protection or public-interest advocates might assist by providing a regularly updated online guide to halting sharing in the more popular programs. Unfortunately, some technical analysis would be needed to confirm that features that seem to let users halt sharing actually do so.

Third, users should assume that they can be held liable for infringing use of filesharing programs *even if* they share or upload infringing files unintentionally and *even if* they do as a result of features that were intended to dupe users. Direct liability for copyright infringement is a form of strict liability.[84] And many users who upload copyright-protected files inadvertently may do so negligently or recklessly: The features discussed above do not *force* users to share infringing files, and do they do not cause sharing that cannot be detected and corrected by a very alert, well-informed user.

Moreover, while duping might cause high-volume uploading that triggers a copyright-enforcement lawsuit against a particular user, discovery will probably reveal other, more intentional, forms of infringement. As one commenter notes, "Virtually everyone who participates in one of the file-swapping networks is breaking the law in the process."[85] So regardless of whether a given user bears some measure of personal culpability for the sort of high-volume uploading of infringing files that can trigger an enforcement lawsuit, that user has probably also engaged in infringement not caused by duping. For example, *uploading* may have led rightsholders to sue one particular user of a filesharing program, but the courts ultimately held her liable for *downloading* infringing files.[86]

Fourth, users should not expect rightsholders or courts to sympathize whenever a user claims that he or she was duped into becoming a high-volume uploader of infringing files. Duping schemes—or features that simply act like duping schemes—are dangerous because they make it difficult to distinguish those who acted unintentionally from culpable wrongdoers who planned to "cry duping" if they were caught. For example, a culpable user of BearShare might use its share-folder feature to store downloaded files in "My Music" folder so he could, if caught, claim that he did not know that BearShare was

recursively sharing all of the subfolders of "My Music" that stored thousands of audio files copied from lawfully purchased CDs.

Fifth, users should recognize that the factors outlined above do not mean that users who have shared files unintentionally lack any form of legal redress. For example, one court adjudicating a lawsuit brought against a user of a filesharing program who claimed that she shared any allegedly infringing files inadvertently has noted that she could bring a state-law contribution or indemnity claim against the distributor of the filesharing program at issue.[87] State consumer-protection laws may provide another means of redress.

Finally, some defenders of filesharing may argue that the prevalence of "technological features" that can "induce users to share" infringing files makes it unfair for copyright holders to sue users of filesharing programs for infringement. They may thus argue that if distributors of filesharing programs have both encouraged users to infringe copyrights voluntarily *and* duped them into doing so involuntarily, then those distributors should be given them what they always wanted: A collective or compulsory license to distribute the copyrighted works targeted by their schemes. One could scarcely conceive of a better means to encourage future copyright piracy, fraud, and duping schemes.

Distributors of filesharing programs: Distributors of filesharing programs may also find that they should eliminate or fully disclose any features that could cause new or unsophisticated users of their programs to share files unintentionally—and do so regardless of whether or how questions about the intent underlying such features are resolved.

Many distributors of filesharing programs have claimed that they want copyright enforcement to "leave the little guys alone"—to avoid targeting the young and unsophisticated users of filesharing programs who seem to be prevalent among the high-volume uploaders of infringing files. The data analyzed above strongly suggests that distributors of filesharing programs could make this aspiration a reality: If children and unsophisticated users shared hundreds of infringing files only when they clearly intended to do so, most would likely choose not to do so. The conclusion that *Usability and Privacy* drew in 2002 remains valid today: Eliminating features that can cause inadvertent sharing, *and halting any continuing effects of previously deployed features,* should be a "top priority" for responsible distributors of filesharing programs.

Raw self-interest on the part of distributors may also dictate such a course. The intentional-inducement doctrine recognized in *Grokster* is unusual: Most civil laws impose liability for wrongful conduct without a showing of intent. This is true for most forms of direct or secondary liability for copyright infringement. It is also true for other forms of civil liability that could be triggered by "technological features" that "induce users to share" files inadvertently.

For example, the distributor of a filesharing program that contains features that do cause users to share infringing files unintentionally could face direct or secondary liability for the resulting infringements absent any showing of intent. Direct liability for copyright

infringement is joint and several: When an infringement occurs as the result of consecutive wrongful acts by two parties, each is held fully liable. An infringing upload might occur only because (1) a distributor released a program that contained a not-so-obvious redistribution feature, and (2) a user unaware of that feature intentionally downloaded an infringing file. In such a case, an infringing upload results from the combined effects of consecutive wrongful acts by the distributor and user of the program.

A similar result might follow under secondary-liability doctrines. If a program deploys a feature that its distributor knew or should have known would cause some users to upload infringing files inadvertently, then vicarious liability may attach: Such a distributor would have had the right and ability to control—indeed, to prevent—the infringing acts that the feature subsequently caused.

Nor is civil liability for copyright infringement the only form of civil liability that might confront the distributor of a filesharing program containing "features" that cause users to share files unintentionally. Regardless of whether a file shared inadvertently is infringing or a sensitive personal file, the affected consumer incurs a significant risk of harm. Civil consumer-protection and tort laws impose forms of strict liability against distributors of products—particularly if those products become, in effect, dangerous toys often used by children. Indeed, as noted above, at least one court has already noted that a user of a filesharing program who shares files inadvertently may have a cause of action for contribution against the distributor of the program.

All of these factors suggest that any more attempts to deploy "technological features" that can "induce users to share" infringing files should be viewed with great skepticism. Six years ago, *Free Riding on Gnutella* questioned whether a viable filesharing network could be based upon "voluntary cooperation between users." The public data analyzed here suggest that the events of the last six years may not answer this question. The events of the next few years probably will.

APPENDIXES

Appendix A: The Scope of This Report

The scope of this report must accommodate both the scope of USPTO's investigatory authority, and the limitations of its investigatory powers. USPTO has an obligation to "advise Federal departments and agencies on matters of intellectual property policy in the United States and intellectual property protection in other countries." 35 U.S.C. § 2(b)(9). It may also "conduct … studies … regarding … the effectiveness of intellectual property protection domestically and throughout the world." *Id.* at § 2(b)(10). Consequently, USPTO can and should investigate whether duping schemes cause unnecessary conflicts between consumers and rightsholders and whether such schemes threaten the security of sensitive or classified government data.

Nevertheless, USPTO is not a specialized investigatory or law-enforcement agency. USPTO does not have relevant legal authority to compel private parties to fully disclose all relevant information in their possession, custody, or control. Distributors of filesharing programs probably possess private data relevant to questions about whether they intended to dupe users into sharing files inadvertently. But USPTO cannot require them to disclose that information; nor can it ensure that any voluntary disclosures of such data are accurate or complete. As a practical matter, these limitations indicate that this report should pursue one of two alternative courses of analysis.

On the one hand, this report could consider only public information or data. Public data can reveal much about the uploading related functions of filesharing programs and how they changed over time. But this approach has a disadvantage: Confining this investigation to publicly available data means that it could not fairly draw conclusions about whether the distributor of a particular filesharing program intended to dupe users of the program into uploading files unintentionally. Duping, like inducement generally, requires a showing of intent. Public data may provide strong evidence of intent: For example, data showing that a distributor of a filesharing program deployed features that a reasonable distributor would have known would cause users to share files unintentionally could permit a reasonable person to infer that this distributor intended to cause inadvertent sharing. Nevertheless, even in such a case, the distributor deploying such a feature might possess nonpublic data suggesting that it deployed such a feature mistakenly, negligently or recklessly.

On the other hand, this report could seek to supplement public data with whatever nonpublic data distributors of the filesharing programs in question might choose to disclose voluntarily. This approach also has a disadvantage. It would be unlikely to reveal any presently nonpublic data indicative of duping: No entity should voluntarily disclose such data. Nor is this concern merely hypothetical: Distributors of filesharing programs have repeatedly disclosed some information about how the sharing-related functions of their programs should or do work to both committees of Congress and administrative agencies. Comparing the content of those representations against the actual behavior of distributors' programs counsels against a repetition of such efforts.

Consequently, this report will consider only public data or information about the sharing related functions of five popular search-and-download filesharing programs. It will thus attempt to answer two questions.

- First, have distributors of these filesharing programs deployed features that could cause users to share infringing files inadvertently—features that could act like duping schemes?

- Second, could the circumstances surrounding the deployment of any such features warrant further investigation into whether those features were intended to dupe users into sharing infringing files inadvertently?

Neither of these questions can be answered simply by determining whether filesharing programs have deployed, or do deploy, features that could cause users to share files inadvertently. Software-interface design is *not* a mature science: At present, users, software, and hardware can interact in ways that software designers and distributors *do not* intend, and, indeed, would rather avoid.

This creates a risk of "false positives": A program could contain a feature that causes users to share files unintentionally *even though* the program's distributors did not intend for it to do so. For example, reports indicate that for nearly a year, bugs in the LimeWire program allowed remote parties to access and download *any* file stored on a computer running LimeWire—regardless of whether that file was stored in a folder being "shared" by the program.[88] This was—and is—a serious security vulnerability that could cause users to unknowingly make files available to others. Nevertheless, no public data suggests that this flaw was intended to cause users of LimeWire to share files inadvertently.

To reduce this potential risk of "false positives"—the risk that flawed interface design could be mistaken for potential duping—this report adopts five precautionary measures. Consequently, it will discuss a particular feature in a particular program only if it meets the following criteria:

- First, the feature must have been *widely deployed.* It must be, or have been, present in multiple filesharing programs.

- Second, the feature must have been widely deployed in *popular* filesharing programs. Scores of filesharing programs exist, so it would not be surprising if a few, marginal programs were irresponsibly designed.

- Third, the feature must have been widely deployed in popular filesharing programs *after* its propensity to cause users to share files inadvertently was, or should have been, known to responsible, informed distributors of filesharing programs. Published research and reports, the representations of distributors of filesharing programs, and violations of the *Code of Conduct* drafted by the distributors of BearShare, eDonkey, LimeWire, and Morpheus could indicate

actual or constructive knowledge of a particular feature's propensity to cause inadvertent sharing.

- Fourth, further protection against false positives can be provided by analyzing how a feature evolved over time: Very different implications might follow if implementations of a feature that had been shown to cause inadvertent sharing become more or less misleading over time. The former case might more strongly suggest possible duping.

- Fifth, a feature that causes inadvertent sharing in a particular type of program could have different effects in a program that had a different architecture. This report will thus focus only on those filesharing programs that provide users with search, uploading, and downloading capabilities functionally similar to those once provided by the filesharing program distributed by Napster, Inc.[89] It will not discuss popular BitTorrent clients because of their significantly different architecture and functionality.

These precautions limit the potential for confusing error with possible duping, but at a cost: They ensure that this report does not purport to identify *all* features in the studied programs that could cause users to share files inadvertently: For example, idiosyncratic or previously unknown features will not be covered. Unfortunately, the research conducted for this report suggests that such features may exist, at least in some programs.

The answers to the two questions raised in this report were obtained by studying the uploading-related features of past and present versions of the programs examined. Versions of the programs examined were obtained, usually from the various websites that provide past and present versions of filesharing programs for downloading. Each program was then installed and operated on test computers that stored various .doc, .pdf, .mp3, .wma, and jpg. files in various subfolders of the "My Documents" folder. Screenshots of relevant behaviors were taken. The program was then uninstalled from the test computer, and the configuration files left behind were deleted. When possible, experiments to confirm the behavior of particular versions of particular programs were conducted repeatedly to ensure that the behavior in question could be replicated.

Information about the sharing-related behavior of users of filesharing programs was obtained from published studies that collected relevant data. Computer-science researchers rely routinely on the results of these studies, and they provide a rare neutral source of systematically collected data on filesharing behavior. Nevertheless, they do not permit fine-grained analysis of users' sharing behavior or how it changed over time.[90]

Information was also obtained from searches of various filesharing networks conducted to determine whether users were still inadvertently sharing sensitive personal files. These searches were done to determine whether inadvertent sharing of sensitive files continued to be a problem in late 2005 and early 2006: They were not an attempt to systematically analyze or quantify the problem of inadvertent sharing. Their results suggest that the problem of inadvertent sharing of sensitive files continues and that it is more prevalent on the Gnutella filesharing network.

Finally, the decision not to draw conclusions about the intent of any particular distributor of a given filesharing program is a conservative precaution. The ultimate goal of this report is to determine whether existing public data could warrant further investigation into the issue of intent: It thus reserves conclusions about the intent of particular distributors to those entities authorized to compel the truthful and complete disclosure of all relevant nonpublic information possessed or controlled by those distributors.

Appendix B: Terms used in this report

The intersection of copyright law and filesharing programs has spawned an array of acronyms, neologisms, and poorly defined terms. This report cannot avoid contributing to the growth of filesharing-related acronyms and neologisms, but it will try to avoid the use of poorly defined terms.

Default settings, behavior, or installation: This report will sometimes refer to the "default" settings or behavior of the programs discussed. These references have an unusually narrow meaning: They refer to the way that a program would behave were it installed on a computer on which no filesharing program had been previously installed. The report also refers to a user performing a "default installation" of a program: This means that the user simply clicks "Next" or "OK" during each step in a program's installation-and-setup process. The report's discussion of partial-uninstall features explains in more detail why default installations of the same program on different computers can "share" very different sets of files and folders.

Distributors of filesharing programs: As used here, the term "distributors" does not encompass all persons or entities involved in the distribution of filesharing programs. Rather, it is a convenient way to refer more narrowly to the natural or legal persons that develop or make available to the public a particular filesharing program. For example, as the term is used here, Metamachines, Inc. is a distributor of eDonkey; Streamcast Networks, Inc. is a distributor of Morpheus; Free Peers, Inc. is a distributor of BearShare;[91] LimeWire, LLC is a distributor of LimeWire; and Sharman Networks, Ltd. is a distributor of the KaZaA Media Desktop.

The term "distributors of filesharing programs" does *not* encompass all entities that play some role in the distribution of filesharing programs. For example, it does not include entities that merely link to, host, or transmit over their own network copies of filesharing programs made available by third parties. It also excludes the individual users of a program who make copies of that program available for downloading by other users, or potential users, of the program in question.

Downloaded files: This phrase refers to files that are stored on a computer running a filesharing program after those files were downloaded from a filesharing network.

Download folder: This phrase refers to the folder on a computer running a filesharing program that will store copies of newly downloaded files.

Filesharing Programs: A filesharing network consists of two basic components—a protocol and client programs that use the protocol to communicate: For example,

LimeWire is a filesharing program that uses the Gnutella protocol. As used here, the phrase "filesharing program" may occasionally refer to those filesharing programs that provide users with uploading, search, and downloading capabilities similar to those once provided by the filesharing program distributed by Napster, Inc: As the *Grokster* courts put it, the phrase refers to those programs that "operate in a manner conceptually analogous to the Napster system…" or to a program that "functions as Napster did, except that it could be used to distribute more kinds of files, including copyrighted movies and software programs." Usually, this phrase refers more specifically to the particular examples of such programs analyzed in this report. Those programs are Bearshare, eDonkey, KaZaA, LimeWire, and Morpheus.

Calling these programs "filesharing programs" may offend parties on both sides of the debate about filesharing. Opponents of filesharing may object that this term obscures the fact that these programs and networks are actually "file-copying" and "file-distribution" systems: Users of these programs may "share" resources like bandwidth, but they do not "share" files in the way that the owner of a CD might share it by loaning it to a friend. The objection has merit, but the term "filesharing program" is widely used, and inventing another name for these programs and networks might cause more confusion than it would eliminate.

On the other hand, proponents of filesharing may object that the programs discussed here create "decentralized," "peer-to-peer" filesharing networks that may have unique advantages. Again, the objection has some merit, but on balance, it should be overlooked. The term "decentralized" has no clear meaning, and whatever meaning it does have appears to be more legal than technical.[92] The term "peer-to-peer" may also be inappropriate: Reportedly, when the programs discussed here are operating in the default manner preferred by their distributors, a user can search for, locate, and download a file without interacting with another "peer" user or a computer owned by such a user.[93] While the term "peer-to-peer" has always been ambiguous, programs and networks that rely, by default, upon specialized search-index servers and dedicated, high-speed, terabyte-sized fileservers to store and transfer requested files may not be "peer-to-peer" in any meaningful sense.

Inadvertent sharing: This phrase refers generally to situations in which individual users of filesharing programs have uploaded or "shared" particular files unintentionally. Inadvertent or unintentional sharing of infringing files is not synonymous with innocent or blameless sharing of such files: A user who did not *intend* to share infringing files may still have done so knowingly, recklessly, or negligently. For example, distributors of filesharing programs might well argue that because almost all such programs contain redistribution features that will cause users to share downloaded files by default, users who failed to educate themselves about a particular program's redistribution feature were negligent or reckless.

In general, reports of inadvertent sharing tend to involve users sharing one of two types of files unintentionally. Some reports involve users inadvertently sharing *downloaded* files—files that a user had downloaded from a filesharing network using the filesharing program in question. Other reports concern users inadvertently sharing *existing* files—

files that had not been downloaded with a filesharing program, but were being stored on a computer running a filesharing program. Inadvertent sharing of either type of file could cause users to share *infringing* files inadvertently.

Infringing file: This term is a convenient way to refer to a file that contains or encodes a copyright-protected work that has been uploaded to or downloaded from a filesharing network without the authorization of the copyright owner. Its use is not intended to deny that there could be rare cases in which unauthorized uploading or downloading might be found not to infringe the exclusive rights of the holder of the copyrights in a work encoded in a given file.

ENDNOTES

[1] John Borland, *Covering tracks: New privacy hope for P2P*, CNET NEWS.COM, Feb. 24, 2004 http://news.com.com/2100-1027-5164413.html); *see also* Press Release, Optisoft S.L., P2P Downloaders Go Anonymous with Blubster 2.5 (June 30, 2003) (announcing "the launch of Blubster 2.5 in the wake of the latest litigious effort by the RIAA and MPAA…. Version 2.5 … disassociate[s] file transfers from specific users"), *available at* http://www.tinfoil.net/modules.php?name=News&file=article&sid=703; *New wave of secret file sharing breaks over Web*, THE INQUIRER, May 10, 2004 ("A spokesperson for Optisoft said that … the RIAA would be forced to do a mass action against every user in the network, and would be unable to identify each person's liability."), http://www.theinquirer.net/default.aspx?article=15808.

[2] *United States v. Gooding*, 25 U.S. 460, 469 (1827) (Story, J.); *see also, e.g.*, *United States v. Giles*, 300 U.S. 41, 49 (1937) (holding the defendant liable for causing an "innocent intermediary" to make false entries in the accounts of a bank); *U.S. v. Bryan*, 483 F.2d 88 (3d Cir. 1973) ("A crime may be performed through an innocent dupe, with the essential element of criminal intent residing in another person."); Baruch Weiss, *What Were They Thinking: The Mental States of the Aider and Abettor and the Causer under Federal Law*, 70 FORD. L. REV. 1341, 1354 (2002) (using the term "causer" to distinguish an abettor who has an illegal act performed by "an innocent dupe").

[3] *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 2006 U.S. Dist. LEXIS 73714 (C.D. Cal. Sept. 27, 2006).

[4] Krishna Gummadi et al., *Measurement, Modeling, and Analysis of a Peer-to-Peer File-Sharing Workload*, PROC. 19TH SYMP. ON OPERATING SYSTEM PRINCIPLES (Oct. 2003) (showing that the volume of data requested by a given KaZaA client declines sharply after its first week of existence and decreases steadily thereafter and concluding that "new clients generate most of the load in Kazaa"); *cf.* Stephan Sariou et al., *An Analysis of Internet Content Delivery Systems*, PROC. 5TH INT'L SYMP. ON OPERATING SYSTEM DESIGN AND IMPLEMENTATION (2002) ("[A] very small number of Kazaa clients have a huge overall bandwidth impact.").

[5] Chad Silver, *Censure the Tree for Its Rotten Apple: Attributing Liability to Parents for the Copyright Infringement of Their Minor Children*, 3 CARDOZO PUB. L. POL'Y & ETHICS J. 977, 978 & n.6 (2006) ("According to 'some estimates, teenagers make up half of the of the … people who use [online] file-swapping services' to illegally trade music.") (citation omitted); PEW INTERNET & AMERICAN LIFE PROJECT, TEEN CONTENT CREATORS AND CONSUMERS iii, 10 (2005) ("51% of online teens say they download music files"); PEW INTERNET & AMERICAN LIFE PROJECT, THE MUSIC DOWNLOADING DELUGE 2 (2001) ("53% of youth between the ages of 12 and 17 have also downloaded music files"); see also Jane Musgrave, *Music Downloads Hit Sour Note for Sued Ordinary Folks*, PALM BEACH POST, June 26, 2006, at 1A ("Not surprisingly, many of the [RIAA] lawsuits are against parents who say they had no idea their teenage children were downloading music illegally."); Memorandum from the Electronic Frontier Foundation to Defense counsel in RIAA and MPAA individual file sharing suits, *Parental Liability for Copyright Infringement by Minor Children* (Nov. 1, 2005) ("In many of these instances, suit has been brought against either a minor child or her parents based on the allegedly infringing activities of the child…."), http://www.eff.org/IP/P2P/Parent_Liability_Nov_2005.pdf.

[6] *See* Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 685 (2003); Jane C. Ginsburg, *Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace*, 95 COLUM. L. REV. 1466, 1488 (1995); *see also* 17 U.S.C. at § 512(b)-(d) (creating limitations on the potential liability of internet-service-providers who, *inter alia*, comply with an expeditious notice-and-takedown process that minimizes the need for copyright enforcement against end-users).

[7] FRED VON LOHMANN, ELECTRONIC FRONTIER FOUNDATION, IAAL: PEER-TO-PEER FILE SHARING AND COPYRIGHT LAW AFTER NAPSTER (2006), http://www.eff.org/IP/P2P/p2p_copyright_wp_v5.pdf. *See*

also, Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 731 (2003) ("The design [of Gnutella] was an intentional effort to create a filesharing protocol that could avoid a lawsuit."); *id.* at 735 ("KaZaA … maintains no power to 'shut down' the network.").

[8] ELECTRONIC FRONTIER FOUNDATION, RIAA V. THE PEOPLE: TWO YEARS LATER 2, 6-7 (2005), http://www.eff.org/IP/P2P/RIAAatTWO_FINAL.pdf. Previously, EFF had argued that RIAA's *failure* to sue individual uploaders of infringing files proved that RIAA's lawsuits against distributors of filesharing programs were intended to control technology rather than to deter copyright piracy. *See, e.g.*, Declan McCullough, *End of an Era for File-Sharing Chic?*, CNET NEWS.COM, Aug. 25, 2003 (reporting that EFF had argued "that P2P users 'are the ones who are the alleged pirates. If this fight were really about stopping piracy, you would have expected some pirate to actually be sued.'"), http://news.com.com/2010-1071_3-5067473.html.

[9] Bruce Byfield, *RIAA conducting "reign of terror," lawyer says*, NEWSFORGE, July 20, 2006, http://trends.newsforge.com/article.pl?sid=06/07/20/1651223.

[10] P2P United, Peer-to-Peer Trade Group to RIAA Bullies: Come Out and Fight Us If You Want, But Leave the Little Guys Alone!!! (Sept. 10, 2003), http://www.bearshare.com/press/riaabullies.htm.

[11] While this report was being prepared, Free Peers, Inc., the distributor of the 4-and-5-series versions of BearShare analyzed in this report, reportedly settled litigation brought by copyright holders and sold the rights to BearShare to another entity that has, or may, re-launch BearShare as an licensed filesharing service. This report has not analyzed any "re-launched" versions of BearShare; its conclusions about potentially problematic sharing-related features in older versions of BearShare do not imply that such features would continue to exist or would have similar effects upon users of a licensed filesharing service.

[12] *See, e.g.*, Nicolas Christin et al., *Content Availability, Pollution and Poisoning in File Sharing Peer-to-Peer Networks*, PROC. OF THE 6TH ACM CONF. ON ELECTRONIC COM, 70 (2005) ("in both FastTrack and Gnutella, leaf nodes are promoted to hubs by the software client, and generally unbeknownst to the user"); *cf.* Krishna Gummadi et al., *Measurement, Modeling, and Analysis of a Peer-to-Peer File-Sharing Workload*, n.3, PROC. 19TH SYMP. ON OPERATING SYSTEM PRINCIPLES (Oct. 2003) ("P2P software is often designed to make it difficult to close the program once it starts, 'fooling' users into making their clients more available than they intended.").

[13] Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505, 549-50 (May 2003); *cf.* Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 724 (2003) (arguing that the design of filesharing programs "brilliantly" exploits ambiguities about "whether home, non-commercial copying is 'wrong'").

[14] Eytan Adar & Bernardo A. Huberman, *Free Riding on Gnutella*, 5 FIRST MONDAY iss. 10, Oct. 2000, http://www.firstmonday.dk/issues/issue5_10/adar/; *see also infra note* 66 (reporting that *Free Riding* has been cited over 100 times in computer-science research papers); *cf.* Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 686 (2003) ("etiquette among users must be engineered or … induced with 'charismatic code'").

[15] *See* Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505, 526 (May 2003); *Compare* MusicLabs, LLC, Gnutella Good Citizen Tips, ("[A] good citizen will always shares files; the more the better."), http://www.bearshare.com/help/citizen.htm (last visited Sept. 19, 2006), *with* MusicLabs, LLC, Press FAQ, ("Gnutella 0.56, was good for its time but should never be used on the network since it does not have 'good citizen' features."), http://www.bearshare.com/help/faqpress.htm (last visited Sept. 19, 2006).

[16] Eytan Adar & Bernardo A. Huberman, *Free Riding on Gnutella*, 5 FIRST MONDAY iss. 10, Oct. 2000, http://www.firstmonday.dk/issues/issue5_10/adar/; Michael Feldman & John Chuang, *Overcoming Free-Riding Behavior in Peer-to-Peer Systems*, ACM SIGECOM EXCHANGES, vol. 5, iss. 4, 42 (July 2005). Professor Wu has argued that "the filesharer's comparative advantage lay in designing code to avoid copyright law." Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 740 (2003). The research cited above shows that this "advantage" comes at a cost: Designs that tend to facilitate the avoidance of copyright law also tend to discourage the sharing of files. *Cf. id.* at 717 ("P2P design shows that avoiding copyright requires important deviations from the optimal design for speed, control, and usability").

[17] Kevin Faaborg, *Losing the Long Tail*, LimeWire Blog (July 13, 2006) at www.limewire.org/blog/?cat=29. LimeWire levels a similar accusation at BitTorrent: "BitTorrent is horrible at rare stuff! As soon as a files becomes rare, it looses [sic] seeders and dies." *Id.*

[18] *See* Kristyn Maslog-Lewis, *Sharman Exec Calls Child Porn Unstoppable*, CNET NEWS.COM, Dec. 9, 2004, http://news.com.com/Sharman+exec+calls+child+porn+unstoppable/2100-1027_3-5486666.html; Richard Wallace, In Memory of Jessica (Mar. 23, 2005) (describing how a pedophile would use inadvertently shared data to abduct and murder a child and noting that "[a]ll names are fictitious, however the information in this scenario is based on my research of inadvertent file sharing via P2P networks"), http://www.seewhatyoushare.com (*available at* http://web.archive.org/web/200503 30014425/http://www.seewhatyoushare.com/).

[19] Similar conclusions are drawn in almost all subsequent research on filesharing networks. *See, e.g.*, Michael Feldman & John Chuang, *Overcoming Free-Riding Behavior in Peer-to-Peer Systems*, ACM SIGECOM EXCHANGES, vol. 5, iss. 4, 41 (July 2005) ("P2P system performance is highly dependent upon the amount of voluntary resource contribution from the individual nodes"); *id.* at 43 ("We find that if societal generosity is below a certain threshold, then there are too many selfish rascals around and the system collapses"); *id.* at 47 ("Overcoming free-riding behavior is central to the performance and robustness of P2P systems."); *id.* at 47 ("[U]ser behavior can have potentially devastating effects on P2P system performance, and so must be explicitly accounted for in P2P system design."); *see also* Stephan Schosser et al., *Incentives Engineering for Structured P2P Systems—A Feasibility Demonstration Using Economic Experiments*, PROC. 7TH ACM CONF. ON ELEC. COM. (2006) (free riding "can even lead to a collapse of these systems"); Robson Santos et al., *Accurate Autonomous Accounting in Peer-to-Peer Grids*, PROC. 3D INT'L WORKSHOP ON MIDDLEWARE FOR GRID COMPUTING (2005) (free riding can "collapse" a P2P network); Emmanuelle Anceaume et al., *Incentive for P2P Fair Resource Sharing*, PROC. 2ND INT'L WORKSHOP ON PEER-TO-PEER SYSTEMS, 139 (2003) (free riding can lead to "system collapse"); Lakshmish Ramaswamy & Ling Liu, *Free Riding: A New Challenge for Peer-to-Peer File Sharing Systems*, PROC. OF THE 36TH HICSS CONF. (2003) (discussing "the seriousness of the free riding problem and the need to tackle this growing menace"). Nevertheless, *Free Riding* remains unusual among the published research on filesharing because it acknowledges more explicitly that distributors and developers of filesharing programs—not merely users—might behave strategically, and in ways that are less than admirable.

[20] *See* Janelle Brown, *The Gnutella Paradox*, SALON, Sept. 29, 2000, http://archive.salon.com/tech/feature/2000/09/29/gnutella_paradox/print/html; *see also id.* (reporting that Gnutella would not scale unless it were to "include a system 'default' that forces all users to share, much like Napster").

[21] Stepan Sariou, P. Krishna Gummadi & Steven D. Gribble, *Measuring and Analyzing the Characteristics of Napster and Gnutella Hosts*, MULTIMEDIA SYSTEMS, vol. 9, iss. 2, 170 (2003). This study still concludes that more than 50% of available files were shared by 7% of users; it thus re-affirmed the conclusion that "Gnutella has an inherently large percentage of free-riders. *Id.*

[22] Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505, 526-27 (May 2003).

[23] Letter from Sharman Networks, Ltd., to Senators Graham, Feinstein, Durbin, Smith, Cornyn and Boxer, 4 (Dec. 15, 2003) (on file with author); *Universal Music Australia Pty Ltd v. Sharman License Holdings Ltd*, 2005 FCA 1242, *slip op.* at 55 (Fed. Ct. of Australia Sept. 5, 2005) (the CEO of Altnet concludes that "p2p exists by virtue of this feature being turned on"); *see also The Future of Peer-to-Peer (P2P) Technology: Hearing Before the Subcomm. on Competition, Foreign Commerce, and Infrastructure of the Senate Comm. on Commerce, Science, & Transportation*, 108th Cong. (June 23, 2004) (written testimony of Michael Weiss) ("[R]equiring a change in 'sharing' default[s]" would "hobbl[e]" Morpheus.); Nicolas Christin et al., *Content Availability, Pollution and Poisoning in File Sharing Peer-to-Peer Networks*, PROC. OF THE 6TH ACM CONF. ON ELECTRONIC. COM. 68, 72 (2005) ("Content replication is a direct result of propagation, and is perhaps the most important reason behind the success of peer-to-peer networks.")

[24] Nicolas Christin et al., *Content Availability, Pollution and Poisoning in File Sharing Peer-to-Peer Networks*, PROC. OF THE 6TH ACM CONF. ON ELECTRONIC. COM., 68 (2005); *see also id.* at 74 (concluding that redistribution features are also "an efficient antidote" to the spoofing efforts of rightsholders).

[25] Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505, 526 (May 2003); *cf.* Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 735 (2003) ("[KaZaA] promotes selfless behavior by sharing user files without telling the user.").

[26] Brief of Amicus Curiae Reviewing Issues of Fact and Law at 12, 44, 49, *Capitol Records, Inc. v. Alaujan*, No. 1:03-CV-11661-NG (Dist. Mass. May 24, 2004); *see also id.* at 2 (noting that their brief was filed not to advocate for a particular side, but "to help the Court strike a fair balance among legitimate and often competing interests in this matter"); *see also id.* at 10 ("Disabling the default file-sharing features in KaZaA is a complicated process due to an intricate series of steps within the software itself. In addition, the available resources that detail how to disable file sharing are often inconsistent or provide incomplete instructions."); *id.* at 12 ("The varying sources of instructions on disabling file sharing and the inconsistencies among them demonstrate that it can be extremely difficult for a non-expert computer user to shut down their file-sharing capability."); *id.* at 10-11 (quoting a college administrator who warns, "many people are unaware, that if file-sharing is on when they download a music or movie file, they automatically turn their computer into a server, providing those files to others across the Internet") (citation omitted); *id.* at 44 (arguing that "technological barriers" can prevent a user from controlling or supervising "infringing conduct of which he neither approves nor is aware"); *id.* at 49 ("[I]t may be unclear to an unsophisticated party that by simply downloading the service and failing to take certain additional affirmative action, the user is making certain files on his computer available to be uploaded by other users."); *id.* at 45 ("[S]ome may be able to point to the complexity of KaZaA's … disabling functions to support a finding that there was no awareness or intent to permit uploading.").

[27] Matthew Sag, *Piracy: Twelve Year-Olds, Grandmothers, and Other Good Targets for the Recording Industry's File Sharing Litigation*, 4 NW. J. TECH. & INTELL. PROP. 133, 148 (2006).

[28] *RIAA Sues another Grandmother*, P2PNET.NET NEWS, Aug. 2, 2006, http://p2pnet.net/story/9501; *see also Privacy and Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry: Hearing Before the Senate Permanent Subcomm. on Investigations of the Comm. On Gov'tal Affairs*, 108th Cong. 132-33 (Sept. 30, 2003) (statement of Lorraine Sullivan); Bob Mehr, *Gnat, Meet Cannon*, THE METER, Feb. 4, 2005 (reporting that Cecilia Gonzalez did not realize that she was sharing downloaded files), http://www.chicagoreader.com/TheMeter/050204.html.

[29] *Privacy and Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry: Hearing Before the Senate Permanent Subcomm. on*

Investigations of the Comm. On Governmental Affairs, 108th Cong. 132-33 (Sept. 30, 2003) (statement of Lorraine Sullivan).

[30] P2P United, Member Code of Conduct (Sept. 29, 2003), http://wiki.morpheus.com/~p2punited/code.php.

[31] Filesharing programs may also disclose information about redistribution features in End-User License Agreements ("EULAs") or "click here for more information" hyperlinks. Absent evidence that significant numbers of new users actually read EULAs or click on such hyperlinks, such disclosures would be, as a practical matter, irrelevant. *See, e.g.*, Ben Edelman, Comparison of Unwanted Software Installed by P2P Programs (March 7, 2005) (explaining the engineered difficulties involved in reading the KaZaA or eDonkey EULAs), http://www.benedelman.org/spyware/p2p.

[32] LimeWire is the exception, but its distributors deserve no credit for their "disclosures." LimeWire discloses its redistribution feature during its setup process, but it does so through an interface that does not allow the user to disable redistribution. Moreover, this interface also lets the user select a different folder to store downloaded files—but without warning the user that all subfolders of this folder will be shared recursively. This interface is, in effect, an undisclosed, recursive-sharing share-folder feature.

[33] Atip Asvanund, Sarvesh Bagla, Munjal H. Kapadia, Ramayya Krishnan, Michael D. Smith, Rahul Telang, *Intelligent Club Management in Peer-to-Peer Networks*, WORKSHOP ON ECON. OF PEER-TO-PEER SYSTEMS (2003), http://www2.sims.berkeley.edu/research/conferences/p2pecon/papers/s6-asvanund.pdf.

[34] *See, e.g.*, Lakshmish Ramaswamy & Ling Liu, *Free Riding: A New Challenge for Peer-to-Peer File Sharing Systems*, PROC. OF THE 36TH HICSS CONF. (2003) (explaining why a "replication enforcement scheme doesn't address the more serious problem of the system not getting new files and becoming stagnant"); *see also* Krishna Gummadi et al., *Measurement, Modeling, and Analysis of a Peer-to-Peer File-Sharing Workload*, PROC. 19TH SYMP. ON OPERATING SYSTEM PRINCIPLES 314, 320 (Oct. 2003) ("[T]he primary object dynamic in the Kazaa workload is the *arrival* of entirely new objects."); *id.* at 324 ("Without new popular [files] to choose from, existing clients quickly exhaust the set of popular objects.").

[35] As the term " share-folder feature" is used here, a program may have no " share-folder feature" even if it has a feature or interface that lets users store downloaded files in a folder other than the default download folder. As long as the interface has little potential to mislead the user into sharing files in a selected folder unintentionally, it is not a " share-folder feature" for purposes of this report. For example, both LimeWire 2.0.4 and KaZaA 2.5 contained features that let users store downloaded files in other folders, but these features were accompanied by disclosures that— while not perfect—distinguish these features from the "share-folder features" discussed in this report.

[36] *Supra*, note 7; *see also* Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 730 (2003) ("*Napster* taught peer network designers that both lack of control and *general functionality* had to be comprehensive and credible to avoid contributory liability.") (emphasis added).

[37] *See* AMERICA ONLINE, INC. & NATIONAL CYBER SECURITY ALLIANCE, AOL/NCSA ONLINE SAFETY STUDY (2005) (finding that 68% of respondents reported keeping sensitive data on their home computer and 74% used the computer for banking, stock trading, or reviewing medical data), http://www.staysafeonline.info/pdf/safety_study_2005.pdf.

[38] Worse yet, the potential for inadvertent sharing of sensitive files increases if users follow ordinary data-management practices. Users are now urged to store the data files created and used by their application programs in a single folder "tree" or hierarchy: In computers using the Windows operating system, the base of this folder hierarchy is usually the "My Documents" folder, or the "Documents and Settings" folder. *See, e.g.*, ED BOTT & CARL SEICHERT, WINDOWS XP INSIDE OUT 261-62 (2001). This

strategy makes it easier for users to locate, backup, and transfer data files. But this strategy means that disastrous breaches of privacy and security can result from inadvertent "sharing"—particularly *recursive* sharing—of existing files and folders, such as a user's "My Documents" folder.

[39] Nathaniel S. Good & Aaron Krekelberg, *Usability and Privacy: A Study of KaZaA P2P File-Sharing* (2002) *reprinted in* PROC. OF THE SIGCHI CONF. ON HUM. FACTORS IN COMPUTING SYSTEMS, vol. 5, iss. 1, 137-144. This study is now considered one of the "classics" of research on the interaction between usability and security. *See generally*, SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE (Lorrie Cranor & Simson Garfinkel eds., 2005).

[40] *Usability and Privacy* also identified other aspects of the KaZaA program that tended to confuse users, though they did not, in themselves, cause users to share files inadvertently. These included the media library view, and the fact that folders shared by the KaZaA share-folder feature were not labeled as shared in KaZaA's Shared Folder list. While these features may make it more difficult for users to detect inadvertent sharing, neither will, in itself, cause inadvertent sharing. Consequently, neither feature will be discussed in detail here.

[41] *See, e.g.*, Staff Report of the United States House of Representatives Comm. on Gov't Reform, *File-Sharing Programs and Peer-to-Peer Networks: Privacy and Security Risks*, 1 (May 2003) ("Committee investigators found … tax returns, medical records, attorney-client communications, and personal correspondence from P2P users [and] … at least 2,500 Microsoft Money backup files, which store the user's personal financial records, available for download.") *reprinted in Overexposed: The Threat to Privacy and Security on Filesharing Networks: Hearing Before the United States House of Representatives Comm. on Gov't Reform*, 108th Cong. 127 (May 15, 2003); *see also* Nicolas Christin et al., *Content Availability, Pollution and Poisoning in File Sharing Peer-to-Peer Networks*, PROC. OF THE 6TH ACM CONF. ON ELECTRONIC. COM. 68, 77 (2005) ("[S]tudies of user behavior show that a vast number of users are vastly unaware of the files they share.")(citation omitted).

[42] *The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of P2P File-Sharing Network?: Hearing Before the Senate Comm. on the Judiciary*, 108th Cong. 8 (June 17, 2003) (statement of Sen. Orrin G. Hatch); *see also id.* at 67 (statement of Sen. Patrick Leahy); *id*. at 2 (statement of Sen. Dianne Feinstein).

[43] *Id.* at 45 (comments on security by Phil Morle, Director of Technology for Sharman Networks, Ltd.); *accord id.* at 73 (written statement of Alan Morris, Executive Vice President for Sharman Networks, Ltd.).

[44] P2P United, Member Code of Conduct (Sept. 29, 2003), http://wiki.morpheus.com/~p2punited/code.php.

[45] *The Future of Peer-to-Peer (P2P) Technology, A Hearing before the Senate Subcommittee on Competition, Foreign Commerce and Infrastructure of the Senate Committee on Commerce, Science & Transportation* (June 23, 2004) (testimony of Mr. Michael Weiss on behalf of the distributors of BearShare, eDonkey, and Morpheus) at http://commerce.senate.gov/hearings/testimony.cfm?id=1247&wit_id=3577.

[46] P2P United, P2P United FAQ, http://wiki.morpheus.com/~p2punited/faq.php (last visited Sept. 18, 2006); *see also* LimeWire, Frequently Asked Questions ("Q: Are there security risks associated with using LimeWire? A: As long as you don't share your entire hard drive, you shouldn't encounter any significant security risks using Gnutella."), http://www.limewire.org/wiki/index.php?title=Frequently_Asked_Questions#sec1 (last visited Sept. 18, 2006).

[47] Comments of P2P United at 12, *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, A Workshop Before the Federal Trade Commission* (Jan. 18, 2005) *available at* http://www.ftc.gov/os/comments/p2pfileshare/index.htm (quoting the Senate testimony of Streamcast CEO Michael Weiss); *id.*at 4 (asserting that Morpheus, BearShare, and eDonkey "are in full compliance with the Code, which directly addresses … user data security"); *id.*at 10 ("[W]e are confident that the following characterizations of 'myth' and fact will prove accurate."); *see also Privacy and Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry: Hearing Before the Senate Permanent Subcomm. on Investigations of the Comm. On Gov't Affairs*, 108th Cong. 109 (Sept. 30, 2003) (statement of Alan Morris, Executive Vice President of Sharman Networks, Ltd.) (testifying that copyright holders "have attempted to smear the P2P industry and scare consumers by making false and misleading claims over bogus security issues and alleged privacy concerns"); Lisa Rein, *Interview with LimeWire COO Greg Bildson*, OPENP2P.COM, Nov. 14, 2003 ("[T]he RIAA is talking about … homeland security and identity theft and all of these things that are really minor concerns, with regard to P2P."), www.openp2p.com/pub/a/p2p/2003/11/14/limewire.html.

[48] *File Sharers, Beware!*, CBS EVENING NEWS, May 5, 2005, http://www.cbsnews.com/stories/2005/05/03/eveningnews/main692765.shtml; *see also id.* (reporting that one vigilant user warned 120 people that they were inadvertently sharing financial documents); *see also* Brian Krebs, *Extreme File Sharing*, WASHINGTONPOST.COM , Oct. 17, 2005 (reporting that when the author searched for inadvertently shared files on LimeWire, "I quickly found what I was looking for, and then some: dozens of entries for tax and payroll records, medical records, bank statements, and what appeared to be company books" and users sharing email "inboxes and archives"), http://blog.washingtonpost.com/securityfix/2005/10/extreme_file_sharing_1.html.

[49] Richard Wallace, Is a Free Song Worth Your Identity? (March 12, 2005) ("I know for a fact that identity theft is occurring via P2P…. I have personally called three different individuals where it was obvious that they were unknowingly sharing information…. All three responded with, thank you very, very much…. Someone has been using my credit cards and the bank's fraud detection system picked up on it; now I know how they got my info!"), http://www.seewhatyoushare.com/2005/03/is-free-song-worth-your-identity.html (*available at* http://web.archive.org/web/20050301025717/http://www.seewhatyoushare.com/).

[50] BLUE SECURITY, P2P EXPLOITED TO SPAM MILLIONS OF USERS 1 (2005) (*cited in* Gregg Keizer, *Spammers Mining P-To-P for Addresses*, INFORMATIONWEEK, April 19, 2005, http://www.informationweek.com/story/showArticle.jhtml?articleID=160903121).

[51] Chris Preimesberger, *Cyber-criminals Use P2P Tools for Identity Theft, Security Analyst Warns*, EWEEK, June 23, 2006, http://www.eweek.com/article2/0,1895,1980963,00.asp; *see also* PAUL PICCARD ET AL., SECURING IM AND P2P APPLICATIONS FOR THE ENTERPRISE, 231 (Marcus Sachs eds., 2005) ("A quick scan of the P2P networks turns up a treasure trove of files . . . including financial information, passwords, and files that you might not want to see the light of day.").

[52] DEPARTMENT OF HOMELAND SECURITY, UNAUTHORIZED PEER TO PEER (P2P) PROGRAMS ON GOVERNMENT COMPUTERS (2005), http://www.dhs.gov/interweb/assetlibrary/IAIP_UnauthorizedP2P ProgramsGovtComp_041905.pdf; *see also* Eric Horton, *Downloading Shared Files Threatens Security*, ARMY NEWS SERVICE, April 22, 2004 ("Over a two-month period at the end of [2003], government organizations identified more than 420 suspected P2P sessions on Army systems in more than 30 locations around the globe."), http://www4.army.mil/ocpa/read.php?story_id_key=5878.

[53] *Compare* Nathaniel S. Good & Aaron Krekelberg, *Usability and Privacy: A Study of KaZaA P2P File-Sharing* (2002) *reprinted in* PROC. OF THE SIGCHI CONF. ON HUM. FACTORS IN COMPUTING SYSTEMS, vol. 5, iss. 1, 138 (2003) (finding inadvertently shared email inbox files on Gnutella "yet in fewer numbers than KaZaA"), *with* Thomas Mennecke, *What's in Your Shared Folder?*, SLYCK, June 30, 2004 ("When it

comes to shared personal information, the most prolific network seems to be Gnutella."), http://www.slyck.com/news.php?story=536.

[54] P2P United, Member Code of Conduct (Sept. 29, 2003), http://wiki.morpheus.com/~p2punited/code.php.

[55] *Cf.* 18 U.S.C. § 1030 (2006).

[56] Thomas Mennecke, *What's in Your Shared Folder?*, SLYCK, June 30, 2004 http://www.slyck.com/news.php?story=536.

[57] Recent versions of Morpheus download and install in a way that makes it very difficult to repeat experiments with non-current 4-series or 5-series versions of Morpheus. Most filesharing programs use a two-step installation process: A new user goes to a website and downloads a "stub" installer to their computer. When activated, this installer connects to the filesharing network and downloads a copy of the relevant filesharing program from another user. This two-step installation process makes it relatively easy to find non-current versions of most filesharing programs.

Since at least Morpheus 4.0, Morpheus has used a three-step installation process: A new user downloads a stub-installer from a website; this stub installer then connects to the Gnutella network and downloads another "smart installer." When run, this smart installer connects to the Morpheus web site and downloads the most recent version of Morpheus. This three-step installation process makes it difficult to obtain copies of non-current 4-series or 5-series versions of Morpheus that can be installed and operated repeatedly to confirm how they behave. Nevertheless, while this smart-installer-based installation process frustrates the type of analysis used in this report, it also has benefits: For example, it would prevent users from downloading and installing past versions of a program that had security flaws. Consequently, this report draws no adverse inferences about the installation process used by Morpheus.

[58] MARK N. COOPER, TIME FOR THE RECORDING INDUSTRY TO FACE THE MUSIC: THE POLITICAL, SOCIAL AND ECONOMIC BENEFITS OF PEER-TO-PEER COMMUNICATIONS NETWORKS 3, 4 (2005), http://www.consumerfed.org/pdfs/benefitsofpeertopeer.pdf.

[59] *See* P2P United, Member Code of Conduct (Sept. 29, 2003), http://wiki.morpheus.com /~p2punited/code.php; *see also* Stopbadware.org, Software Guidelines (defining "badware" to include "software which is not easy to uninstall completely" and asserting that once uninstalled, "an application must not leave behind any functionality or design elements"), www.stopbadware.org/home/guidelines (last visited Sept. 18, 2006).

[60] *Privacy and Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry: Hearing Before the Senate Permanent Subcomm. on Investigations of the Comm. On Gov't Affairs*, 108th Cong. 44 (Sept. 30, 2003) (testimony of Alan Morris, Executive Vice President of Sharman Networks, Ltd.).

[61] *When Private Files Become Public*, SYDNEY MORNING HERALD, Aug. 6, 2004, *available at* http://www.smh.com.au/articles/2004/08/05/1091557983595.html.

[62] *Supra, n. 48.*

[63] MusicLabs, LLC, An Important Word from BearShare about Keeping Your Private Information Private, http:/www.bearshare.com/data-security.htm (last visited Sept. 18, 2006).

[64] Scores of detailed, illustrated instructions are available on the Internet; most originate from one of three sources. Some instructions were provided by public-interest groups like EFF. *See, e.g.*, Electronic

Frontier Foundation, How Not to Get Sued by RIAA for File-Sharing, http://www.eff.org/IP/P2P/howto-notgetsued.php (last visited Sept. 18, 2006). Most were provided by colleges and universities like Duke University or the University of Chicago. *See, e.g.*, University of Chicago Networking Services and Information Technologies, Disabling Peer to Peer File Sharing, http://security.uchicago.edu/peer-to-peer/no_fileshare.shtml (last visited Sept. 18, 2006). Others were provided by ISPs. For reasons discussed below, most of these instructions now appear to be dated and inaccurate.

[65] ELECTRONIC FRONTIER FOUNDATION, RIAA V. THE PEOPLE: TWO YEARS LATER, 11 (2005), http://www.eff.org/IP/P2P/RIAAatTWO_FINAL.pdf. EFF speculates that this "leeching" will not harm filesharing networks because "there is no shortage of offshore uploaders for U.S. file sharers to rely on." *But see infra* note 66. EFF also invokes the "darknet defense" of piracy: It claims that enforcing the law against users of popular filesharing programs will just drive them to adopt "darknet" technologies that hinder private law-enforcement efforts. EFF cites several such technologies, including DirectConnect, FreeNet, and MUTE.

It is irresponsible to refer blithely to these three "darknet" programs as if they were just extra-hip-and-sneaky substitutes for KaZaA. They differ significantly, and these differences can have life-altering implications for their users and potentially life-ending implications for others. In truth, users of popular filesharing programs are not likely to adopt these programs—if they understand the potential consequences.

FreeNet contains a true forced-sharing feature: Every user of FreeNet must share files; the program itself decides which files a user will share and copies them onto the user's hard drive. The developers of FreeNet admit that this means that you can only run FreeNet if you are willing to have your computer store and distribute violent child pornography or terrorists' plans for a new 9-11-like attack on civilians: "If [harboring 'child porn' or 'terrorism'] is not acceptable to you, you should not run a FreeNet node." *See* FreeNet, Frequently Asked Questions, http://freenetproject.org/index.php?page=faq#offensive (last visited Sept. 18, 2006). This means that no reasonable person can run a FreeNet node. Nor should users assume that they will be held blameless for facilitating pedophilia or terrorism just because the files distributed from their computer will be weakly encrypted: FreeNet's distributors explain that this encryption does not protect the privacy of the stored files, but it does provide "plausible deniability" so FreeNet users can deny knowing which files they were storing and distributing. *Id.* A similar attempt to use encryption as a blindfold to avoid knowledge of illegal acts not only failed, it backfired affirmatively: It was held to provide evidence of the sort of "willful blindness" from which courts will infer criminal intent. *See In re Aimster Copyright Litigation*, 334 F.3d 643, 650 (7th Cir. 2003).

DirectConnect software creates "closed," non-public filesharing networks in which one user's computer acts as a "hub," as a network search-index server like those that once imposed billion-dollar liability upon Napster, Inc. These non-public networks do make private enforcement more difficult: And that is why participants in Direct Connect filesharing networks have been prosecuted criminally. *See* United States Dept. of Justice, *Attorney General Ashcroft Announces First Criminal Enforcement Action Against Peer-to-Peer Copyright Piracy*, (Aug. 25, 2004), http://www.usdoj.gov/criminal/cybercrime/operation_gridlock.htm. One convicted felon has offered a moving account of the price of "free music" via Direct Connect. *See* Mickey Borchard, *The tale of the sinking of an online music pirate*, JOURNAL TIMES, Apr. 10, 2006, http://www.journaltimes.com/articles/2006/04/10/opinion/iq_3987486.txt.

MUTE is a specialized copyright-piracy tool. Its developer explains that MUTE "helps people break the law." He admits this openly: "Sure many other P2P developers and companies blatantly lie about what their software is for, but I refuse to lie." Howard Wen, *Open Source P2P with MUTE*, ONLAMP.COM, Aug. 12, 2004, http://www.onlamp.com/pub/a/onlamp/2004/08/12/mute.html?page=1. MUTE, *How File Sharing Reveals Your Identity*, *at* http://mute-net.sourceforge.net/howPrivacy.shtml (last visited Sept. 18, 2006). But MUTE helps its infringing users break the law through a forced-proxying feature: As with FreeNet, users who run MUTE must be willing to store and distribute files containing child pornography or terrorist training manuals. *See* Michael Ingram, *Ants P2P2P: A New Approach to File-Sharing*, SLYCK NEWS, Sept.

13, 2004 (The developer of an open-source clone of MUTE explains that users should not worry about distributing child pornography because "with this way of reasoning, people should still live in caves."), http://www.slyck.com/news.php?story=567.

[66] Daniel Hughes et al., *Free Riding on Gnutella Revisited: The Bell Tolls*?, IEEE DISTRIBUTED SYSTEMS ONLINE, vol. 6, iss. 6, (June 2005), http://csdl2.computer.org/comp/mags/ds/2005/06/o6001.pdf. At first, it might seem odd that the authors of *Revisited* assert that their findings confirm the findings of *Free Riding on Gnutella*: After all, the Gnutella network had not collapsed by 2005, even with levels of sharing far lower than those reported in 2000. But, as *Revisited* notes, the architecture of the Gnutella network had changed significantly between 2000 and 2005. In 2000, the search process on Gnutella was genuinely decentralized: All users participated as "peers" in the search process. This limited both the functionality and the scalability of Gnutella. By 2005, Gnutella had become more centralized: "Ultrapeers" indexed files shared by others and responded to search queries. These "ultrapeers" act as search-index servers like the "supernodes" on the FastTrack network or the search-index servers on the filesharing system created by Napster, Inc. As a result, the 2005 version of Gnutella could function with lower levels of sharing than the 2000 version of Gnutella. This difference in architecture reconciles the findings of *Free Riding* and *Revisited*: The 2000 study could fairly conclude that a 34% sharing level put the 2000 version of Gnutella on the verge of collapse, and the 2004 study could conclude that a 15% sharing level put the 2005 version of Gnutella on the verge of collapse.

Another study has also drawn interesting conclusions about the effects of enforcement on users' propensity to share files. *See* Sudip Bhattacharjee, et al., *Impact of Legal Threats on Online Music Sharing Activity: An Analysis of Music Industry Legal Actions*, 49 J. L. & ECON. 91, 102-106 (April 2006) (concluding that the filing of "John Doe" lawsuits significantly reduced user's propensity to share files). It reports that before lawsuits were announced, the average and median number of audio files shared by studied KaZaA users were, respectively, 343 and 227. After the filing of lawsuits, the average number of files shared dropped to 93, and the median number of files shared plunged to 11. *Id.* at 102. The increasing difference between the average and median number of files shared indicates that almost all users radically curtailed their sharing while a few kept sharing very large numbers of files. *Cf. id.* at 106. The authors note that these undeterred high-volume sharers may have been located oversees. If so, then there should have been few or no high-volume U.S. sharers to be targeted by subsequent rounds of lawsuits.

[67] Distributors deriving revenue from the production or use of their filesharing programs would have strong incentives to avoid such defections: "Leeching" users may contribute nothing to *other users* of a filesharing program, but they generate advertising revenues for its distributor. *See, e.g., MGM Studios, Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764, 2782 (2005) ("Since the extent of the software's use determines the gain to its distributors, the commercial sense of their enterprise turns on high-volume use, which the record shows is infringing."). Professor Strahilevitz agrees with this analysis and proposes that distributors who deployed true forced-sharing features could be held vicariously liable. Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505, 522 n.68 (May 2003) (arguing that this "might make the peer-to-peer networks more plainly guilty of vicarious copyright infringement").

[68] *Cf.* XAVIER GABAIX & DAVID LAIBSON, SHROUDED ATTRIBUTES, CONSUMER MYOPIA, AND INFORMATION SUPPRESSION IN COMPETITIVE MARKETS, NPER WORKING PAPER NO. 11755 (2005) (describing circumstances in which both producers and sophisticated users of a product or service can benefit when producers conceal information about the true costs of a product or service from "myopic" consumers), http://www.nber.org/papers/w11755. The "myopic" consumers discussed in *Shrouded Attributes* are not dupes for purposes of inducement liability. Nevertheless, its analysis appears highly relevant to filesharing because it shows that both distributors and their advertising-revenue-generating, sophisticated "leaching" users could benefit from the content added to the network by an *avoidable* feature that tends to trick young or new users into sharing infringing files.

[69] KaZaA does not contain a coerced-sharing feature of the sort described here. Nevertheless, its Participation Level feature did, as a practical matter, require users who wanted to download files from others to share files that other users wanted to download. This Participation-Level feature may require users to share—and it may deter use of a copy-and-delete strategy for downloading—but users who want to improve their ability to download by increasing their Participation Level must understand that the feature exists and how it works. Consequently, while KaZaA's Participation Level feature might persuade users to share infringing files intentionally, it is not a duping scheme.

[70] This report will not discuss the "mechanisms" in each program that seem to let sophisticated users disable sharing of their download folder. Confirming that these mechanisms actually work would require extended packet-level monitoring of the data being received and transmitted by the program in question. Such analysis exceeds the scope of this report, and it would be imprudent to recommend or suggest that users employ these "mechanisms" until extended analysis proves that they are effective. *See, e.g.*, Hofstra University Student Computer Services, How to Disable File Sharing in KaZaA or Morpheus (2000) (reporting that even if a user changed the "maximum simultaneous uploads" limit in Morpheus 2.0 to "0," "Morpheus may still attempt to share files regardless of these changes"), http://www.hofstra.edu/StudentServ/CC/SCS/scs_Filesharing.cfm.

[71] LimeWire retains an undisclosed, recursive-sharing share-folder feature in its installation-and-setup process.

[72] *See* Nathaniel Good and Aaron Krekelberg, *FTC Comments on P2P Filesharing and Privacy*, at http://www.ftc.gov/os/comments/p2pfileshare/050126nathanielgoodandaaronkrekelberg.pdf.

[73] *Is Gnutella Dying?*, THE WORLD ON A STRING, April 19, 2006, http://theworldstrung.com/?p=38.

[74] *The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of P2P File-Sharing Networks: Hearing Before the Senate Comm. on the Judiciary*, 108th Cong. 86 (June 17, 2003) (written statement of Consumers Union).

[75] *See, e.g.*, p2pecon@berkeley, Project Overview, http://p2pecon.berkeley.edu (last visited Sept. 18, 2006); JOHN CHUANG, IN SEARCH OF HOMO SWAPPUS: EVOLUTION OF COOPERATION IN PEER-TO-PEER SYSTEMS (2005), http://p2pecon.berkeley.edu/ppt/swappus.pdf.

[76] Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 725 & fig. 3 (2003).

[77] *Overexposed: The Threat to Privacy and Security on Filesharing Networks, a Hearing Before the United States House of Representatives Comm. on Gov't Reform*, 108th Cong. 63 (May 15, 2003) (testimony of Derrick Broes).

[78] TRUSECURE, THE PEER-TO-PEER HOLE IN YOUR NETWORK 2 (finding malicious code in 45% of popular downloads and 60% of popular executable files); *see also Overexposed: The Threat to Privacy and Security on Filesharing Networks, a Hearing Before the United States House of Representatives Comm. on Gov't Reform*, 108th Cong. 37 (May 15, 2003) (statement of Dr. John Hale describing the Duload worm that "copies itself to several provocatively named files within a media folder which it exposes to the P2P network"); *see also* David J. Stang, *The Impact of a Peer-to-Peer File Sharing Program…*, PestPatrol Research Center (Mar. 13, 2004) ("A P2P worm can masquerade as a desired music file, and be distributed the same way that other P2P files are shared. But the damage that it can cause is effectively without limit."), http://research.pestpatrol.com/KnowledgeBase/Whitepapers/P2P_Impact.asp; WEBSENSE, THOSE AREN'T JUST FILES YOU'RE SWAPPING—THE DANGERS OF PEER-TO-PEER 6 ("P2P networks can be, and are, easily exploited to distribute viruses and worms, allowing them to bypass normal security and filtering barriers."), http://www.websense.com/docs/WhitePapers/PeertoPeer.pdf; OSTERMAN RESEARCH, MANAGING IM AND P2P THREATS IN THE ENTERPRISE 6 (2004) ("Downloading content from P2P networks

bypasses corporate messaging security systems, leaving an enterprise network susceptible to viruses, worms, Trojans, buffer overflow vulnerabilities, spyware, adware and similar threats."), http://www.spywareguide.com/whitepapers/osterman.pdf; Lance Ulanoff, *Welcome to Spyware City*, PC MAGAZINE, Apr. 6, 2005 ("Trojans and other garbage are always piggybacking on the files you want, and sometimes *masquerading* as the files you want"); John E. Dunn, *File-sharing app compromises power station*, PC ADVISOR, May 17, 2006 (reporting that a virus downloaded from a filesharing network compromised the security of files that revealed a power plant's security procedures, layout, control room location, and the names and addresses of its security staff); *id.* (This article reports another incident in which "Mitsubishi Electric leaked 40MB of data, some of which related to a nuclear power station…. Again, the culprit was a single PC using a P2P program that allowed a virus to sneak through conventional data defenses.").

[79] McGill Network and Communications Services, *Introduction to P2P Security* (Feb. 3, 2006) at http://www.mcgill.ca/ncs/products/security/p2p/.

[80] Jonathan Schmidt, *When Music Becomes a Security Threat*, BANKERS' IDEANET, July 2003, http://www.sheshunoff.com/email/archive/0703/oper_new1.html; *see also* BLUECOAT, ESTABLISHING AN INTERNET USE POLICY TO ADDRESS PEER-TO-PEER (P2P) USE 2 (2004), http://www.bluecoat.com/downloads/whitepapers/BCS_Controlling_P2P_survey.pdf; *see also* TRUSECURE, THE PEER-TO-PEER HOLE IN YOUR NETWORK 2 ("blocking your users from using KaZaA is almost impossible"); OSTERMAN RESEARCH, MANAGING IM AND P2P THREATS IN THE ENTERPRISE 1 (2004) (P2P clients "are quite adept at circumventing existing security defenses"), http://www.spywareguide.com/whitepapers/osterman.pdf; *Overexposed: The Threat to Privacy and Security on Filesharing Networks: Hearing Before the United States House of Representatives Comm. on Gov't Reform*, 108th Cong. 29 (May 15, 2003) (written testimony of Jeffrey I. Schiller, Security Architect, MIT at 29) ("The authors of the peer to peer file sharing networks continue to modify and adapt their programs with the apparent goal, among others, of subverting attempts to control them."); *id.* ("[A] major risk of peer to peer filesharing is that it attempts to subvert legitimate controls placed on its use."). Common evasion tactics include port-hopping, tunneling and push-message requests. *See, e.g.,id.* at 36 (written testimony of Dr. John Hale, Director, Center for Information Security, University of Tulsa) ("Another commonly used trick is for P2P clients to vary their communication ports—a technique called port hopping. This thwarts blocking and scanning software…."); SANDVINE, MEETING THE CHALLENGE OF TODAY'S EVASIVE P2P TRAFFIC 9 (2004) (discussing tunneling and noting, "The P2P development community … has developed several tactics for hiding the true identity of packets."), http://www.sandvine.com/solutions/resource_library.asp.

[81] WEBSENSE, THOSE AREN'T JUST FILES YOU'RE SWAPPING—THE DANGERS OF PEER-TO-PEER 10 ("[T]here is no business application for the use of P2P file sharing in most organizations…."), http://www.websense.com/docs/WhitePapers/PeertoPeer.pdf; BLUECOAT, ESTABLISHING AN INTERNET USE POLICY TO ADDRESS PEER-TO-PEER (P2P) USE 2 (2004) ("The business value of P2P file sharing is very limited…. Most businesses derive no value from P2P file sharing on their networks…."), http://www.bluecoat.com/downloads/whitepapers/BCS_Controlling_P2P_survey.pdf; *id.* at 4 ("P2P use does not generally serve a productive business function; therefore, there is no need for it to exist on the corporate network."); OSTERMAN RESEARCH, MANAGING IM AND P2P THREATS IN THE ENTERPRISE 4 (2004) ("P2P networks … have far less—if any—legitimate use in a corporate environment…."), http://www.spywareguide.com/whitepapers/osterman.pdf; JIM MURPHY & DAVE ZWIEBACK, PROTECTING THE ENTERPRISE FROM INSTANT MESSAGING AND PEER-TO-PEER THREATS 6 (2005) ("In the majority of enterprise settings, it is almost impossible to find justification for the use of current incarnations of Internet peer-to-peer filesharing applications."), http://www.surfcontrol.com/general/assets/whitepapers/IM_and_P2P_whitepaper.pdf.

[82] *MGM Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029, 1041 (C.D. Cal. 2003), *aff'd*, 380 F.3d 1154 (9th Cir. Cal. 2004), *rev'd*, 125 S. Ct. 2764 (2005).

[83] LAWRENCE LESSIG, CODE 57 (1999) (calling this the "bovine account" of human nature).

[84] The *amicus* brief filed by the Berkman Center law professors in *Alaujan* theorizes that users of filesharing programs who have shared files unintentionally may not be liable even under a theory of strict liability because sharing can occur "without the [user's] participation" or "without [the user] acting at all." Brief of Amicus Curiae Reviewing Issues of Fact and Law at 44 n.46, *Capitol Records, Inc. v. Alaujan*, No. 1:03-CV-11661-NG (Dist. Mass. May 24, 2004). This is incorrect: *None* of the "features" discussed here can cause sharing absent some affirmative "participation" and "act" by the user of the program. In the cases of redistribution and coerced-sharing features, the act is downloading. In the case of share-folder and search-wizard features, the act is activating the feature and accepting the results. Consequently, the problem is not that users can share files inadvertently without acting at all. Rather, it is that users may share files inadvertently because filesharing programs often do a poor job of ensuring that users will understand the consequences of their own actions. In such cases, a contribution or other legal action by the user against the distributor of the program in question may provide a means to assess the relative culpability and contribution of their respective acts to any resulting infringement. *See infra* note. *87*.

[85] Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505, 553 (May 2003).

[86] *BMG Music v. Gonzalez*, 430 F.3d 888 (7th Cir. 2005).

[87] *Interscope Records v. Duty*, No. 05-CV-3744-PHX-FJM, 2006 U.S. Dist. LEXIS 20214 at *9 (D. Ariz. Apr. 14, 2006).

[88] *See, e.g.*, Secunia Advisory: SA14555 (Mar. 15, 2005), http://secunia.com/advisories/14555/; *see also* John Leyden, *Limewire patches serious snooping bugs*, THE REGISTER, Mar. 16, 2005, www.channelregister.co.uk/2005/03/16/limewire_vuln/print.html.

[89] This report focuses on programs that "operate in a manner conceptually analogous to the Napster system…." *Metro-Goldwyn Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029, 1032 (C.D. Cal. 2003); *see also Grokster*, 125 S. Ct. at 2781 ("Morpheus software functions as Napster did, except that it could be used to distribute more kinds of files….").

[90] For a useful survey of most of the reported studies and their methodology, see Danny Hughes, James Walkerdine, and Kevin Lee, *Monitoring Challenges and Approaches for P2P File-Sharing Systems*, INT'L CONF. ON INTERNET SURVEILLANCE AND PROTECTION, 18 (2006).

The published studies cited in this report rely on data collected from filesharing networks from 2000 through 2004. There are also two presently unpublished analyses of data collected during 2005. Individually and collectively, they are very interesting.

The first analysis arose after an author of this report asked the authors of *Free Riding on Gnutella Revisited: The Bell Tolls?* whether they had collected any additional trace data since May of 2004. They graciously analyzed trace data collected in March of 2005 for another study, *Is Deviant Behavior the Norm on Peer-to-Peer File-Sharing Networks?*, IEEE DISTRIBUTED SYSTEMS ONLINE, vol. 7, iss. 2, (Feb. 2006). Preliminary analysis of their March 2005 data showed that 93.3% of studied users shared no files.

A second unpublished study is Shanyu Zhao, Daniel Stutzbach, Reza Rejaie, *Characterizing Files in the Modern Gnutella Network: A Measurement Study* at http://www.cs.uoregon.edu/~reza/PUB/mmcn06.pdf. This study used a different method to collect data from the Gnutella network during June, August, and October of 2005. *Characterizing* tried to study the population of Gnutella users by using a crawler to identify users participating in the network and then using the browse-host feature implemented in programs

like LimeWire and BearShare to identify the files that each user was sharing. *Characterizing* reported that the studied users shared an average of about 350 files, and that only 13% shared no files.

The 13% free-riding rate reported in *Characterizing* is interesting when compared against the 93% free-riding rate derived from the March 2005 dataset used in *Deviant Behavior*. The vast discrepancy in these results may result from some fundamental, but as yet unidentified, change in the programs themselves. Nevertheless, the different data-collection methods used in *Deviant Behavior* and *Characterizing* could explain some or even most of the differences in user's sharing behavior. As *Characterizing* notes, its data-collection method would work only if a particular user 1) was connected to the network for a relatively long time; 2) was not firewalled; and 3) had not disabled the browse-host feature. In practice, this method worked only 18.5% of the time.

As a result, the data-collection method used in *Characterizing* may tend to show – not the sharing behavior of Gnutella users generally – but the behavior of the two disparate subgroups of users who would be likely to be running an unfirewalled, browse-host enabled filesharing program for relatively long periods. One subgroup might consist of highly *un*sophisticated users who were using browse-host-enabled filesharing programs without a firewall. The other subgroup might consist of sophisticated "true-believers" in filesharing who had both the expertise and the motivation needed to configure their firewall in order to give a filesharing program unrestricted access to the Internet. *See, e.g.*, BearShare, *Gnutella Good Citizen Tips* at http://www.bearshare.com/help/citizen.htm (last visited June 19, 2006) ("You don't need to get rid of your firewall completely, you just need to "drill a hole" in it for BearShare. It won't decrease your security because BearShare doesn't contain any security holes.") Both groups would be very likely to be sharing files, and in significant numbers, though probably for very different reasons.

In short, while it is too early to draw conclusions about the 2005 datasets, they are intriguing, and they suggest that more remains to be learned about the effects that program design and legal enforcement have upon users' propensity to share files.

[91] *See supra, n.11*.

[92] In effect, a filesharing program is said to create a "decentralized" filesharing network if it has been designed to create search-index servers—and perhaps even dedicated fileservers—on computers owned by parties other than the distributor of the filesharing program. So used, the term "decentralized" has a legal rather than technical meaning: Napster, Inc., could thus have converted its "centralized" filesharing network into a "decentralized" filesharing network just by giving the computers that housed its search-index servers to third parties. *See* Edward Felten, *"Centralized" Sites Not So Centralized After All*, FREEDOM TO TINKER, Oct. 6, 2005 ("The issue is who controls those computers."), http://www.freedom-to-tinker.com/?p=906.

[93] Under early versions of the Gnutella protocol, users did participate as peers in a decentralized search process, but the programs discussed here now create "ultrapeers," (search-index servers), on the computers of users who have high-speed Internet access. *See supra* note. *66*. Reports also indicate that these programs now, whenever possible, thwart the actual peer-to-peer file transfers that once occurred over the Napster, Inc. network: By default, these programs will redirect a user's request to download a file from another "peer" user to a specialized, high-speed, terabyte-sized fileserver that exists solely to store and transfer files "shared" over filesharing networks. Programs use this fileserver-based architecture by default because "downloads … are faster": "[E]nd-users typically experience a net acceleration effect of 2x—4x." Joltid, Benefits and Recent Statistics, http://www.joltid.com/index.php/peercache/ benefits_and_recent_statistics (last visited March 1, 2005) (*available at* http://web.archive.org /web/20041027021141/http://www.joltid.com/index.php/peercache/ benefits _and_recent_statistics). For example, the owner of the FastTrack protocol and the KaZaA filesharing program warns users that disabling use of these fileservers and actually downloading files from peers "will most likely slow down downloads dramatically." *Id.* at http://www.joltid.com/index.php/peercache/faq/enduser (last visited March

1, 2005) (*available at* http://web.archive.org/web/20041022005537/www.joltid.com/index.php/peercache/faq/enduser). This report does not reconcile this reported preference for faster, fileserver-based file transfers with representations about the alleged advantages of peer-to-peer file transfers made to the Supreme Court and the Federal Trade Commission. *See, e.g.,* MGM Studios, Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2770 (2005) ("[peer-to-peer] file … retrievals may be faster than on other types of networks"); Brief for Respondents at 3, *MGM Studios Inc. v. Grokster, Ltd.,* No. 04-480 (March 1, 2005) ("if material sought by a user already resides on other users' computers that can be accessed over already-in-place communication lines, then it is a wasteful redundancy *also* to store the material on a group of central servers").