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:

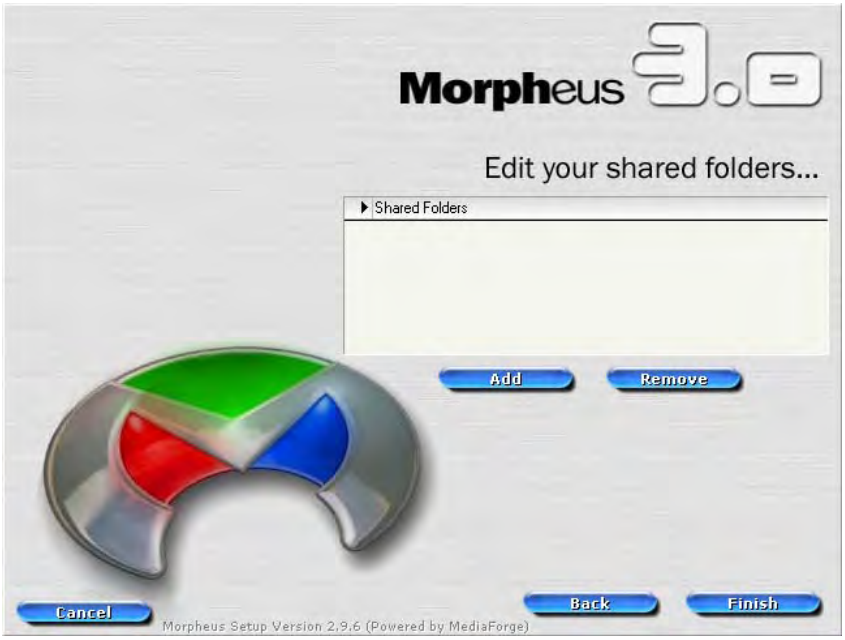


Figure 1: Morpheus 3.0.36

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:

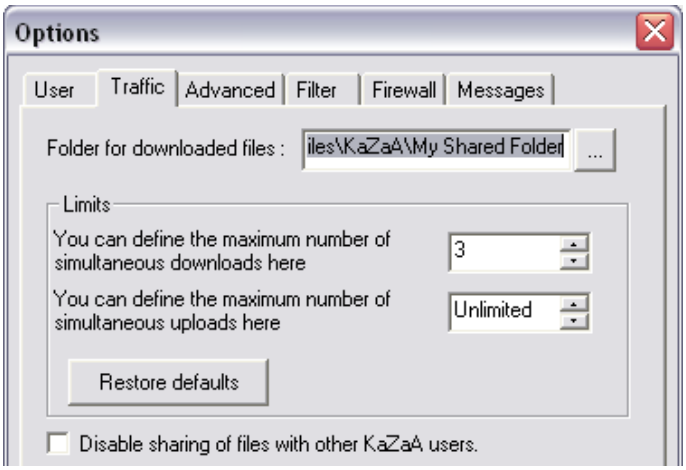


Figure 4: KaZaA 1.7.1

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:

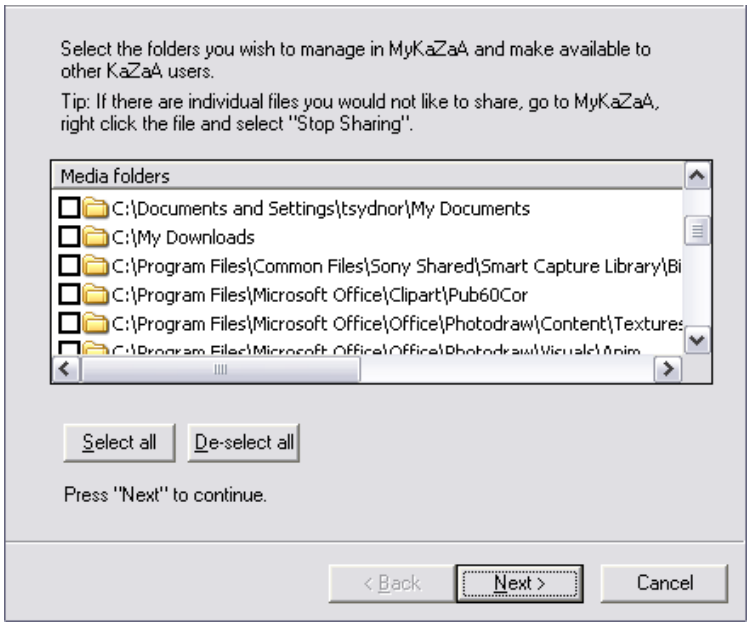


Figure 5: KaZaA 1.7.1

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":

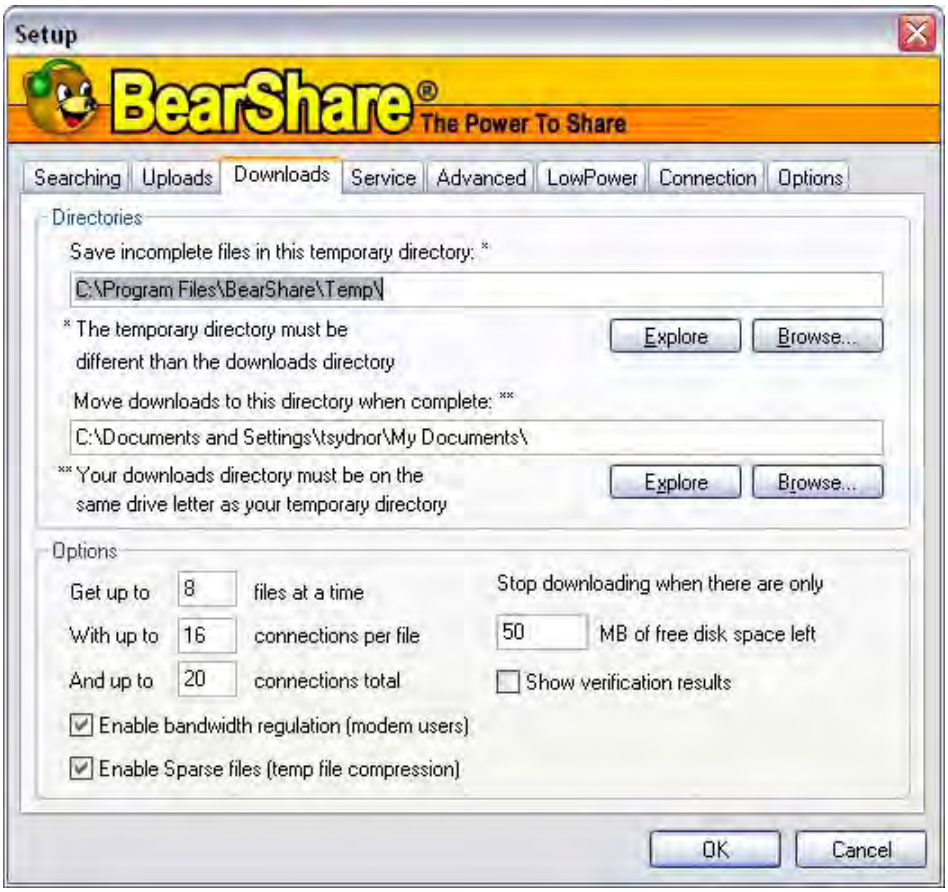


Figure 7

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":

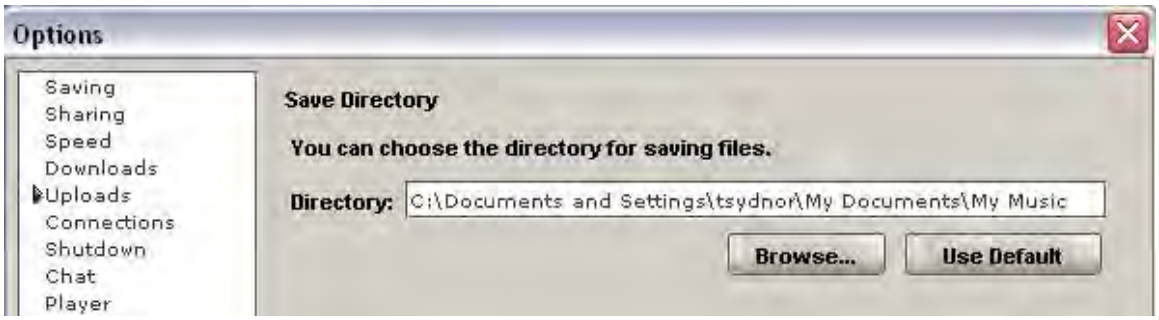


Figure 8: LimeWire 4.0.7

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:

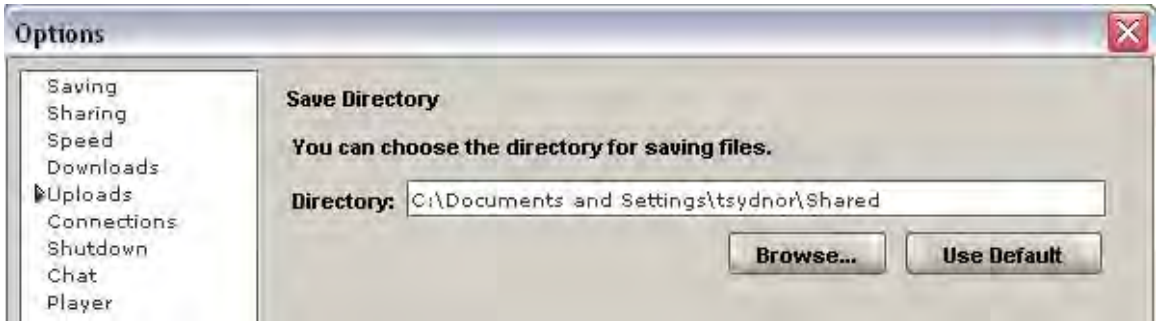


Figure 9: LimeWire 4.0.7

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:

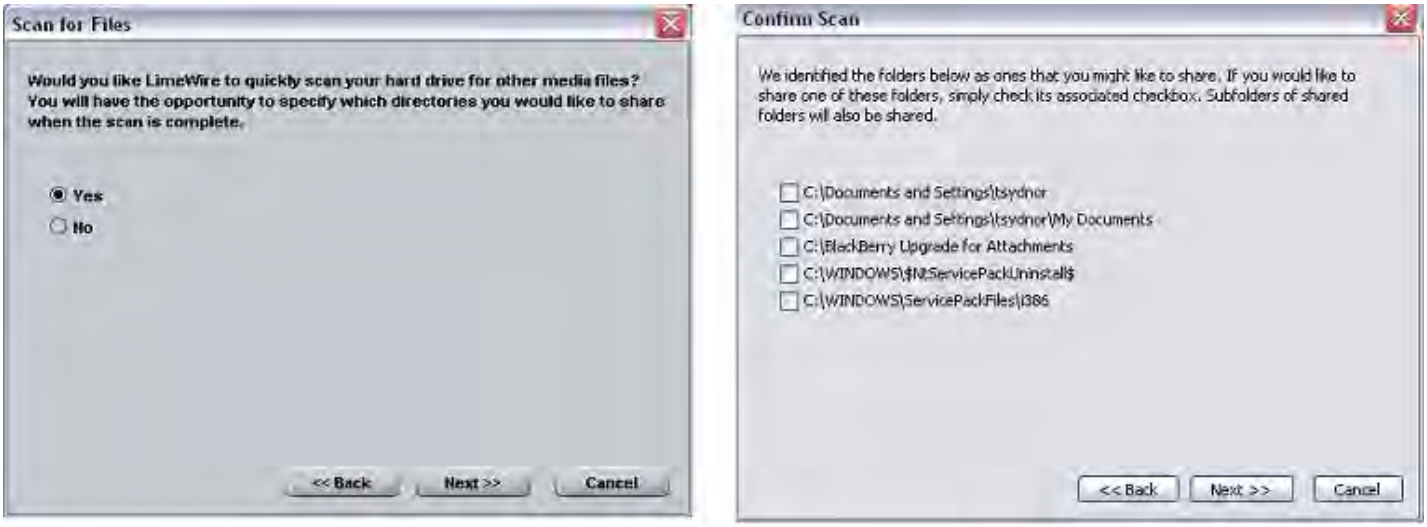


Figure 11: LimeWire 4.10.9

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.

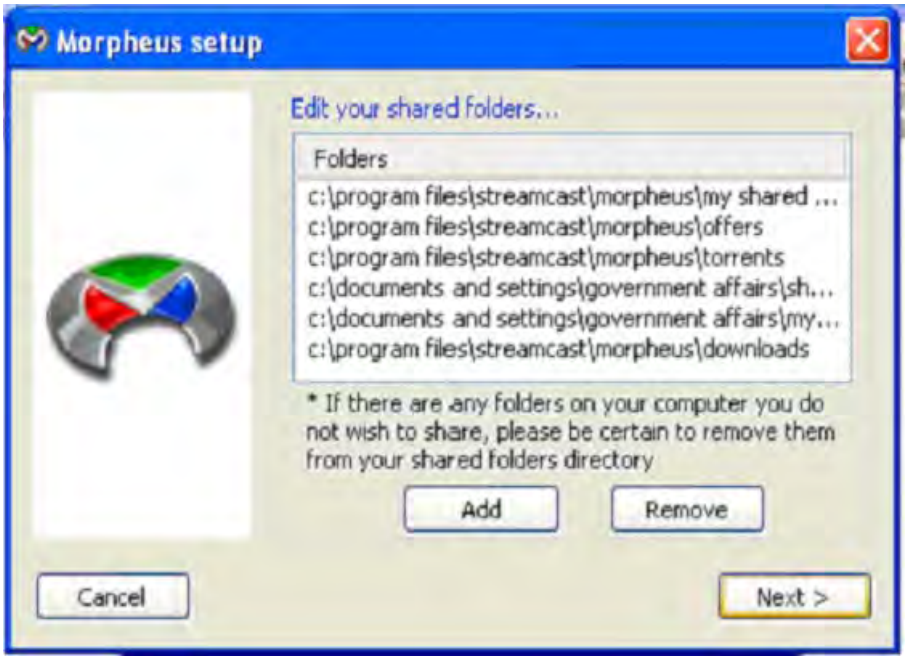


Figure 13: Morpheus 4.7.1.326

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:

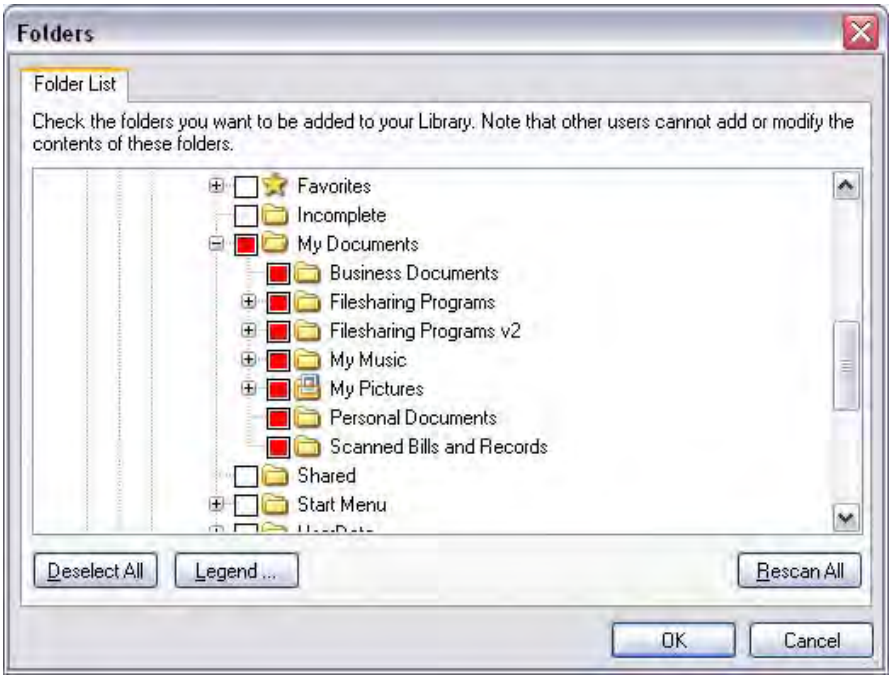


Figure 14: BearShare 4.7.0.76

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:

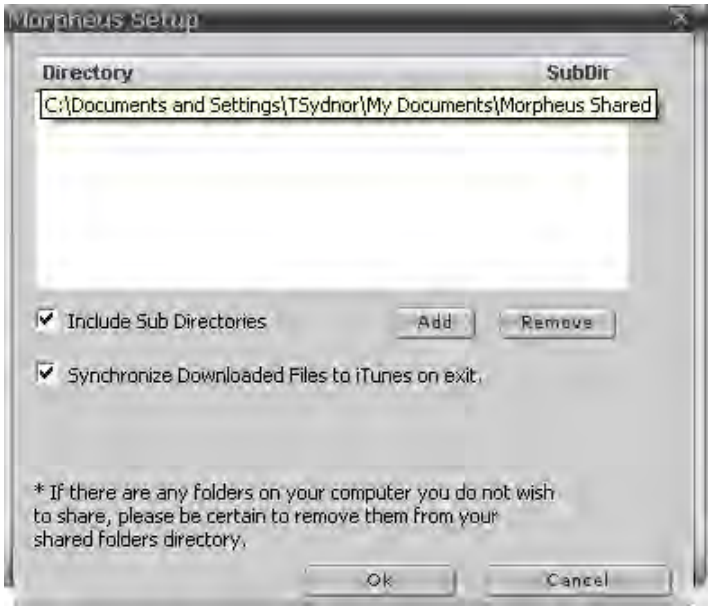


Figure 15: Morpheus 5.1.2

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:

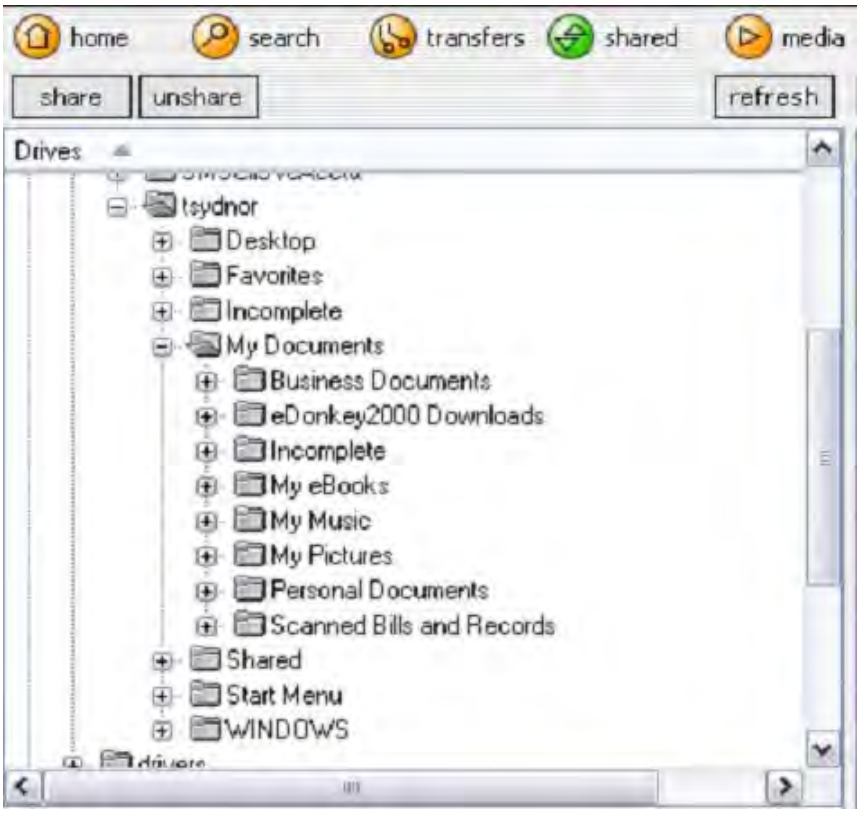


Figure 21: eDonkey 1.4.3

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:

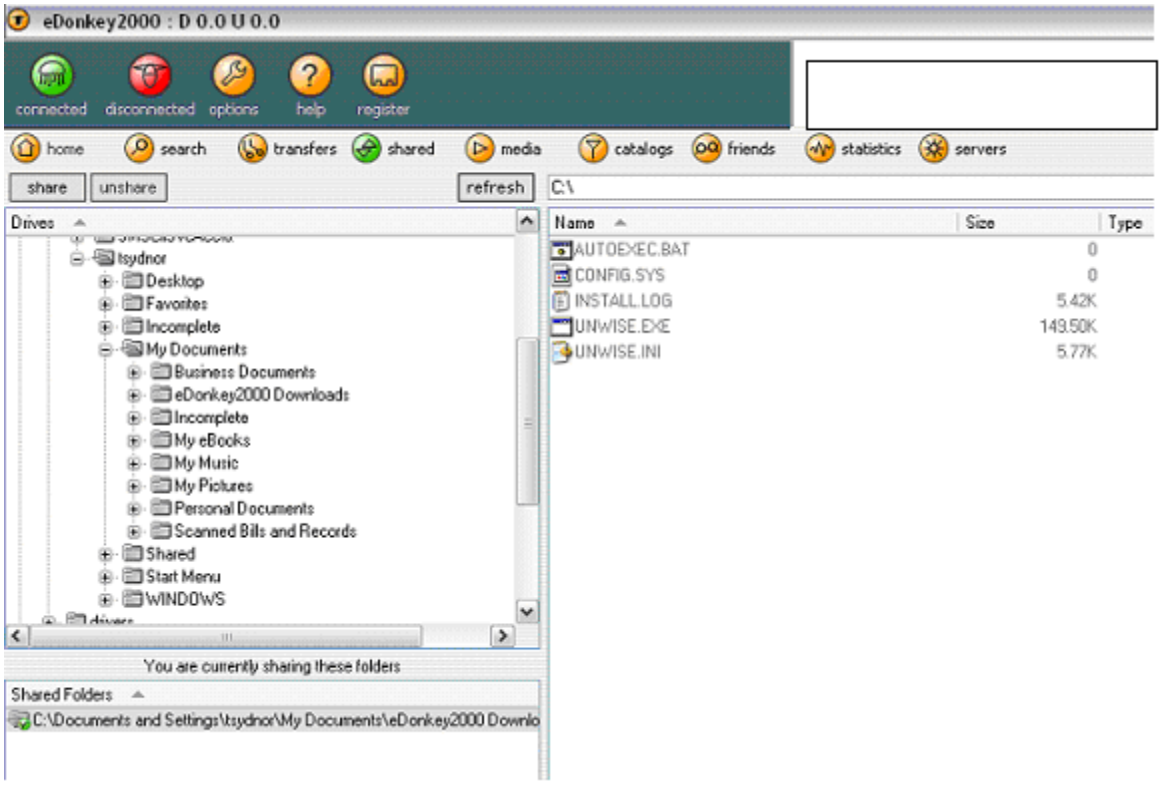


Figure 22: eDonkey 1.4.3

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:

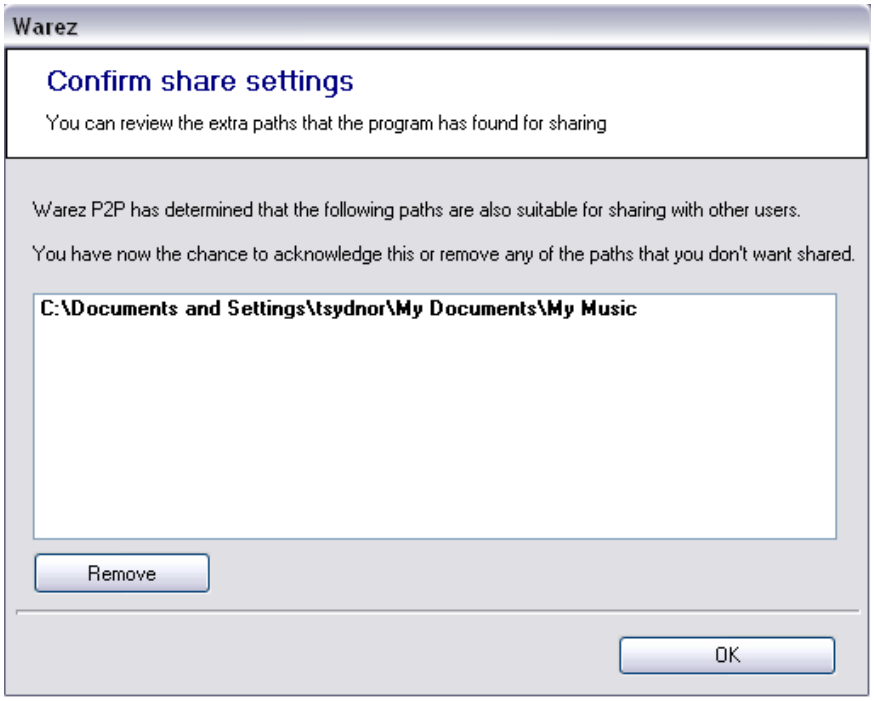


Figure 23: Warez P2P 2.9.5.3040

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").

THE PROGRESS & FREEDOM FOUNDATION

Progress on Point

Release 14.22 October 2007 **Periodic Commentaries on the Policy Debate**

Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform

by Thomas D. Sydnor II, John Knight, and Lee A. Hollaar *

Background

On March 5, 2007, the United States Patent and Trademark Office released a report on inadvertent filesharing entitled *Filesharing Programs and "Technological Features to Induce Users to Share"* (the "USPTO Report").[1] Based on public data, the USPTO Report concluded that (1) distributors of popular filesharing programs had deployed at least five features that were known would cause users to share files inadvertently, and (2) these features may have been intended to cause inadvertent sharing because (a) they became more prevalent and more aggressive after they were known to cause inadvertent sharing, and (b) they were deployed in waves—new "features" appeared as users learned to disable those previously deployed. In the summer of 2007, the House Committee on Oversight and Government Reform gave the distributors of LimeWire two chances to respond to these concerns.

On June 19, 2007, the House Committee on Oversight and Government Reform sent a letter, (the "Committee's Letter"), to LimeWire LLC. It asked LimeWire to respond to nine questions and to the USPTO Report. On July 5, 2007, LimeWire gave the Committee a 47-page response consisting of cover letter, a response to the nine questions, an Appendix on the USPTO Report, and a "Walkthrough" of inadvertent sharing precautions in LimeWire (collectively, the "Response"). On October 17, 2007, the Chairman, Ranking Member, and 17 other members of the Committee sent a public letter to the Federal Trade Commission that called for an investigation of inadvertent filesharing and attached LimeWire's Response.

---

* Thomas Sydnor is a senior fellow and director of the Center for the Study of Digital Property at The Progress & Freedom Foundation. Lee A. Hollaar is a professor at the School of Computing at the University of Utah. John Knight is a student at the University of Utah pursuing a master's degree in computer science; he currently assists professor Hollaar as a graduate research assistant and holds a J.D. and MPA from the University of Utah.

[1] Thomas D. Sydnor II, John Knight, Lee A. Hollaar, *Filesharing Programs and "Technological Features to Induce Users to Share"* (USPTO, 2006) (http://www.uspto.gov/web/offices/dcom/olia/copyright/oir_report_on_inadvertent_sharing_v1012.pdf). While the authors of this analysis also authored the USPTO Report, the opinions and conclusions presented here are those of the authors, not USPTO.

Next, on July 24, 2007, the Committee invited Mark Gorton, CEO of LimeWire LLC, to testify at its hearing, "*Inadvertent Filesharing over Peer-to-Peer Networks*."[2] Mr. Gorton was shocked by the extent and consequences of inadvertent sharing: "I had no idea that there was the amount of classified information out there or that there were people who are actively looking for that and looking for credit card information." *Transcript,* at 19. "I think I've always felt that it was inexperienced users who didn't know what they were doing. However, when you see documents coming from people who specialize in computer security about, you know, military documents, it really makes you think twice." *Id.* at 20. Mr. Gorton also said that—now that he understood the prevalence and consequences of inadvertent sharing—LimeWire would remediate it: "I absolutely want to do everything in my power to fight inadvertent file-sharing. And I am sorry to say that I didn't realize the scope of the problem…." *Id.* at 22.

To assist further investigatory efforts by the Committee, the FTC, and other law-enforcement agencies, we analyzed LimeWire's Response to the Committee's letter and its response to the Committee's hearing in order to answer two questions.

- *First*, does data provided in LimeWire's Response to the Committee's letter show that it did not deploy the five problematic "features" discussed in the USPTO report or reveal credible, good-faith explanations for why it did deploy such features?

- *Second*, during the three months since the Committee's hearing, has LimeWire done "everything in [its] power" to implement changes to its program that would significantly reduce or eliminate inadvertent sharing?

We conclude that the answer to each question is "No." LimeWire's Response to the Committee's Letter identifies no material defects in the USPTO Report's analysis or conclusions. Nor are the changes that LimeWire made after the hearing likely to significantly reduce or eliminate inadvertent sharing: Once again, LimeWire has "improved" its program in ways that *perpetuate* inadvertent sharing.

LimeWire's Response to the Committee's Letter and the USPTO Report

LimeWire's Response includes answers to the Committee's questions, an Appendix, and a "Walkthough" that overlap significantly. Consequently, a point-by-point analysis of each of its claims would bury and disperse information about the five problematic features discussed in the USPTO Report. This analysis will thus focus on those features, and discuss them in the order presented in the USPTO Report. It will focus, in particular, on the most disturbing features deployed in LimeWire: Share-folder and search-wizard features like those condemned in the 2002 study *Usability and*

[2] A video of the hearing and copies of the witnesses written statements are available on the Committee's web site at http://oversight.house.gov/story.asp?ID=1424. A transcript is also available. *See* Federal News Service, *Hearing of the House Oversight and Government Reform Committee, Inadvertent File-Sharing over Peer-to-Peer Networks* (July 24, 2007) [hereinafter Transcript at __].

Privacy and the Committee's May 15, 2003 hearing.[3] These features can cause catastrophic inadvertent sharing that results in emptied bank accounts, lost jobs, *and* a copyright-infringement lawsuit. Moreover, their risks were detailed in *Usability and Privacy* and the 2003 congressional hearings that led LimeWire to adopt the *Code of Conduct* that should have precluded their use.

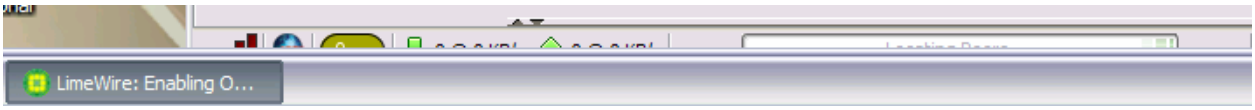
1. LimeWire's Redistribution Feature.

The USPTO Report (pp. 14-15) criticized LimeWire for replacing its once-useful main-interface display of the number of files a user was sharing, "Sharing 42 files" with a cryptic number, "42." LimeWire's Response (p. 9, Fig. 8 & p. A8, FigA7) claims that a user hovering a mouse pointer over the number will see a tooltip explaining its meaning, "You are sharing 42 files."

This claim surprised us: We had never seen a floating (or clickable) tooltip in LimeWire 4.10.9. Then we re-examined Figure 8 in the Response. In Windows, programs can run in full-screen mode or in "windowed mode," (in a smaller window occupying only part of the screen). Figure 8 shows LimeWire running in windowed mode, and the tooltip appears *below* the window running LimeWire.

Because newer users are likely to do so, we ran LimeWire in full-screen mode. This made the tooltip *invisible*: It "appeared" behind the Windows "Start" menu. This is what we saw when "hovering" a mouse over the cryptic number:

On another computer, we could get the tooltip to appear on-screen, but on this computer, LimeWire looked like this in windowed mode:



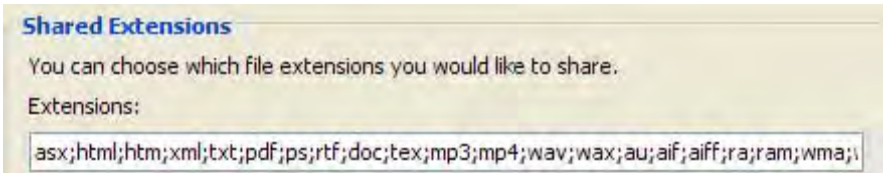
In any case, these screenshots, and Figure 8 of the Response, undermine LimeWire's claim, (p.A7), that the clarifying information in the tooltip was removed from the main screen, "with screen real-estate constraints in mind." In the horizontal bar in which the cryptic number appears, "screen real estate" is available, and unused.

Moreover, while we have not scrutinized them all, other screenshots in the Response also showed the Committee information hidden from most LimeWire users.

---

[3] *See* 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 [hereinafter, *Usability,* at __]; *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. *passim* (May 15, 2003) [hereinafter, *Overexposed,* at __]

For example, the "Shared Extensions" window in Figure 6 of the Response, (p. 8), indicates that users opening LimeWire's "Sharing" menu will see that ".doc" and ".pdf" files will be shared by default:



But this is wrong. When important data cannot be completely displayed on-screen, programs usually warn users, as shown by the ellipses, (…), in Figures 4 and 9 of the Response, (pp.6, 10). But the "Shared Extensions" window in Figure 6 *does not* warn that it displays only 16% of the file types LimeWire shares by default. Worse yet, if users guess this, click into the window, and try to see if other file types are shared, most will scroll to the *right* because they read information from left-to-right. Doing so will indicate that "Shared Extensions" window displays all file types shared by default. Only if LimeWire users scroll to the *left,* (for about 15 seconds), will they learn that LimeWire shares ".doc" and ".pdf" files by default.

2. LimeWire's Share-Folder Features.

The Committee's Letter asked LimeWire to "explain why warnings which were included in previous versions of LimeWire, which seem to have been intended to help users avoid inadvertent sharing, have been removed in more recent versions." The pop-up warnings referenced were displayed in the "Saving" menu of LimeWire 2.0.4, as shown in the USPTO Report (p.27, Fig. 10). These warnings, while imperfect, (*see id.* at p. 28 & n.35), did distinguish the "Save Directory" in LimeWire 2.0.4 from the KaZaA share-folder feature criticized by *Usability and Privacy* and the Committee because they (1) warned that a folder storing downloaded files would be shared; (2) let the user chose *not* to share this folder; and (3) warned that this folder, if shared, would be shared *recursively,* (all of its subfolders would also be shared).

LimeWire's Response, (p.11), claims that these warnings were never removed: "[C]urrent versions do include a warning…. We are not aware of a time when warnings were not included; if these warnings were ever omitted from a released version, the exclusion was due to a bug that was quickly fixed." These claims reflect "the recollection of the developers," (p.A10).[4]

The USPTO Report, (p. 23-26 & Figs. 8-10), shows that the share-folder feature in 4.0.7, a 2004 version of LimeWire displayed no such warnings. LimeWire thus seems to claim that it does not "recall" that the share-folder feature in LimeWire 4.0.7 lacked pop-up warnings, but if so, this was "due to a bug that was quickly fixed."

[4] LimeWire later claims, (Response, p.A4), that one of these developers cannot correctly describe the behavior of 2006 versions of LimeWire.

LimeWire's recollections appear to be wrong. Public data indicates that the pop-up warnings displayed in LimeWire 2.0.4 were removed from LimeWire in June of 2003. For the next two years, its share-folder feature displayed *no* pop-up warnings. Nor have the LimeWire 2.0.4 warnings *ever* reappeared. *Different pop-up warnings* did appear in LimeWire 4.9.0 and later. But these warnings can mislead users about LimeWire's most dangerous behavior: Its recursive sharing of all subfolders of a shared folder.

a. From June of 2003 to June of 2005, LimeWire's share-folder feature did not warn users that a "Save Directory" would be shared, or shared recursively.

The USPTO Report (pp. 23, 25; Figs. 6, 8-9), displayed the share-folder feature in LimeWire 4.0.7 because it behaved like other studied versions of LimeWire released from June of 2003 to June of 2005. Because LimeWire does not "recall" that these versions behaved like 4.0.7, we re-verified our analysis using available public data.

As LimeWire CEO Mark Gorton noted in a recent interview with *IEEE Spectrum*, many versions of LimeWire are available on the Web—collections are housed at sites like www.oldversion.com. We thus were thus able to download and run copies of the following versions of LimeWire: 3.0.2; 3.4.4; 3.6.15; 3.8.6; 4.0.7; 4.4.5. We also re-checked screenshots of the share-folder feature in 4.8.0.[5]

No pop-up warnings appeared in any copy of any of these versions of LimeWire. Consequently, we again conclude that available public data indicates that *no version* of LimeWire released from June of 2003 to June of 2005 displayed *any* warning when a user activated its share-folder feature. The behavior of LimeWire 4.0.7 appears to be neither atypical nor "due to a bug that was quickly fixed."

b. Since June of 2005, one of LimeWire's share-folder features and its "Sharing" menu displayed potentially misleading warnings.

LimeWire, (p.2), cites several "newly added" warnings that it claims prevent inadvertent sharing. But these warnings were "added" two years ago. This raises a question: Why does LimeWire keep causing catastrophic inadvertent sharing? Two factors may explain why these recent warnings fail to prevent inadvertent sharing.

First, the USPTO Report, (p.33), criticized LimeWire for implementing anti-inadvertent-sharing measures in ways that denied their benefits to users upgrading from the past versions of the program that had necessitated such measures. Consequently, the vast majority of LimeWire users who had once used pre-4.9.0 versions of LimeWire would not benefit from more recent changes in the program: Their sharing settings were not be rechecked or reset, so they would never see the warnings—even if they are

[5] Because LimeWire is an open-source program, we should have been able to cross-check public data by compiling executable copies of older versions of LimeWire from the code stored in LimeWire's Concurrent Versioning System (CVS) depository. Unfortunately, the data needed to compile versions of LimeWire prior to 4.13.1 appears to have been removed from LimeWire's public CVS depository.

sharing a "sensitive" folder like "Documents and Settings."

Second, the more recent warnings LimeWire cites differ from the warnings in LimeWire 2.0.4 in two ways: (1) they do not disclose that sharing a given folder will recursively share all shareable files in all of its subfolders, and (2) most indicate that sharing *will not be recursive*—that the user will share only "this folder," the one selected through a share-folder feature or displayed in a pop-up sensitive-folder warning.

We will address below LimeWire's unsubstantiated claim that "[r]ecursive sharing is the behavior that most experienced computer users expect." For now, even were this claim relevant and accurate, recursive sharing would still cause inadvertent sharing if a program that shares folders recursively indicates that it does not.

(1) The share-folder feature in LimeWire's setup process indicates that sharing will *not* be recursive.

Since June of 2003, LimeWire has deployed a share-folder feature in its setup process. This share-folder feature will be encountered mostly by new users installing LimeWire for the first time—by those who are least likely to understand LimeWire and its capabilities. It is shown in LimeWire's Walkthrough (p. 9, Fig. 10).

It displays the default "Shared" folder and lets the user choose to store downloaded files in a different folder. Unlike the share-folder feature and "Sharing" menu within LimeWire, this share-folder feature displays *no* pop-up warnings: Users cannot avoid sharing a selected folder, and they will not be warned if they select a "sensitive" folder.

Worse yet, while the feature does disclose that a folder selected as the download folder will be shared, it also indicates—wrongly—that sharing will *not* be recursive: "*This folder* will also be shared…." (emphasis added). This wording is inexcusable: *Usability and Privacy* warned, five years ago, "The word "folder" is singular, implying one folder, and does not hint that all folders below it will be recursively shared with others." *Usability*, at 140.

(2) The pop-up warning in LimeWire's internal share-folder feature fails to disclose recursive sharing.

LimeWire's Response, (p. 6), claims that its internal share-folder feature will display a pop-up "recursive-sharing warning." This claim is facially wrong: When LimeWire disclosed recursive sharing, it did so as follows: "Subfolders of shared folders will also be shared." USPTO Report p. 28, Fig. 11. It used similar language in its 2.0.4 pop-up warnings. *Id.* at 27, Fig.10. The Response, (p.6, Fig. 4), shows that no similar language appears in more recent pop-up warnings.

It thus appears that LimeWire claims that LimeWire 4.12.15's share-folder feature discloses recursive sharing because its warning refers to "your new save folders." That

"s," LimeWire seems to claim, informs even young or inexperienced users that storing downloaded files in a "Documents and Settings" folder that contains no existing files will recursively share the data files of all users of that computer.

The Response, (p.6, Fig. 4), reveals the flaw in this claim. LimeWire has altered its share-folder feature so users can select *multiple* "download locations" for different types of files: Users can now store downloaded audio files in "My Music," documents in "My Documents," and image files in "My Pictures." As a result, the share-folder feature that used to recursive share only *one* folder per use can now recursively share up to *six* folders per use. Indeed, the Response (Fig. 4) shows a user being asked whether they want to share *two* "new save folders" as a result of one use of the share-folder feature.

Users could thus reasonably conclude that the "s" in "new shared folders" reflects this new multiple-folder-sharing capability, not that shared folders would be shared recursively. In any case, LimeWire's Response cannot reasonably claim that recursive sharing can be effectively disclosed through warnings more opaque than those given in the search-wizard feature that it eliminated because it had "the potential to be misused by inexperienced users," (p.5).

(3) The sensitive-folder warning in LimeWire's "Sharing" menu indicates that sharing will not be recursive.

LimeWire's Response, (p. 2, 9), repeatedly touts pop-up "sensitive-folder" warnings that will appear if someone using LimeWire 4.12.15's "Sharing" menu tries to share a folder likely to contain sensitive data. While such warnings could be helpful, the Response overlooks three factors that, collectively, may make these sensitive-folder warnings misleading.

First, sensitive-folder warnings could mislead w they provided inconsistently. The list of "sensitive" folders in the Response, (p.2), contains two obvious omissions:

- "My Music": Most media players save files ripped from CDs in subfolders of "My Music." Sharing "My Music" would thus cause many or most users to share thousands of infringing audio files and become targets for lawsuits.

- "My Pictures": Many digital cameras will store photographs in subfolders of "My Pictures," and many scanners or multifunction printers will also store scanned documents, (like bank statements or tax records), in subfolders of "My Pictures."

Second, four interfaces in LimeWire 4.12.15 will share folders: (1) the "Sharing" submenu of its Options menu; (2) the "Saving" submenu of its Options menu; (3) its "Library" interface; and (4) the share-folder feature in its setup process. The sensitive-folder warnings appear *only* if folders are shared through the "Sharing" submenu: In the Library, a user receives no warning if he shares "Documents and Settings," (and thus recursively shares the "My Documents" folders of all users of that computer).

Third, the sensitive-folder warning does not disclose that a "sensitive" folder will be shared recursively. Indeed, the warning indicates, (p.9, Fig.7), that sharing *will not be recursive*: "You are attempting to share *a* folder that is likely to contain sensitive information… Share *this* folder?" (emphasis added). This could easily mislead users. For example, *recursive* sharing of a "Documents and Settings" folder will be disastrous, but users who think that sharing is non-recursive could examine their "Documents and Settings" folder and find that "this folder" contains no sensitive files.

For all of the above reasons, LimeWire 4.12.15 appears to be neither the version most compliant with LimeWire's *Code of Conduct* nor the version least likely to cause inadvertent sharing. This seems attributable to LimeWire's instance that recursive sharing, (p.12), "is the behavior that most experienced computer users expect." No supporting evidence is cited, but the Response seems to claim, (p.6), that because selecting a folder in Windows Explorer will recursively select its subfolders, then "most experienced computer users" will expect filesharing programs to share folders recursively. For several reasons, this claim is both irrelevant and wrong.

LimeWire's claim is irrelevant because many or most users of filesharing are not experienced computer users. Many are teenagers or pre-teen children who may be neither experienced nor safety-conscious. As the USPTO Report notes, (p.8), LimeWire itself has referred to users of filesharing programs as "the Munchkins" and "the little guys."

LimeWire's claim also appears to be wrong. As the Response notes, (p.A5), users of filesharing programs may not expect them to behave like computer operating systems or any "other class of software." The consequences of selecting folders in Windows differ profoundly from those of "sharing" whole trees of folders and files with thousands of anonymous strangers. Users need not—and should not—expect the latter act to be no more difficult than the former.

Moreover, five years ago, *Usability and Privacy* warned that filesharing programs should *not* share folders recursively: Recursive sharing—even if disclosed—imposes upon users a burden that too many will be unable to bear: Even if users *do know* that sharing will be recursive, they can assess its implications only if they have "detailed knowledge" of (1) what types of files a given program will share, (2) the structure of their folder hierarchy and (3) the contents, locations, and sensitivity of all files it contains. *See Usability,* at 140. If most users possessed this detailed structural and substantive knowledge, Windows would not contain a file/folder search system—and filesharing programs would not have contained search-wizard features.

During the five years since *Usability and Privacy* was published, LimeWire has been testing its contrary theories about the obviousness of recursive sharing on the public. The results of its experiments spoke for themselves during the Committee's hearing.

3. LimeWire's Search-Wizard Feature.

LimeWire's Response to the Committee's question about its search-wizard feature is unhelpfully vague. The Response admits, (pp. 5, 14, A8), that LimeWire did deploy—but has "recently" stopped deploying—a search-wizard feature. It does not disclose when it was first deployed or when it was removed.

We have thus reviewed public data to provide more information. We first found a search wizard in LimeWire 3.8.6, released in February of 2004. We found it in each subsequent studied version through 4.12.12, which was available in June of 2007. LimeWire thus deployed a search wizard for about 3½ years. In all studied versions, the search wizard tended to "recommend" recursive sharing of the user's "My Documents" folder and all of its subfolders—the user's "principle data repository."

This search-wizard feature did not differ materially from the KaZaA search-wizard features condemned by *Usability and Privacy* and the Committee. In some ways, it was slightly worse: Unlike the KaZaA wizard, it would be triggered by default during setup, and the LimeWire wizard told users that it would search for "media files"—the Response now admits, (p.A8), that this was wrong. In other ways, it was slightly better: It did disclose that selected folders would be shared recursively—but as the Response concedes, (p.5), this failed to eliminate its "potential to be misused by inexperienced users." In the end, LimeWire had to do what KaZaA did in 2003: Remove the search wizard from its program.

LimeWire states, (p.5), that the *Code of Conduct* it drafted, published, and promoted in 2003 imposed "common-sense" obligations. While we agree, those obligations also responded to two specific problems—share-folder and search-wizard features—identified in *Usability and Privacy* and the Committee's 2003 hearing. Nevertheless, LimeWire's Response, (p.2), claims "strict adherence" to the *Code* while the search wizard was deployed.

We disagree. LimeWire's *Code* required that its program be designed "to reasonably prevent the inadvertent [sharing] of the contents of the user's … principle data repository." For about 3½ years, LimeWire tended to recommend that new and inexperienced users recursively share their "My Documents" folders. A program does not "reasonably prevent" sharing of a "principle data repository" by recommending that users share it. Nor does a "reasonably designed" program make "recommendations" that would be unreasonable for almost any user to accept.

Nor can we understand why any distributor of a filesharing program would keep deploying a search wizard three years *after* identifying it as a cause of catastrophic inadvertent sharing. In August of 2004, a reporter asked LimeWire's Chief Operating Officer why users of LimeWire were inadvertently sharing classified military documents. In response, he cited the search wizard: "One possible weakness in LimeWire is a feature that automatically scans the user's hard drive, looking for files to be shared over the network. [LimeWire's COO] said this feature can make it easy to expose private

information by mistake."[6] Nevertheless, LimeWire kept deploying the search wizard for nearly three more years.

4. LimeWire's Partial-Uninstall Feature.

LimeWire's Response provides an incomplete and potentially misleading answer to the Committee's question, "How can users completely uninstall the LimeWire program without leaving behind files that might affect subsequently installed versions of its program?" The instructions given, (p.12), will not work for users of *most* versions of LimeWire and they omit a key detail that makes them useless to users of the most recent versions of LimeWire. These instructions are flawed because they do not disclose a critical change in LimeWire's partial-uninstall feature.

In studied versions of LimeWire from mid-2003 through mid-2006, the datafile used by the partial-uninstall feature was stored in a *visible* folder called ".limewire" located in C:\Documents and Settings\[username]. Deleting this folder would disable the partial-uninstall feature.

Recently, LimeWire *relocated* the relevant datafile. LimeWire 4.12.15 stored it in a subfolder within the user's "Application Data" folder. By default, the "Application Data" folder is a *hidden folder*: Users can neither see that it exists nor delete any of its subfolders. In short, LimeWire recently changed its partial-uninstall feature in a way that prevents even users who *once* knew how to disable it from doing so again.

The rest of LimeWire's explanations for its partial-uninstall feature are not credible. First, it argues that this is an "industry standard" (p.12). But "others were doing it" is no answer—particularly in an industry that pledged to provide "a method by which [its] software may readily be uninstalled."

Second, it argues that saving user-defined settings can make it easier for users to upgrade to new versions of a program (pp. 12, A11). No one disputes that user-defined settings can be retained when a *presently installed* version of a program is upgraded to a new version.[7] Nor does anyone assert that all programs must delete all user-defined settings when uninstalled. Problems like those caused by partial-uninstall features arise only if (1) non-deleted user-defined settings could have potentially dangerous consequences, and (2) a program was specially designed to re-use—rather than overwrite—any non-deleted datafiles containing those potentially dangerous user-defined settings.

If a program does this, then no one can predict the consequences of installing it on a computer. LimeWire's Response states (p.6): "No files are marked for sharing

[6] Hiawatha Bray, File-Sharing Imperils US Secrets, The Boston Globe (Aug. 4, 2004) (http://www.boston.com/business/technology/articles/2004/08/05/file_sharing_imperils_us_secrets/).

[7] The Report notes, however, that if a distributor alters its program because potentially dangerous or misleading features deployed in previous versions caused inadvertent sharing, then user-defined settings *should be* reset or re-confirmed. If this is not done, the "improved" program will perpetuate the effects of previous errors. USPTO Report at 33. LimeWire's Response did not dispute this point.

unless the user has explicitly chosen that file, a folder containing that file, or a folder containing a parent folder of that file…; or the user has initiated a download of the file." At the hearing, Mr. Gorton said, "[T]he defaults are secure. So if you hit enter, enter, enter using LimeWire, you don't share any files and—there is no information that would be on your computer that would be made public to anybody." *Transcript,* at 19. LimeWire's partial-uninstall feature makes such statements dangerously wrong.

Finally, LimeWire's Response claims (pp. A10-A11) that while its partial-uninstall feature could reinstate settings *more* dangerous than the usual defaults, it might also perpetuate settings *less* dangerous than the defaults: "[I]f the previous user had wanted complete privacy and prevented all sharing, then LimeWire would automatically perpetuate that privacy and continue not sharing." Wrong again: As discussed below, LimeWire's "Individually Shared Files" feature ensures that any lucky user who unwittingly inherits settings that *once* "prevented all sharing," will begin sharing as soon as they begin downloading.

5. LimeWire's "Individually-Shared-Files" Feature.

LimeWire's Response, (pp. 12, A3), repeatedly denies that its Individually-Shared Files (ISF) feature is a coerced-sharing feature. But its alternative explanation for this feature cannot explain its behavior. LimeWire claims, (p.A11), "ISF was added along with the 'Download As' feature, to allow a user to save a download to an arbitrary location." But LimeWire will tag downloaded files as "Individually Shared Files" even if they were *not* downloaded using its "Download As" feature. LimeWire has thus failed to offer any credible alternative to the explanation proposed in the USPTO Report (pp. 35-36, 44-45): ISF is a form of coerced-sharing feature implemented because too many LimeWire users had learned how to stop sharing files.

6. Other Issues.

Only one other issue in LimeWire's Response bears note: It persistently reveals a troubling attitude toward LimeWire users and the problem of inadvertent sharing. In 2003, distributors of filesharing programs that had caused inadvertent sharing acknowledged their duty to protect their users. One told the Committee, "I firmly believe that it is the responsibility of peer-to-peer file-sharing companies to proactively protect the privacy and security of the users of their software application." *Overexposed* at 59.

LimeWire's Response, (A10), displays a different attitude toward users and their safety: "LimeWire recognizes that a file-sharing program's purpose is to share files, and has stated that it found it odd when people complain about files being shared by such programs." Similar statements litter the Response, (pp. 1, 13, A5, A6). LimeWire thus portrays inadvertent sharing as a stupid-user problem to be blamed on "ill informed," "careless," "inexperienced," "negligent," users who "drive[] software developers crazy" (pp. 1, 5, 13, A9).

For example, the USPTO Report, (pp. 25-26), showed why a user who had inadvertently shared thousands of legally acquired audio files via the share-folder

feature in LimeWire 4.0.7 might think that the sharing caused by that feature could be cured by clicking the provided "Use Default" button that *seems* to restore its default setting. LimeWire's Response, (p.A8), belittles the user who fails to realize that in LimeWire, sharing caused by one menu must be corrected in a different menu: "[T]his is an example of precisely the sort of user who drives software developers crazy…. In this case the user navigates to an option titled "Saving" instead of the option titled "Sharing" when that user wishes to change what is being shared."

But the problem illustrated resides in the *program,* not the user. Ordinarily, no one would think that a "Saving" menu dedicated to the saving of files would affect the sharing of folders. In LimeWire, it does. When "saving" causes "sharing," it is reasonable to expect a user who discovers this—and thus realizes that she has shared sensitive *folders* by changing the default setting for *saving* files—to return to the menu that caused the problem and click its "Use Default" button to restore its default setting.

Unfortunately, this attitude that pervades LimeWire's Response is still evident in its program: Today, users of LimeWire 4.14.10 who try to halt inadvertent sharing of recursively-shared "Save Directories" by using its share-folder feature's "Use default" button will receive the same potentially misleading feedback that users of LimeWire 4.0.7 received in 2004.

LimeWire's Response to the Committee's Hearing

Because LimeWire's CEO testified under oath at the Committee's hearing that he would "do everything in my power to fight inadvertent sharing," *Transcript,* at 22, LimeWire could hardly fail to make some improvements during the next three months. The critical question is thus whether LimeWire has made *meaningful* changes that will significantly reduce inadvertent sharing.

As of this writing, the current version of LimeWire Basic is 4.14.10. To determine how it has changed, we compared its behavior to that of LimeWire Basic 4.12.15, the last version that we downloaded before the Committee's hearing.

One change in 4.14.10 could have been meaningful: When users share folders through its "Saving," "Sharing" and "Library" interfaces, they will see a pop-up warning that displays a graphic representation of the folders and some of the subfolders that will be shared and they can alter or cancel their actions.[8] While imperfect, these graphic pop-up warnings could have prevented some inadvertent sharing: But *not* if they were implemented in a way that tended to deny their benefits to users upgrading from previous versions of LimeWire *and* to users installing LimeWire for the first time.

Regrettably, that is how they were implemented.

[8] Unfortunately, these new warnings can also provide misleading feedback. If a user "deselects" a folder that would be shared, the warning will provide feedback indicating that it will not be shared. But if the user then selects one of its subfolders, the program will re-select for sharing all files stored in the parent folder that the user just chose not to share.

The new pop-up warnings will help few users of prior versions of LimeWire because LimeWire has again "improved" its program by *perpetuating* most inadvertent sharing caused by prior versions. LimeWire's popularity ensures that the vast majority of 4.14.10 users will be upgrading from past versions of LimeWire that caused inadvertent sharing. These users will not benefit from the "improvements" in 4.14.10. For example, if a user of LimeWire 4.12.3 recursively sharing her "Documents and Settings," "My Documents" or "My Music" folder, then that "preference" will be perpetuated when she upgrades to LimeWire 4.14.10: Her file-sharing preferences will not be re-checked or reset; nor will she see its new graphic pop-up warnings.

A section of the USPTO Report, (pp. 33-35), criticized distributors—like LimeWire—that had denied the benefits of new anti-inadvertent-sharing features to users upgrading from prior versions that caused the inadvertent sharing that necessitated such features. LimeWire's Response did not dispute this criticism, which was intended to ensure that no distributor could credibly "play dumb" if it repeated such conduct. This appear-to-improve-but-perpetuate tactic is shopworn: In 2003, the distributors of KaZaA did get away with perpetuating the effects of their search-wizard and share-folder features when they "improved" their program. Today, this tactic should not be overlooked—or excused—yet again.

LimeWire 4.14.10's new warnings are also unlikely to help new users installing LimeWire for the first time. These warnings *do not appear* in LimeWire's most dangerous interface: The undisclosed, recursive-sharing share-folder feature that LimeWire's setup process displays to new users—the one that falsely suggests that sharing will *not* be recursive. The USPTO Report, (25 & n.31), repeatedly criticized this feature. So have others. After the Committee's hearing, the pro-filesharing web site Slyck tried to defend LimeWire by publishing *Sharing for Dummies,* a guide to avoiding inadvertent sharing.[9] It identified the setup-process share-folder feature as the place "where people **get themselves and their organizations in trouble.**" Slyck then highlighted some of its defects by annotating screenshots of it with large text balloons that display critical information that the feature itself does not. LimeWire has thus incorporated its graphic pop-up warnings into *some* sharing-related interfaces, but not into the one most dangerous to new or inexperienced users. That is inexcusable.

Finally, not only have LimeWire's graphic pop-up warnings been implemented in a way that will not benefit many new or existing users, LimeWire has also failed to take other obvious steps "to fight inadvertent sharing."[10] The following illustrate some of the problematic behaviors still present in LimeWire 4.14.10:

---

[9] Thomas Mennecke, *Sharing for Dummies,* SLYCK.COM (July 25, 2007) (http://www.slyck.com/story1550_Sharing_for_Dummies)

[10] LimeWire has made another long-overdue change: It no longer allows recursive sharing of the root directory "C:\." Programs like BearShare implemented a similar precaution about four years ago.

- All its sharing-related interfaces recursively share subfolders of selected folders.
- Its partial-uninstall feature still makes its default behavior so unpredictable that neither LimeWire's Response nor its CEO can correctly describe it.
- Its Individually-Shared-Files (ISF) feature still tags all downloaded files as ISFs, forcing users who want to stop sharing downloaded files to complete a complex, multi-step process across multiple interfaces.
- It no longer displays the "Sensitive Folder" warnings repeatedly cited in LimeWire's Response.
- Its "content filter" is still optional, and disabled by default.
- The "Use Default" button on its "Saving" interface still provides potentially misleading feedback.
- By default, it still shares downloaded files, partially downloaded files, and torrent files not licensed for distribution over the Gnutella network.
- The interface that lets users view and change the types of files that LimeWire shares is now even more difficult to find.
- Its main interface displays only a cryptic number to disclose the number of files shared, and the clarifying tooltip still displays off-screen on some computers.

In summary, LimeWire's Response to the Committee's letter and its response to the Committee's hearing have failed either to redress the concerns expressed in the USPTO Report or to show significant progress in reducing or eliminating inadvertent sharing. As a result, the critical conclusion expressed in the USPTO Report, (47-48), stands: Law-enforcement agencies should investigate to determine whether distributors of popular file-sharing programs intended to blunt the deterrent effects of copyright-enforcement actions by duping users of their programs into sharing files inadvertently.

The Progress & Freedom Foundation ■ 1444 Eye Street, NW ■ Suite 500 ■ Washington, DC 20005
voice: 202/289-8928 ■ fax: 202/289-6079 ■ e-mail: mail@pff.org ■ web: www.pff.org

THE PROGRESS & FREEDOM FOUNDATION

Progress on Point

Volume 16, Issue 14 **July 2009**

Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5

by Thomas D. Sydnor II

Executive Summary

For nine years, popular "peer-to-peer" file-sharing programs used almost exclusively for *illegal* purposes (like infringing copyrights) have caused users to "share" files (like tax returns) that no one would intentionally offer to anonymous strangers. The resulting problem has been called "inadvertent sharing."

But now, LimeWire LLC claims that LimeWire 5 has "put the final nail in the coffin of inadvertent sharing of sensitive files," by implementing certain *Voluntary Best Practices. Indeed, LimeWire 5 has been hailed as the "poster child" for implementing these Best Practices.* For four reasons, this paper concludes that LimeWire 5 is a dangerous program that can both cause and perpetuate inadvertent sharing.

First, LimeWire 5 seems to be *intended* to cause *catastrophic* inadvertent sharing of *thousands* of a user's personal files. One mistaken click on LimeWire 5's dangerously ambiguous "share all" feature can publish *all* of the audio, video, image, and documents files in a user's "Library." LimeWire warns that a user's "Library" must never include "any folder… that contains personal information." But by default, LimeWire 5 will *automatically* include in a user's "Library" all of the documents, family photos, scanned documents, home movies and entire collections of popular music and movies stored in *My Documents* and its subfolders. This seemingly deliberate wrongdoing thus put millions of families one click away from multiple threats of financial ruin—or something worse:

> [C]hild… predators are actively searching P2P networks for personal photos of children and others that may be stored on private computers…. [T]hese individuals will [then]… download all additional information being shared from that computer…. This accompanying information can be used by the predator to locate… the potential victim.[1]

Tom Sydnor (tsydnor@pff.org) is a Senior Fellow and Director of the Center for the Study of Digital Property at The Progress & Freedom Foundation. The views expressed here are his own, and may not reflect the views of PFF staff, board members, or advisors.

[1] *See infra,* n.27.

No prior version of LimeWire inflicted such serious risks upon so many of its users and their families.

Second, "poster child" LimeWire 5 violated *at least eight* critical requirements imposed by the *Best Practices* that it supposedly implemented:

- LimeWire 5 can share User-Originated Files by default.
- LimeWire 5 shares User-Originated Files without timely and conspicuous warnings.
- LimeWire 5 shares "Sensitive File Types" by default—like the image files that store entire collections of scanned financial documents and family photos.
- LimeWire 5 recursively shares *folders* by default.
- LimeWire 5 does not uninstall completely.
- LimeWire 5 does not make users of prior versions "reconfirm" their "sharing selections."
- LimeWire 5 can "share" entire *networks* by recursively sharing *Documents and Settings*.
- LimeWire 5 gives no "prominent warning" to users sharing more than 500 files.[2]

Third, LimeWire 5 also perpetuates the Prey-on-the-Weak model of file-sharing reflected in prior versions of LimeWire and similar programs. New users of these programs are often preteen or teenage children. Nevertheless, these programs' default settings tend to be dangerous—and changing them can be more dangerous. Such programs thus ensure that *unsophisticated* children will tend to unwittingly "share" their downloaded files and, perhaps, their family's entire collections of media files. Not only can these Prey-on-the-Weak tactics endanger children and families, they can also grant reduced jail sentences to dangerous pedophiles—like the LimeWire user convicted for "sharing" the video of the rape of a little girl "bound with a rope and being choked with a belt by what appeared to be an adult male.'"

Fourth, LimeWire 5's alleged efforts to deter *infringing uses* of the LimeWire program—the only "major" uses of the LimeWire program—fail to rise even to the level of farce. They suggest that LimeWire intends to perpetuate infringement—not deter it.

LimeWire 5 thus confirms that *no one* can expect LimeWire to "put the final nail in the coffin" of inadvertent sharing. Indeed, inadvertent sharing may be *essential* to the success of file-sharing programs and networks that make "sharing" the files that most users want to download so dangerous that only the most zealous *or unsophisticated* users would do so. Officials who want to end inadvertent sharing should thus pursue a two-pronged strategy.

---

[2] *See* Distributed Computing Industry Association, *Voluntary Best Practices for P2P File-Sharing Software Developers To Implement To Protect Users Against Inadvertently Sharing Personal or Sensitive Data* (2008).

Civil and criminal referrals should be sent to the both the U.S. Department of Justice and interested State Attorneys General. These law-enforcement agencies possess the *civil* enforcement authority that could *quickly* remediate inadvertent sharing and the *criminal* enforcement authority needed if an entity like LimeWire LLC really did *intend* to trick users into "sharing" files unintentionally—even if the predictable collateral damage would include family finances "shared" with thieves, national secrets "shared" with terrorists, and the identities of children shared with dangerous pedophiles.

*C*ongress should also work with law-abiding technologists to revise H.R. 1319, The Informed P2P User's Act, to grant the Federal Trade Commission the substantive and remedial authority needed to stop distributors of Prey-on-the-Weak file-sharing programs from exploiting vulnerable users in order to sustain piracy-based "business models.[3]

Analysis

Inadvertent sharing has long been associated with implementations of "peer-to-peer" networking technologies that facilitate piracy-based business models.[4] For the past nine years, P2P file-sharing programs used mostly for unlawful purposes have caused too many of their users to "share" files *inadvertently*—even highly sensitive files that no one would *deliberately* share with the identity thieves, pedophiles, terrorists, and spies lurking on file-sharing networks.[5] The latest round of these disturbing incidents surfaced in early 2009.

---

[3] *MGM Studios, Inc. v. Grokster, Ltd.,* 454 F. Supp. 2d 966, 981 (2006) (noting that the distributors of the Gnutella-based Morpheus file-sharing program claimed that their business model gave them "the ability to get all the music" and "no product costs to acquire music.").

[4] *See, e.g., id.* at 985 (relying upon a study showing that 97% of the files selected for downloading by users of Gnutella-based file-sharing programs were, or were highly likely to be, infringing); Alexandre M. Mateus and Jon M. Peha, *Dimensions of P2P and digital piracy in a university campus*, (2008) (""Some might suggest that there are many people who use P2P [for lawful purposes] but do not engage in the illegal transfer of copyrighted material. However, we found no evidence of this among college students.").

[5] Studies of the causes and consequences of inadvertent sharing, in chronological order, include the following, Nathaniel S. Good & Aaron Krekelberg, *Usability and Privacy: A Study of KaZaA P2P File-Sharing* (2002) (causes) *reprinted in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, vol. 5, iss. 1 at pp. 137-144; Thomas D. Sydnor II, John Knight, Lee Hollaar, *Filesharing Programs and "Technological Features to Induce Users to Share,"* (US. Patent & Trademark Office 2007) (causes) [hereinafter, "*USPTO Report*"]; M. Eric Johnson, *Information Risk of Inadvertent Disclosure,* 25 J. OF MAN. INF. SYS. 97-123 (Fall 2008) (consequences); Thomas D. Sydnor II, John Knight, Lee Hollaar, *Inadvertent Filesharing Revisited* (PFF 2007) (causes); M. Eric Johnson, *Data Hemorrages in the Heath-Care Sector,* LECTURE NOTES IN COMPUTER SCIENCE (April 2009) (consequences). Congressional testimony by the security company Tiversa, Inc. also provides invaluable data on the *consequences* of inadvertent sharing. *See* Written Statement of Tiversa, *Legislative Hearing on H.R. 2221 and H.R. 1319 Before the Subcomm. on Commerce, Trade and Consumer Protection of the H. Comm. On Energy and Commerce*, 111th Cong. (May 5, 2009) [hereinafter *Boback II*]; Written Testimony of Tiversa, *Hearing on Inadvertent File Sharing on Peer-to-Peer Networks Before the H. Comm. on Oversight and Government Reform,* 110th Cong. (July 24, 2007) [hereinafter *Boback I*].

In late February of 2009, inadvertent file-sharing disclosed to Iran the plans for Marine One, President Obama's helicopter.[6] Today Investigates also published a report on inadvertent file-sharing that revealed that the citizens of New York State alone were "sharing" over 150,000 tax returns over "peer-to-peer" file-sharing networks used mostly to pirate popular music and movies.[7] This report thus suggests that, nationally, over 2,000,000 tax returns were being inadvertently shared in February of 2009—an enormous data-security problem. Today Investigates also profiled the Bucci family, whose daughters, by misconfiguring the LimeWire file-sharing program, inadvertently "shared" their parents' tax returns with identity thieves who stole the family's tax refund.

As a result of these, and other, reports, on April 20, 2009, the House Committee on Oversight and Government Reform, (the "Oversight Committee"), opened—*for the third time*—an investigation into why file-sharing programs like LimeWire *continue* to cause so many of their users to share files inadvertently.[8]

LimeWire LLC ("LimeWire") then responded to these new concerns about *more* egregious harms caused by inadvertent sharing. Indeed, it used them as a launching pad for a PR campaign for the *new* version of its program, LimeWire 5.[9] Three sets of actions followed.

First, LimeWire sent spokesperson Linda Lipman and Lime Group CEO Mark Gorton to reassure journalists and the public with statements like these:

> We've been diligent in working with our trade association and regulatory agency representatives to develop *and implement* [software upgrades] to protect users against inadvertent file-sharings….
>
> Our newest verision LimeWire 5.0, by default, cannot share sensitive file types such as spreadsheets or documents. *In fact, the software can not share any file or directory without explicit permission from the user*.[10]
>
> "LimeWire [5] has ensured the complete lockdown of the safety and security of LimeWire users," said [Lime Group Chairman Mark Gorton].[11]

---

[6] *See Boback II*, *supra* note 5, at 10.

[7] Today Investigates, *New warnings on cyber-thieves,* at http://today.msnbc.msn.com/id/26184891/vp/29405819%2329405819.

[8] *See, e.g.,* Letter from Chairman Towns, Ranking Member Issa, and the Hon. Mr. Welsh of the H. Comm on Oversight and Government Reform to Mr. Mark Gorton, Chairman, The Lime Group (Apr. 20, 2009).

[9] LimeWire uses the term "LimeWire 5" to refer to a series of newer versions of the LimeWire program including LimeWire 5.0.11, 5.1.1, 5.1.2, and 5.1.3. This paper's references to the behaviors of "LimeWire 5" refer to those of LimeWire 5.1.2 and 5.1.3. These were the current versions of LimeWire 5 when this analysis was prepared, and they do not seem to differ materially.

[10] Jack M. Germain, *Congress Squeezes LimeWire for Straight Talk on P2P Security,* TechNewsWorld (April 22, 2009), *at* http://www.technewsworld.com/story/66879.html?wlc=1244950408; Today Investigates, *LimeWire releases a statement* (Feb. 26, 2009), *at* http://today.msnbc/msn.com/id/29305054.

Next, LimeWire's trade association, the Distributed Computing Industry Association, ("DCIA"), announced that LimeWire 5 had implemented self-regulatory standards called the *Voluntary Best Practices for P2P File-Sharing Software Developers To Implement To Protect Users Against Inadvertently Sharing Personal or Sensitive Data* (the "*VBPs"*). DCIA then proclaimed that LimeWire 5 "served as a 'poster child for compliance'" with these *VBPs*, which had made inadvertent sharing "an increasingly outdated concern over a very specific feature [recursive sharing of sensitive file types] of a small number of applications…."[12]

Finally, LimeWire responded to the *third* opening of an Oversight Committee investigation into inadvertent sharing. On May 1, 2009, Lime Group CEO Mark Gorton sent the Committee a letter, (the "Gorton Letter").[13] The Gorton Letter is riddled with evasions and sweeping, bold claims. In effect, these bold claims assert that LimeWire 5 had already resolved any concerns about inadvertent sharing:

> "LimeWire is absolutely committed to helping protect our users against inadvertent filesharing.… LimeWire is absolutely committed to making changes to our software toward that end.… True to my word, LimeWire has absolutely done this.… LimeWire 5 culminates a concerted effort to combat and eliminate inadvertent file-sharing."
>
> "In LimeWire 5.0,… LimeWire fundamentally changed the way file sharing works. LimeWire started from the ground up and addressed the fundamental problems that led to inadvertent sharing.… With these changes, LimeWire 5 put the final nail in the coffin of inadvertent sharing of sensitive files."
>
> "LimeWire 5 was designed to prevent inadvertent file-sharing. Its effectiveness in preventing inadvertent file-sharing is proven in the successful function of its design."[14]

But such claims should seem familiar. They have been made before.

In 2003, the Oversight Committee's *first* hearing on inadvertent file-sharing focused on the study *Usability and Privacy: A Study of KaZaA Peer-to-Peer File Sharing,* which had identified two features in the file-sharing program KaZaA that had caused catastrophic inadvertent

---

[11] LimeWire LLC, *LimeWire Committed to Protecting Users Against Inadvertent File Sharing* (press release, 2009).

[12] Elinor Mills, *Can peer-to-peer coexist with network security?* CNET (March 6, 2009) (quoting DCIA's CEO); DCIA Written Statement at 23, *Legislative Hearing on H.R. 2221 and H.R. 1319 Before the Subcomm. on Commerce, Trade and Consumer Protection of the H. Comm. On Energy and Commerce*, 111th Cong. (May 5, 2009).

[13] Letter from Mark Gorton, Chairman, The Lime Group, to the H. Comm. on Oversight and Government Reform (May 1, 2009) [hereinafter, the "Gorton Letter"]. Reportedly, the Gorton Letter was given to journalists even before it was delivered to the Oversight Committee. *See* Eliot Van Buskirk, *LimeWire Chairman Assures Congress: Privacy Safeguards Are in Place,* Wired (May 1, 2009) at http://www.wired.com/epicenter/2009/05/limewire-ceo-assures-congress-privacy-safeguards-are-in-place/.

[14] Gorton Letter, *supra* note 13, at 1, 6-7, 7.

sharing. KaZaA's distributors responded by removing both of these features from their program. LimeWire and other distributors responded by drafting, and having their trade association promulgate, a self-regulatory *Code of Conduct* that prohibited use of either of these dangerous features. Soon, this trade association was claiming that its *Code of Conduct* had reduced inadvertent sharing to a mere "urban myth."[15]

But this claim was the real "myth": neither LimeWire nor other authors of this *Code* bothered to comply with it. For example, by 2004, the two dangerous features identified in *Usability and Privacy* had been condemned 1) by published research; 2) by two Committees of Congress; 3) by the distributors of KaZaA; and 4) by LimeWire's own *Code of Conduct.* But by 2004, *both* had also been deployed in LimeWire—long *after* it was known that catastrophic inadvertent sharing would be the inevitable consequence of deploying *either* one.

And catastrophic inadvertent sharing *was* the inevitable consequence of deploying these features.[16] In 2007, the Oversight Committee thus opened its *second investigation* into, and held its *second* hearing on, inadvertent sharing.[17] This time, even Lime Group CEO Mark Gorton was shocked by the consequences of LimeWire's reckless-at-best acts:

> I had no idea that there was the amount of classified information out there or that there were people who are actively looking for that and looking for credit card information.
>
> I think I've always felt that it was inexperienced users who didn't know what they were doing. However, when you see documents coming from people who specialize in computer security about, you know, military documents, it really makes you think twice.…
>
> I absolutely want to do everything in my power to fight inadvertent file-sharing. And I am sorry to say that I didn't realize the scope of the problem….[18]

Nevertheless, after the 2007 hearing, LimeWire opted for a familiar response: it decided to "help" its *new* trade association, DCIA, draft a *new* set of "voluntary" industry-self regulations so that responsible implementation of these *new* self-regulations could, again, be declared to have made inadvertent sharing a mere urban myth—an increasingly outdated concern.

---

[15] 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) at http://www.ftc.gov/os/comments/p2pfileshare/index.htm.

[16] *See, e.g.,* Hiawatha Bray, *File-Sharing Impairs U.S. Secrets,* Boston Globe (Aug. 5, 2004) at http://www.boston.com/business/technology/articles/2004/08/05/file_sharing_imperils_us_secrets/.

[17] Detailed information about this hearing, including a video, transcript, and copies of witnesses' written statements can be found on the Oversight Committee's website at http://oversight.house.gov/story.asp?id=1424.

[18] *Inadvertent File-Sharing over Peer-to-Peer Networks: Hearing Before the H. Oversight and Gov. Reform Comm.,* 110th Cong.*,* 114-15, 117 (July 24, 2007); *but see* Good & Krekelberg, *supra* note 5, at 138 (proving, in 2002, that users were looking for inadvertently shared credit-card numbers).

Concerned officials should *not* risk their own reputations by trusting LimeWire—again. By default, LimeWire 5 is a dangerous program that seems *intended* to make it too easy for consumers to "share" *all* of the files stored in their *My Documents* folder and all of its subfolders—including their entire collections of family photos, home movies, scanned medical, identifying and business documents, popular music, and even, perhaps, *all* of their documents. Moreover, LimeWire 5 can be this dangerous *because* it violates *eight* of the most critical obligations imposed by DCIA's LimeWire-drafted *Voluntary Best Practices*. LimeWire appears to take self-regulation no more seriously in 2009 than it did in 2003.

A. LimeWire 5 seems to increase the risk of catastrophic inadvertent sharing.

The design of LimeWire 5 centers upon a premise that verges upon lunacy: LimeWire 5 presumes that most users really *want* to be one click away from "sharing" all of the audio, video, image, and, (perhaps) document files stored in their *My Documents* folders and all of its subfolders—in other words, their entire collections of popular music and movies; all of their family photos; all of their home videos; and many or all of their scanned or faxed business, medical, legal, and identifying documents. Consequently, the following claim is simply wrong:

> In LimeWire 5.0… LimeWire fundamentally changed the way file-sharing works. LimeWire started from the ground up and addressed the fundamental problems that led to inadvertent file sharing.[19]

LimeWire 5 "fundamentally changed" *nothing*. Indeed, it seems like merely a slightly different means to a familiar end: making it *too easy* for one reasonable mistake to share *thousands* of personal files that cannot be safely "shared" via LimeWire.

Granted, the design of the *prior* versions of LimeWire that caused widespread breeches of national, personal, and military security certainly did reveal the "the fundamental problems that led to inadvertent file sharing":

- Users who opened certain submenus of LimeWire's *Tools>Options* menu could activate dangerously ambiguous sharing-related "features."
- These "features" could trigger *catastrophic* inadvertent sharing of thousands of personal files because their effects were linked to a confusing file-sharing *construct*—a "shortcut for selecting many files and sharing them individually."[20]
- The file-sharing construct used, (recursive sharing of folders), was confusing because it tended to misappropriate a file-management tool—the user's *My Documents* folder and its subfolders—*that was never intended* to define the set of personal files that someone might *want* to "share" with strangers.

---

[19] Gorton Letter, *supra* note 13, at 6.

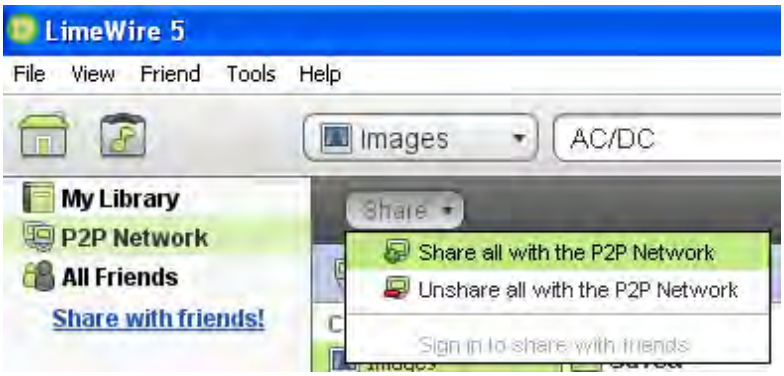
[20] Gorton Letter, *supra* note 13, at 6.

In short, the "fundamental problems that led to inadvertent file sharing" were simple. LimeWire deployed ambiguous sharing-related "features" that used *My Documents* and its subfolders as a "shortcut for selecting many files and sharing them individually." This ensured that one mistake could cause *catastrophic* inadvertent sharing of thousands of personal files.

Consequently, *nothing* "fundamental" has changed in LimeWire 5. Prior versions of LimeWire were dangerous because *changing their default settings* could permit one reasonable mistake to share *thousands* of personal files stored in *My Documents* and its subfolders. [21] LimeWire 5 is dangerous because *accepting its default settings* can permit one reasonable mistake to share *thousands* of personal files stored in *My Documents* and its subfolders.

1. LimeWire 5 now has a *new* dangerously ambiguous "share all" feature on major user-interfaces.

On its *My Library* and *P2P Network* interfaces, LimeWire 5 provides this "share all" feature:



One problem with this feature is obvious: "Share all" *of what*? Files, probably, but share all of *what set* of files? Adding to the confusion, a default installation of LimeWire 5 can present a user with up to *eight* "views" or "sub-views" in which files can be shared: a *My Library* view divided into Audio, Video, Image and Document sub-views, and a *P2P Network* view divided into the same four sub-views.

Consequently, "share all" should mean different things in different "views." For example, in *My Library>Images,* it might mean "share all image files in *My Library*." But in *P2P Network>Images* it might mean "share all image files that I have downloaded from the P2P Network"—because "share all" should refer to a set of files viewable in, and presently relevant to, the current view.

---

[21] For example, in one of the *worst* past versions of LimeWire, 4.0.7, users who completed default installations would not be one mistaken mouse-click away from sharing all of the image, video, and audio files in their *My Documents* folder and all of its subfolders until they had 1) navigated away from the main interface; 2) opened its *Tools* menu; e) opened its *Options* submenu; 4) selected its *Save* tab; 5) activated its *Save Directory* "feature," and 6) tried to save downloaded files in their *My Documents* folder.

At least, that is what I guessed, when I began researching LimeWire 5. Consequently, I downloaded three CD-box-art image files; "unshared" two of them; and then clicked "share all," guessing that, in the *P2P Network>Images* view, "share all" must mean "re-share all previously downloaded image files." Wrong: in this view, "share all" meant "*share all audio, video, image files stored your My Documents folder and its subfolders.*" Later, I also made the other mistake ensured by a design that stacks a *small* "share all" feature above a small "unshare all" feature: I meant to select "unshare all"—but clicked "share all" instead.

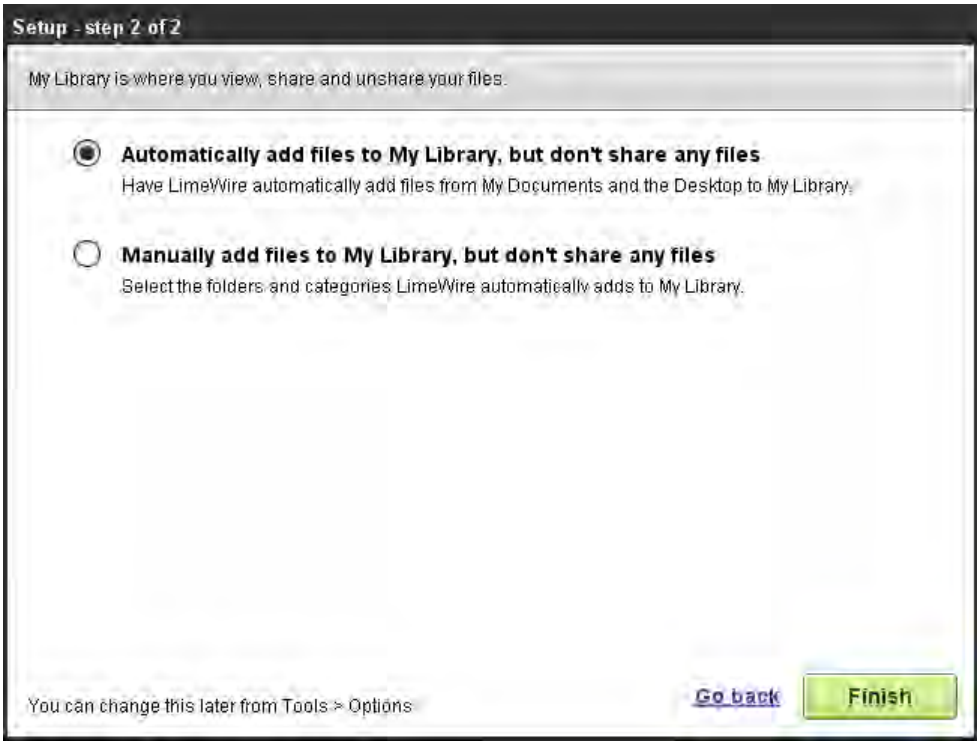
Over time, most LimeWire 5 users may make either or both of these errors. But to understand the *consequences* of such errors, one must understand what users of LimeWire 5 *may not* understand—the types and the locations of the files that a default installation LimeWire 5 will *automatically* load into a user's *My Library*.

2. The effects of LimeWire 5's "Share all" feature depend upon an obscure file-sharing construct called *"My Library."*

In LimeWire 5, *My Library* supposedly defines the set of files that *the user* wants to "manage," (that is, view, play, or offer to strangers) using LimeWire 5.[22] Consequently, LimeWire 5 should have left its users' "Libraries" empty by default, informed users that they would be one click away from sharing *every* shareable file in their "Library" (including documents, were defaults changed), and then let users *choose* whether to add any given file to their "Library."

But LimeWire 5, by default, automatically loads into *My Library* the set of files ambiguously defined by the small print on the following setup screen:

[22] In LimeWire 5, *My Library* is "new" only because it is now a file-sharing *construct*—"a shortcut for selecting many files and sharing them each individually." Gorton Letter, *supra* note 13, at 6. More specifically, by default, *My Library* serves as a "shortcut" for one-click "sharing" of a family's entire collections of popular music, home videos, popular movies, family photos, and scanned documents. Its pathetic "file-management" capabilities are not new. Nor is LimeWire 5's "Library view" new: the versions of LimeWire that facilitated widespread catastrophic sharing also had a "Library view" that displayed the files that the program was sharing, or could potentially share.



Few, if any, LimeWire 5 users will understand this screen's implications. Many will not read the fine print before clicking *Finish*. Many of those who *do* read the fine print may *not* guess that "add files from My Documents" actually meant "*recursively* add all files from *My Documents* and all of its hundreds of subfolders." Even those who *do* read the fine print, and *do* guess its meaning may lack the "perfect knowledge" of folder-structures and file-locations needed to discern that the set of files thus defined should include their entire collections of music, photos, home videos and scanned documents.[23] Moreover, during the LimeWire 5 setup process, no new user would know about the one-click "share all" feature whose effects *are linked* to the contents of *My Library*: without that information, no user installing LimeWire 5 can make an *informed* decision about what files should be in their "Library."

And worse yet, LimeWire *knew* that it was endangering users and exploiting by ensuring that LimeWire 5's default settings would load into *My Library* all of the audio, video, image, and document files in a user's *Desktop* and *My Documents* folder and its subfolders. The "LimeWire team" proved this when they tried to protect *themselves* by burying the following "warning" on their website: "***Please ensure that any folder on your computer that contains personal information is not included in your LimeWire library.***"[24]

---

[23] *See* Good & Krekelberg, *supra* note 5 at 140 (criticizing programs that presume "that users have perfect knowledge of what kind of files" are stored in *My Documents* and its subfolders).

[24] LimeWire LLC, *Using P2P Software Safely* at http://www.limewire.com/legal/safety.

This advice is sound, but it also seems to foreclose any claim that LimeWire 5's developers were acting in good faith when they created the default settings that will include in LimeWire 5 users' "Libraries" *all* of the document, image, audio, and video files in their *My Documents* folder and its subfolders—folders they knew are "often used to store personal or sensitive data."[25]

Worst of all, LimeWire also knew that such acts would be *particularly* likely to deceive *because* they exploit consumers' reasonable expectations. As one LimeWire developer recently testified, consumers expect *sensible* default settings that are *in the user's* interest:

> LIMEWIRE DEVELOPER: …[T]he program provides meaningful defaults which are set by the programmers.
>
> DEFENSE ATTORNEY: What do you mean by meaningful defaults?
>
> LIMEWIRE DEVELOPER: I mean defaults that make sense and are in *the user's interest*.[26]

LimeWire thus knew that consumers *would expect* LimeWire 5's "defaults" to be sensible, and "in the user's interest"—particularly if press releases were claiming that "LimeWire [5] has ensured the complete lockdown of the safety and security of LimeWire users."

In summary, the design of LimeWire 5 seem to reflect bad faith and frightening contempt for the safety of children and their families. Virtually no one who understood the risks would *choose* to use LimeWire 5 to "manage" their entire collections of documents, family photos, scanned documents, videos, or popular music. For example, were someone to "share all" of their family's collections of popular music, scanned documents and family photos stored in *My Documents* and its subfolders, the result could be an infringement lawsuit; it could be identity theft; or it could be something far worse:

> [We have] documented cases where child pornographers and predators are actively searching P2P networks for personal photos of children and others that may be stored on private computers. Once photos are downloaded and viewed, these individuals will… download all additional information being shared from that computer.… This accompanying information can be used by the predator to locate the… potential victim.[27]

That is *one* of the risks that LimeWire 5 *knowingly* inflicted upon children and their families.

---

[25] DCIA *VBPs*, *supra* note 2, at Def. (4).

[26] Trial Transcript of March, 5, 2008 at 300, *United States v. Spivack,* 05-cr-98(ERK) (E.D.N.Y. 2008) (emphasis added).

[27] *See Boback II* at 5, *supra* note 5, at 5; *see also USPTO Report* at 21 & n.49 (reporting 2005 warnings about pedophiles collecting inadvertently shared data on particular children). LimeWire was also reminded about this risk in 2007, when I described what could happen to my family were the *My Documents* folder on our main home computer inadvertently shared. *See Inadvertent File-Sharing over Peer-to-Peer Networks*, *supra* note 18, at 18-19.

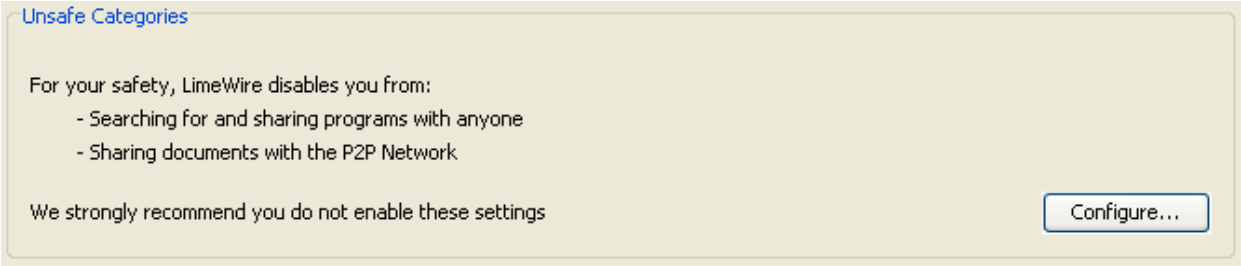
3. Users can *reasonably* disregard LimeWire 5's "warnings" and enable document-sharing.

In the Gorton Letter, LimeWire congratulates itself because LimeWire 5 users cannot share document-type files by default. Sadly, this two-year-old change in default settings reveals little about the *long-term* potential for inadvertent document-sharing among LimeWire 5 users. Indeed, LimeWire's fixation on the default settings of LimeWire 5 suggests a disturbing ignorance about *why* users of past versions of LimeWire inadvertently shared millions of personal documents.

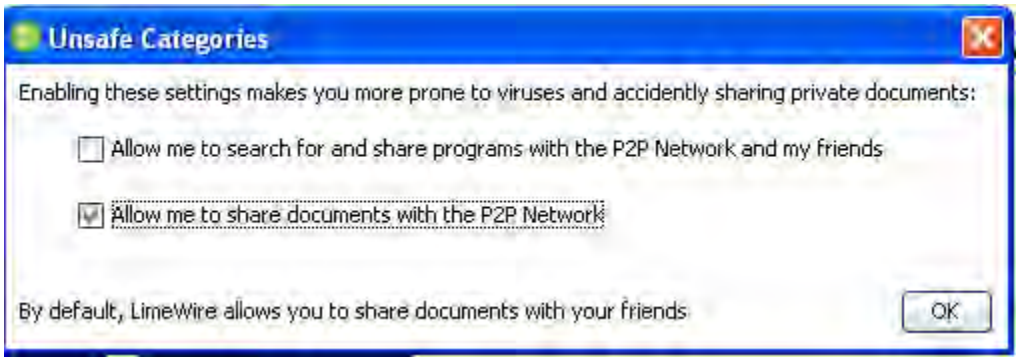
It has always been clear that almost all users of prior versions of LimeWire who inadvertently shared hundreds of personal files did so because *they had changed* "default settings." Consequently, history suggests that—over time—LimeWire 5's "default settings" will *not* determine how many of its users will inadvertently share documents.

To the contrary, history strongly suggests that the long term prevalence of inadvertent document-sharing will depend upon whether LimeWire 5 gives users who want to *change* its defaults the information that they need to make an informed decision about the benefits and risks of doing so. Sadly, LimeWire 5 fails *miserably* to disclose to users *why* it would be dangerous for them to enable document-sharing. It does warn users *not* to enable document sharing, but its disingenuous warnings sound nonsensical.

Before enabling document sharing, a user *might* read the following tiny-type warning before clicking the "Configure" button:



But this "warning" sounds wrong. Is sharing a document file encoding my own short story *really* more "unsafe" than sharing, say, audio files encoding popular music—an act that has gotten nearly 30,000 file-sharers sued? Is blog-authoring software really a safety hazard? Is it really more "unsafe" to share document files encoding my own short stories than image files encoding "adult," (and potentially obscene), images? Consequently, reasonable users could ignore these recommendations and click *Configure*. Then they *may* see another tiny "warning":



More nonsense: "sharing" documents already stored on your computer does *not* make you more "prone to viruses." And as for the risk of "accidentally sharing private documents," LimeWire itself has dismissed such concerns: "With LimeWire 5,… 'LimeWire has ensured the complete lockdown of the safety and security of LimeWire users….'"[28]

Reasonable LimeWire 5 users could thus conclude that its document-sharing warnings can be *safely* disregarded. Consequently, these warnings *cannot* be "improved" by *more* histrionics or half-truths. Rather, they must truthfully disclose *why* it is unsafe for LimeWire 5 users to enable document-sharing.

And, truthfully, it *is* unsafe for *any* LimeWire 5 user to enable document sharing—even users who just want to *legally* share a few of their own short stories. But it is unsafe for LimeWire 5 *users* to enable document-file sharing for the same reason that it was equally unsafe for LimeWire 5 *developers* to enable audio-file sharing, video-file sharing, or image-file sharing. In each case, the danger flows from the same source: by default, LimeWire 5 makes it *too easy* to inadvertently "share" *all* "shareable" types of files stored in *My Documents* and all of its subfolders.

That is the fundamental problem. And unless LimeWire 5 users are warned about it, they *will* enable document-sharing. And then, any short-term decrease in inadvertent document-sharing will recede.

In conclusion, the design of LimeWire 5 is not just dangerous—it seems to have been *intended* to *cause* inadvertent sharing. LimeWire's website warning seems to preclude any claim that its developers really did believe, in good faith, that so many American families would *want* to publish their entire collections of popular music and movies, home videos, family photos, scanned documents, and documents that LimeWire 5 needed to included them in *My Library* and provide an ambiguous, one-click means to share them all. The design of LimeWire 5 thus seems *intended* to make it *too easy* for users to inadvertently "share" entire collections of the types of media files that users of the Gnutella network want to download—while disclosing financial data to identity thieves and identifying information about children to pedophiles.

---

[28] LimeWire LLC, *supra* note 11.

B. LimeWire 5 violates *at least eight* of the DCIA *Best Practices*.

Voluntary self-regulation is *critical* to the future of technology law and policy. But LimeWire has displayed open contempt for "voluntary self-regulation." Back in 2003, LimeWire helped its previous trade association draft a self-regulatory *Code of Conduct* intended to prevent inadvertent sharing—and then violated at least three critical duties imposed by that *Code.*

LimeWire 5 seems to reflect even more contempt for the *new* LimeWire-drafted, self-regulatory *Voluntary Best Practices for P2P File-Sharing Software Developers To Implement To Protect Users Against Inadvertently Sharing Personal or Sensitive Data,* (the "*VBPs"*), promulgated and promoted by LimeWire's *present* trade association, the Distributed Computing Industry Association ("DCIA").[29] At least eight of LimeWire's violations of the DCIA *VBPs* seem to either let LimeWire 5 either (1) *perpetuate* catastrophic inadvertent sharing caused by prior versions, or (2) cause *future* catastrophic inadvertent sharing.

1. LimeWire 5 will share User-Originated files by default.

> "An application's default settings for file sharing at the point of software installation… shall not share User Originated Files" which are "any files stored on a user's computer prior to installation of the file sharing application." [30]
>
> "All respondents now have default settings for file sharing at the point of software installation that only permit redistribution of files the user subsequently downloads from the respective P2P network…. They do not share user-originated files by default."[31]

The DCIA *Compliance Reports* were wrong: LimeWire 5 will share User-Originated files by default, just by being installed. This can occur if a previous version of LimeWire was sharing User-Generated Files when a user installed LimeWire 5. This can also occur if *no* version of LimeWire was installed on a user's computer when LimeWire 5 was installed.

For example, the following screenshot shows the results of a default installation of LimeWire 5 on a test computer. This computer housed *only* User-Originated Files, and no version of LimeWire was installed when LimeWire 5 was downloaded and installed:

---

[29] To be clear, this paper assesses LimeWire 5's compliance with the *VBPs* to determine whether LimeWire has, belatedly, acted in good faith by complying with voluntary self-regulations. This paper neither states nor implies that either DCIA or its other member companies acted in bad faith when promulgating and implementing these *VBPS.* Nor does it assert that compliance with these *VBPs* would adequately prevent or remediate either inadvertent sharing generally, or catastrophic inadvertent sharing of personal files in particular. In short, the *VBPs* are relevant because they reflect self-imposed standards for preventing and remediating inadvertent sharing that can be used to assess the design of LimeWire 5. Consequently, this paper does not assess the inherent merits and limitations of these *VBPs*.

[30] DCIA *VBPs*, *supra* note 2, at (1) (emphasis added); *id* at Def. (6).

[31] DCIA*, Compliance Report on Voluntary Best Practices for P2P File-Sharing Software Developers To Implement To Protect Users Against Inadvertently Sharing Personal or Sensitive Data,* at 1 (2009) [hereinafter, the "*DCIA Compliance Report*"].

LimeWire 5 thus violated the *VBPs* by sharing 1,244 User-Originated Files—by default.

2. LimeWire 5 will share *thousands* of User-Originated Files without any clear, timely, and conspicuous plain-language warnings.

> In order for User-Originated Files or pre-existing folders to be shared, the user must take Affirmative Steps subsequent to the point of installation. These steps *shall include clear, timely, and conspicuous plain-language warnings* about the risk of inadvertent sharing of personal or sensitive data." [32]

LimeWire 5's default settings ensure that one reasonable, mistaken click of either of its ambiguous "share all" features can share a family's *entire collections* of popular music, home movies, family photos *and* scanned legal, medical, financial, and business documents—all without any "clear, timely, and conspicuous plain-language warnings about the risk of inadvertent sharing of personal or sensitive data."

3. LimeWire 5 shares "Sensitive File Types" by default.

> Even if the user of a *VBP*-compliant program changes its default settings in order to share User-Originated Files, the program "shall not … permit[] to be distributed via the P2P network" any "Sensitive File Types" that are "known to be associated with personal or sensitive data, including document file-types like word-processing documents and .pdfs."
>
> "In fact, to share sensitive file types in LimeWire 5 or beyond, a user must change his/her settings by going to *Tools -> Options -> Security* and clicking *Configure* under the heading "Unsafe Categories", and disregarding the following warning, "We strongly recommend you do not enable these settings."[33]

In fact, LimeWire 5 users can share *highly* sensitive file types that encode passwords, account numbers, tax returns, and identifying information about children just by installing LimeWire 5 on their family computer—without changing *any* settings or disregarding any warnings. LimeWire 5 thus grossly violates *VBP* obligations related to sharing of Sensitive File Types.

Because file-sharing programs and networks vary widely, the DCIA *VBPs* could not define any fixed set of file-types that were "sensitive." Consequently, the *VBPs* defined a standard to be applied, gave an example of its application, (document file-types), and required each program distributor to determine which file types were "sensitive" when shared by an average user of their program over the network to which it connects.

To comply with the *VBPs*, LimeWire thus had to decide what file types were "Sensitive File Types" when shared over the Gnutella network. This created a test of good faith. By default,

---

[32] DCIA *VBPs*, *supra* note 2, at (1)(A) (emphasis added).

[33] Gorton Letter, *supra* note 13, at 2.

LimeWire 5 will recursively load all of audio, video, image, and document files in a users' *My Documents* folder and its subfolders into a "Library." All the media files in this "Library" *could* then be shared by one mistaken "click" on the ambiguous "share all" feature.

But the *VBPs* prescribe that programs must *disable by default* any sharing of any type of User-Originated files "known to be associated with personal or sensitive data."[34] Consequently, if entire collections of images, movies, and music qualified, then the "share all" button would be inert—at least until users started burrowing into *Tools>Options* submenus and changing settings. This confronted LimeWire with a easy question: Are the entire collections of image, video, and audio files that people tend to store in their *My Documents* folder, (which is "often used to store personal or sensitive data") *themselves* "known to be associated with personal or sensitive data?"

Unless they chose to violate the *VBPs*, LimeWire executives and developers somehow concluded that a family's entire collections of scanned documents, family photos, home movies, copyrighted popular movies, and copyrighted popular music were *not* "known to be associated with personal or sensitive data" when shared over the Gnutella file-sharing network.

Frankly, it is difficult to imagine that even the "LimeWire team" could, in good faith, reach the conclusions reflected in the design of LimeWire 5. But if they did, then their conclusions seem inexplicable and inexcusable.

Image files: The image files that most families would tend to store in *My Documents* and its subfolders—like JPEGs, TIFFs and bitmaps—are *very strongly* "associated with personal or sensitive data." Most consumer and business scanners and multi-function copier-printers can save scanned documents in bitmap, TIFF or JPEG formats. Scanned documents can include *very* sensitive or personal records like tax returns, business records, financial data, legal documents, medical records, lists of account numbers and passwords, and identifying documents. Entire collections of family photos will be stored as JPEG files. LimeWire has known for years that these files could disclose very sensitive data—like identifying information about children—to LimeWire-using pedophiles.[35]

Audio files: Sharing the contents of one's music collection could certainly disclose "personal information." But here, the "sensitive data" prong of the *VBPs* seems even more dispositive. By definition, most music collections will tend to contain a lot of *popular* music—and almost none of it will be legal to "share" over the Gnutella network. Consequently, when entire collections can be "shared" at once, audio files become "sensitive."

---

[34] Because the *VBPs* do not define "personal data" or "sensitive data," each trigger should be given a common-sense interpretation. Consequently, this analysis interprets "personal data" to mean data that encodes either personally identifying information or other private information that would be dangerous or embarrassing to share with strangers. It interprets "sensitive data" to mean data that would be problematic to share for some other reason. For example, most work-related documents might contain no personal data, but they would still be associated with "sensitive data" because they are an employer's property, and could get someone fired if shared.

[35] *See supra* note 27.

Indeed, copyrighted audio files are dangerous to share for the same reason that it is dangerous to "share" work-related documents: doing so tends to infringe the proprietary rights of a third party who can then take legal action.[36] Catastrophic inadvertent sharing can thus inflict financial ruin on a given family in at least three different ways: 1) identity thieves could steal the family's savings; 2) inadvertent sharing of work-related files could provoke firings and damage careers, or 3) the family could be sued for infringing thousands of copyrights. From the family's perspective, these are just three routes to the same destination: potential financial ruin. Consequently, any rational set of *Voluntary Best Practices* must treat them the same.

Video files: Many home computers now store collections of home videos, in addition to family photos. Camcorders are inexpensive and common; many digital cameras also record videos; and video-editing programs like Adobe Premier and Pinnacle Studio and popular video-sharing sights like YouTube encourage consumers to store their video collections on their computers. Collections of home movies will tend to be associated with personally identifying and private information. Moreover, consumers may also have copies of popular copyrighted audiovisual works stored on their computers: these will raise the same concerns discussed below.

4. LimeWire 5 enables recursive sharing by default.

> "'Recursive Sharing' means the automatic sharing of subfolders of any parent folder designated for sharing.… Recursive Sharing shall be disabled by default…."[37]
>
> "[Inadvertent file-sharing is] an increasingly outdated concern over a very specific feature [recursive sharing of folders] of a small number of applications…."[38]
>
> "LimeWire 5 did away with recursive sharing… did away with folder sharing…."[39]

Wrong: By default, LimeWire 5 recursive shares folders. Indeed, that is why a default installation of LimeWire 5 can share files *never actually shared* by any prior version of LimeWire. Perhaps that is also why the Gorton Letter violated the VBPs—again—by re-defining "recursive sharing."[40]

---

[36] Doing this would be particularly absurd for users whose audio files have been safely and lawfully acquired. Nevertheless, LimeWire presumes that users who paid to buy music legally really might *want* to endanger themselves in order to "share" it with Gnutella freeloaders. Consequently, a default installation of LimeWire 5 will load into the users' "Libraries"—for one-click mass sharing—all audio files that a user has ripped from purchased CDs or downloaded legally from iTunes and Amazon.

[37] DCIA *VBPs*, *supra* note 2, at Def. (2).

[38] Written Statement of DCIA at 23, *Legislative Hearing on H.R. 2221 and H.R. 1319 Before the Subcomm. on Commerce, Trade and Consumer Protection of the H. Comm. On Energy and Commerce*, 111th Cong. (May 5, 2009).

[39] Gorton Letter, *supra* note 13, at 2.

[40] *Compare* DCIA *VBPs*, *supra* note 2 at 7(A) ("'Recursive Sharing'"… shall always have the same meaning whenever used in communications from the P2P file-sharing software provider"), *with* Gorton Letter *supra* note 13, at 6 ("recursive sharing, (i.e., automatic sharing of newly added files to a shared folder) also no longer exists").

For example, many earlier versions of LimeWire did not "share" bitmap (.bmp) files by default even if they were stored in a "shared" folder. This was wise: consumer copiers and scanners can save scanned medical, legal, or financial records as bitmap files. But LimeWire 5 shares bitmap files, and this can show that it enables recursive sharing of *folders* by default.

When LimeWire 5 is installed on a computer, it will automatically search a hidden folder called *Application Data* for a file called "limewire.props" that lists the *parent folders* once recursively "shared" by an installed, (or uninstalled), version of LimeWire. LimeWire 5 will then, by default, *recursively* share all of the "shareable" files stored in those folders and their subfolders.

To prove this, I set up a test computer to represent a user of LimeWire 4.12.15 who was inadvertently recursively sharing her *My Music* and *My Pictures* folders. Although this user had 1252 audio and image files stored in subfolders of these folders, she was "sharing" *only* 980 image and audio files—because LimeWire 4.12.15 did not share bitmap files by default. But when she "upgraded" to a default installation of LimeWire 5, she was sharing 1252 files—including the never-before-shared bitmap files. LimeWire 5 thus read the earlier version's configuration files, identified *My Music* and *My Pictures* as shared folders and *recursively shared* all "shareable" files in those folders and all of their subfolders.[41]

5. LimeWire 5 does not uninstall completely.

> "Complete uninstallation of the P2P file-sharing software also shall be simple to do… e.g., by using the standard Add/Remove Program functionality on Windows…."[42]
>
> "100% of respondents also provide complete uninstallation of the P2P file-sharing software that is simple to do and explained in plain language (e.g., by using the standard Add/Remove Program functionality on Windows…)."[43]

DCIA's *Compliance Report* is wrong again. LimeWire 5, like prior versions of LimeWire, *cannot* be uninstalled "completely" by using "the standard Add/Remove Program functionality [in] Windows." That process will leave behind—in a *hidden folder* invisible to most users—data files like "limewire.props," "library.dat," and "library5.dat." If LimeWire 5 is subsequently installed on that computer, it will read those data files and, by default, resume recursively sharing folders and files once "shared" by an *uninstalled* version of LimeWire.

This "partial-uninstall" feature has been condemned for years *because* it is absurdly dangerous. It ensures that users who make serious mistakes cannot correct them by uninstalling the program and starting over. Worse yet, it ensures that, ordinarily, *no one* can predict the effects

---

[41] This point can be confirmed as follows: install a version of "LimeWire 4;" configure it to recursively "share" an empty *My Music* folder; uninstall it; rip new audio files to new subfolders of *My Music*; and then install LimeWire 5: files *never before shared by any version of LimeWire* will thus be shared, by default.

[42] DCIA *VBPs, supra* note 2, at 7(B).

[43] *DCIA Compliance Report, supra* note 31, at 1.

of completing a "default installation" of LimeWire 5—even on a computer on which no version of LimeWire is presently installed.

For example, in the Gorton Letter, Mr. Gorton and LimeWire were *certain* that a default installation of LimeWire 5 could *not* share document files. Indeed, they were *so certain* that they challenged the Oversight Committee to install LimeWire 5 *on any computer* to prove that LimeWire 5 would *never* share document files by default:

> In short, there is absolutely no way to access a LimeWire 5 user's documents unless that user affirmatively elects to make them available.…
>
> To understand first-hand the level of security we have achieved I encourage any member of the Committee to do a default install of LimeWire 5 or later *on any computer* and attempt to share a document file type: LimeWire will not permit it.[44]

But it will: on some computers—even those on which no version of LimeWire is installed—invisible, hidden files ensure that merely installing LimeWire 5 can have unpredictable, dangerous consequences, including *default sharing of all of a user's documents*.

For example, I set up a test computer that had 1752 audio, image, and document files stored in various subfolders of its *My Documents* folder. I then confirmed that *no* version of LimeWire was installed on that computer, and then completed a default installation of LimeWire 5.1.3.

1752 files—including document files—were shared by default. Not only did a default installation of LimeWire 5 *permit* sharing of document files, it actually *shared* all of the document files in *My Documents* and its subfolders—with no input from, or warning to, the user, who certainly did *not* "affirmatively elect" to share document files, or any other files.

LimeWire's challenge backfired because neither LimeWire 5 nor prior versions of LimeWire uninstall completely. As *Usability and Privacy* explained *seven years* ago: "[U]sers often work in shared computer settings, so it is quite possible for one user to change all the settings and another to know nothing about it."[45] Consequently, a user installing LimeWire 5 might not know that a *different user* had once *uninstalled* an earlier version of LimeWire 5 *because* it had been misconfigured. That was the scenario underlying the test-computer experiment just described.

Nor is this scenario merely hypothetical. For example, when the Bucci family profiled by Today Investigates learned that one of their daughters had inadvertently shared the family's tax returns by misconfiguring a version of LimeWire, they responded in a reasonable way—they uninstalled LimeWire from their computer. But someday, one of the Buccis' daughters may mistakenly trust people claiming that "'LimeWire [5] has ensured the complete lockdown of the

---

[44] Gorton Letter, *supra* note 13, at 2-3 (emphasis added).

[45] Good & Krekelberg, *supra* note 5, at 142; *see also id.* (finding that 75% of KaZaA users sharing their entire hard drive reported that another user of the computer must have changed the default settings).

safety and security of LimeWire users….'" If that happens, no one can *honestly* say what a mere default installation of LimeWire 5 would do to the Bucci family.

6. LimeWire 5 does not require users upgrading from prior versions to "reconfirm" their "previously chosen sharing selections."

> "Previously-chosen sharing selections should be reconfirmed by the user upon installation of the new version of the software. In the reconfirmation process, users shall be warned… before Sensitive Folders are shared and users must take Affirmative Steps to continue sharing Sensitive Folders and their subfolders."[46]

Obviously, any *good-faith* effort to remediate inadvertent sharing caused by prior versions of a file-sharing program would require users upgrading from those versions to reset or repeatedly re-confirm their file-sharing settings. Otherwise, the "improved" program would create a mere *facade* of improvement that *perpetuated* all inadvertent sharing previously caused. But many distributors allegedly "remediating" inadvertent sharing have long done just that—created a *facade* of improvement that *perpetuated* inadvertent sharing caused by dangerous prior versions of their programs.[47]

LimeWire 5 is still pulling this same old trick. For example, suppose that a user of LimeWire 4.16.0 was recursively sharing files stored in her *My Documents* folder and all of its subfolders. If this user upgrades to LimeWire 5, he will *neither* have to "reconfirm" his prior "sharing selections" *nor* take any "Affirmative Steps to continue sharing Sensitive Folders and their subfolders." LimeWire 5 will, by default, rely on recursive sharing of *folders* to *perpetuate* sharing of all sharable file-types stored in his *My Documents* folder and all of its subfolders—including, of course, all family photos, many or all scanned documents, all home movies, and entire collections of popular videos and music.[48]

---

[46] DCIA, *VBPs*, *supra* note 2, at (7)(C). The *VBPs* define "Sensitive Folders" as "those often used to store personal or sensitive data, for example, the 'My Documents' folder in Windows…." As noted above, all *subfolders* of *My Documents*—including *My Pictures*, *My Videos*, and *My Music* should also qualify as "Sensitive Folders."

[47] *USPTO Report, supra* note 5, at 33.

[48] For three reasons, LimeWire cannot excuse this violation of the *VBPs* by claiming that a LimeWire 4.16.0 user recursively sharing her *My Documents* folder *must* have received a "Sensitive Folder" warning and *chosen* to recursively share her *My Documents* folder. First, *if* a 4.16.0 user received such a warning, it was affirmatively misleading. *See Revisited*, *supra* note 5, at 7-8. Second, that user would *not* have received such a warning if she had renamed her *My Documents* folder, a practice that Microsoft permits and encourages. *See, e.g.,* Ed Bott, et al. Microsoft Windows XP Inside Out 261 (Microsoft Press 2001) ("you can change the name of *My Documents* in the same way that you can change the name of any other folder: right-click and choose Rename"). Third, if LimeWire wanted even misleading "Sensitive Folder" warnings in prior versions of its program to negate the "reconfirmation" requirement, the *VBPs* that it drafted should have clearly permitted such misconduct.

7. LimeWire 5 will share *Documents and Settings* and its subfolders.

> "[Even if a user changes default settings] additional protection shall be provided against known instances of potentially-harmful user error.... *Any* attempt to share… a 'Documents and Settings' folder in Windows… *must be prevented*."[49]

The *VBPs* prohibit *any attempt* to share *Documents and Settings* because its subfolders store *all* of the personal and data files of *all* of a computer's users. For example, on a network drive, "sharing" *Documents and Settings* will share the data files of all of the users of the network. Consequently, *VBP*-compliant programs can *never* share *Documents and Settings.*

But LimeWire 5 will share *Documents and Settings.* It can share *Documents and Settings* if users change default settings when configuring *My Library*. By default, it may even load all of the audio, video, image, and document files stored under *Documents and Settings* into *My Library*—for convenient one-click sharing. Indeed, a default installation of LimeWire 5 can even *share* all of the image, video and audio files stored under *Documents and Settings*.[50] LimeWire 5 even *eliminated* the half-hearted "sensitive folder" warnings that *prior* versions of LimeWire gave to users sharing *Documents and Settings*.[51]

8. LimeWire 5 fails to warn users sharing more than 500 files.

> "The user shall be shown a prominent warning when [500+] files… are shared...." This warning shall contain options to reduce the number of shared files."[52]

LimeWire 5 inarguably violates the 500+ files-shared "prominent warning" requirement. The Gorton Letter claimed that, back in late 2007, versions of LimeWire did display a too-many-files-or-folders warning.[53] But LimeWire 5 eliminated it completely.

In conclusion, LimeWire 5 seems like déjà vu all over again: In 2003 and 2004, LimeWire appears to have repeatedly violated a LimeWire-drafted, self-regulatory *Code of Conduct* intended to prevent and remediate inadvertent sharing. In 2009, LimeWire appears to have repeatedly violated LimeWire-drafted, self-regulatory *Voluntary Best Practices… To Protect Users Against Inadvertently Sharing Personal or Sensitive Data.*

---

[49] DCIA, *VBPs*, *supra* note 2, at 4, 4(B) (emphasis added).

[50] A default installation of LimeWire 5 can either recursively populate *My Library* with the contents of *Documents and Settings* or actually *recursively share* all of the then-shareable file-types stored beneath *Documents and Settings* if a user was "upgrading" from an installed—or uninstalled—prior version of LimeWire. Whether LimeWire 5 will recursively "library" or *share* the contents of *Documents and Settings* by default seems to depend upon the *version number* of the installed, (or uninstalled), version of LimeWire 4 that was recursively sharing *Documents and Settings.*

[51] *See* Gorton Letter, *supra* note 13, at 4.

[52] DCIA *VBPs*, *supra* note 2, at (6)(A).

[53] Gorton Letter, *supra* note 13, at 5.

C. Other significant problems with LimeWire 5 and the Gorton Letter.

As noted above, by default, LimeWire 5 appears to be an *intentionally* dangerous program that re-creates the conditions required for catastrophic inadvertent sharing and repeatedly violates the DCIA *VBPs*. But there are other serious problems with LimeWire 5.

1. LimeWire 5's Prey-on-the-Weak default settings can endanger children and empower child predators.

> Our newest verision LimeWire 5.0, by default, cannot share sensitive file types such as spreadsheets or documents. *In fact, the [LimeWire 5] software can not share any file or directory without explicit permission from the user*.
> –Linda Lipman, LimeWire spokesperson.[54]

Of all the claims that LimeWire has made about LimeWire 5, this may be the one most likely to mislead. But Ms. Lipman's claim is also revealing: LimeWire's own spokesperson forgot that LimeWire 5 shares downloaded files *by default*—without any "explicit permission from the user." If an adult paid to explain LimeWire 5's behavior to the press and the public tends to forget this counter-intuitive behavior, similar errors will be rampant among the preteens, teenagers, and other new users of LimeWire. As a result, these new users may inadvertently share *downloaded* files—almost all of which will be *illegal* to "share" with other LimeWire users.

Ms. Lipman's misstatement thus highlights one of the most quietly deplorable aspects of LimeWire 5: it perpetuates the Prey-on-the-Weak model of file-sharing reflected in prior versions of LimeWire and many similar programs. Many new users of these programs will tend to be preteen or teenage children. Nevertheless, the default settings of these programs tend to be dangerous—and changing them can be more dangerous.

For example, by default, new LimeWire 5 users will "share" all of the files that they download from the Gnutella network—even though those files strongly tend to be infringing, and thus, illegal to "share" with other LimeWire users.[55] Sophisticated users thus disable this feature.

Similarly, by default, new LimeWire 5 users also "agree" to house, on their computers, databases of files shared by others—"search-index servers" like the one that subjected Napster Inc., to billion-dollar liability for the infringing acts of *other people* using that database.[56] Worse yet, by "playing Napster" and housing one of these liability-bomb databases, users slow down their own computers *while* increasing their risk of being sued for their *own* infringing acts or

---

[54] Jack M. Germain, *Congress Squeezes LimeWire for Straight Talk on P2P Security,* TechNewsWorld (April 22, 2009), *available at* http://www.technewsworld.com/story/66879.html?wlc=1244950408; Today Investigates, *LimeWire releases a statement* (Feb. 26, 2009), *available at* http://today.msnbc/msn.com/id/29305054.

[55] Electronic Frontier Foundation, *How to Not Get Sued for File Sharing,* http://www.eff.org/wp/how-not-get-sued-file-sharing ("[U]sers of publicly-accessible P2P networks can take the following steps to reduce their chances of being sued:… Disable the 'sharing' or 'uploading' features on your P2P application").

[56] *See, e.g., A&M Records, Inc. v. Napster, Inc.,* 239 F.3d 1004 (9th Cir. 2001).

prosecuted for distributing child pornography.[57] Virtually no one who understood the risks would *choose* to house such a database on their computer. Consequently, in programs like LimeWire 5, these risks are not disclosed—just *imposed,* by default. Eventually, sophisticated users discover these risks and disable these capabilities.

In short, programs like LimeWire 5 use unsafe, unwise default settings to ensure that the new and unsophisticated users of these programs will do most of the "dirty work"—the file-uploading and search-index serving—that more sophisticated users avoid.

But Prey-on-the-Weak filesharing does more than just endanger children and their families. It can also *empower* child predators. For the same reason that programs like LimeWire attract students and children who do not want to get caught illegally "sharing" popular music and movies, they also attract pedophiles who do not want to get caught "sharing" illegal child pornography. As a result, *scores* of LimeWire-related child-pornography prosecutions are now moving through the federal courts.[58]

And some of the LimeWire users being prosecuted are not just collectors of child pornography—they are dangerous pedophiles who may be data-mining the Gnutella network for inadvertently shared files that identify new victims.[59] When federal prosecutors identify and charge such defendants, they can, of course, charge them with possession of child pornography. But because possession is a rare strict-liability criminal offense, long jail terms are not generally imposed.[60]

Consequently, if prosecutors identify a LimeWire user who appears to be "a danger to the community,"[61] they may also charge a more serious crime: *knowing distribution* of child pornography. A knowing-distribution conviction can sequester dangerous predators from their

---

[57] Electronic Frontier Foundation, *How to Not Get Sued for File Sharing, supra* note 55 ("to further reduce the risk of having your ISP subpoenaed or of being sued yourself, we recommend that you make sure your computer is not being used as a [search-index server]"); Beryl A. Howell, *Real World Problems of Virtual Crime, in* Cybercrime: DIGITAL COPS IN A NETWORKED Environment 93-95 (Jack M. Balkin et al. eds., 2007) (reporting that the FBI raided a suburban home because the family's KaZaA-using teenage son had not only inadvertently downloaded child pornography, but was also acting as a search-index server for others seeking child pornography, which "made his machine a much bigger target for law enforcement"). In LimeWire 5, the checkboxes that disable this capability, and the similar DHT capability, are buried deep in the *Tools>Options>Advanced>Super Really Advanced>Performance* submenu under this warning: "We recommend that you don't touch these unless you really know what you are doing."

[58] Though few such cases produce reported opinions, the tip of the iceberg can be viewed by searching databases like LEXIS or Westlaw for cases containing the terms "LimeWire" and "child pornography."

[59] *See, e.g., United States v. Postel,* 524 F. Supp. 2d 1120, 1123 (N.D. Iowa 2006) (a LimeWire user obtained child pornography that he then used to "groom" the little girl that he molested for four years); *see also supra* note 27.

[60] *See United States v. Sudyka,* 8:07CR383, 2008 U.S. Dist. LEXIS 42569 at *22 (D. Neb. April 14, 2008) ("A possessor of child pornography is considerably less culpable than one who produces or distributes….")

[61] *See, e.g., United States v. O'Rourke,* CR-05-1126-PHX-DGC, 2006 U.S. Dist. LEXIS 1044 (D. Ariz. Jan. 12, 2006) (holding a LimeWire user to be a "danger to the community" because he shared many "extraordinarily abusive" images of "horrific child abuse" inflicted on "a very young girl, with hands bound and mouth gagged").

potential victims for a long time—*but only if the prosecutor can prove beyond a reasonable doubt that the defendant knew that he was "sharing" files containing child pornography.*

As a result, LimeWire developers are not just writing dangerous code, they are also testifying in child-pornography cases. But as the following March 2008 trial transcript shows, testimony from LimeWire can be as valuable to the defendant as to the prosecution:

> PROSECUTOR: Your Honor, I don't believe it is possible to share files inadvertently.
>
> ***
>
> THE JUDGE: … [D]oes your software make it possible make it possible for people to accidentally share personal files or sensitive data?
>
> LIMEWIRE DEVELOPER: Accidentally?
>
> THE JUDGE: Yes.
>
> LIMEWIRE DEVELOPER: Yes.[62]

Indeed, the difficulty of proving scienter in LimeWire-related child-pornography cases has already had serious consequences. For example, in *United States v. Park,* a LimeWire user was "sharing," *inter alia,* a three-hour video of the rape of a little girl "bound with a rope and being choked with a belt by what appeared to be an adult male.'" Nevertheless, he secured a reduced sentence because he "lacked an understanding of the software and thus … the knowledge to distribute the illegal wares that he possessed."[63]

Consequently, LimeWire has long known that unless LimeWire 5 comprehensively foreclosed *any* potential inadvertent sharing—*even of downloaded media files*—it would continue to exploit its new users *and* compromise the ability of prosecutors to sequester dangerous pedophiles from their potential victims. Nevertheless, LimeWire LLC *chose* to design LimeWire 5 so that it would *perpetuate* inadvertent sharing of all previously shared media files and *continue* to automatically "share" all media files that a user might download. Prey-on-the-Weak programs like LimeWire 5 thus endanger children—and empower pedophiles.

2. LimeWire's efforts to prevent *infringing* uses of its program fail to rise even to the level of farce.

The Gorton Letter concluded with tales about LimeWire's "efforts" to deter unlawful *infringing* uses of its program. The Gorton Letter thus bragged to the Oversight Committee about "efforts" to deter infringing uses of the LimeWire program that any competent developer should have known for years were inane farce. For example, on July 6, 2005, the *File Sharer's*

---

[62] Trial Transcript of March, 4, 2008 at 126, March 5, 2008 at 346-47, *United States v. Spivack,* 05-cr-98(ERK) (E.D.N.Y. 2008).

[63] 2008 U.S. Dist. LEXIS 19688 (D. Neb. March 13, 2008).

Guide to the Universe advised developers on how to *perpetuate* infringing uses of their programs and networks while appearing to deter it:

> [T]he *Grokster* decision sets out a roadmap for technologists who want to build P2P software.
>
> [M]ake an attempt, however lame, to install a user-optional filter which would spot copyright marked songs/movies and make them non-downloadable. You may even ship the P2P software with the "anti-infringing" filter turned on and leave it up to the user to make their own decision.… [M]ake sure that you put a big, honkin' disclaimer on your site – "The software on this site is to be used for sharing files which you own. It is illegal to share copyrighted material. If you don't know, don't share."[64]

The *Guide* proclaimed that such ruses would perpetuate piracy so pervasive as to preclude the very idea of private copyrights in expressive works: "If the copyright holders cannot shut down the inventors of these technologies, and *Grokster* seems to mean that they can't, another model for paying the creators is going to have to be found. Collective licensing or a media levy would seem to be it."

To be clear, the *File-Sharer's Guide to the Universe* is a farce: its author's plan not only fails—it backfires. Judges and juries can infer unstated intent from facts and circumstances. Consequently, intent to promote illegal acts can be inferred from wrongdoers' attempts to remain willfully blind to them. Similarly, intent can also be inferred from really "lame" efforts to "deter" illegal acts: neither those who *did* intend to deter illegal acts, nor those merely neutral to them, would waste their own resources on efforts destined to fail. Nevertheless, the *Guide's* farce is relevant here for two reasons.

First, the *File-Sharer's Guide to the Universe* shows that any competent distributor of a Gnutella -based file-sharing program who—like the *Guide's* author—*intended* to promote and perpetuate *infringing* uses of his program should have known that he could achieve that goal while providing: 1) a big honkin' disclaimer requiring users to represent that they will not infringe copyrights; and 2) a "lame" copyright-infringement filter that users could disable.

Second, in the Gorton Letter, the "LimeWire team" explained that they have been deterring infringing uses of LimeWire by providing: 1) a big honkin' disclaimer requiring users to represent that they will not infringe copyrights; and 2) a *really* lame copyright-infringement filter that users not only *could* disable, but that actually *is disabled for them*, by default, by LimeWire.[65] The Gorton Letter also claims that in 2009, LimeWire imposed an End-User-

---

[64] Jay Currie, *The File Sharer's Guide to the Universe*, 1 (July 6, 2005) at http://techcentralstation.com/070605E.html. Others have made similar arguments. *See* Johnathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J. L. & TECH. 253, 291 (2006) ("In the wake of *Grokster,* even software makers without good lawyers will know not to tout the copyright-infringing uses of their generic tools").

[65] Gorton Letter, *supra* note 13, at 8-9.

Licensing-Agreement (EULA) that *prohibits* infringing uses of LimeWire 5.[66] And so, LimeWire finally *began* doing what had been done—for years—by *all three* of the distributors of functionally similar file-sharing programs that were found to have *intended* to authorize or induce pervasive infringing uses of their programs.[67]

Fortunately, the cynical vacuity of LimeWire's dated antics has been exposed by developers of P2P file-sharing programs who respect both federal civil rights and the welfare of users of their programs. Some companies using P2P technologies protect their users using *mandatory* state-of-the-art filtering technologies. Others protect their users by authenticating all files that their programs will distribute. Others have implemented notice-and-takedown regimes to ensure that users of their programs who make mistakes can be notified—not sued. LimeWire 5 only lacks such capabilities because LimeWire *chose* to keep subjecting LimeWire 5 users to the risk of being ruined by the infringement lawsuits that LimeWire has advocated in court—but denounced in the press.[68]

Conclusion

LimeWire 5 is *not* "the final nail in the coffin of inadvertent sharing…." Indeed, by default, LimeWire 5 appears to be an *intentionally* dangerous program. Nor does LimeWire 5 even arguably comply with its *latest* trade association's *latest* set of self-regulatory standards, the DCIA *Voluntary Best Practices*. Indeed, from its "share all" button to its default settings to its "big honkin' disclaimer," the design of LimeWire 5 remains profoundly problematic—at best.

As a result of such repeated bungling or wrongdoing, it would be ridiculous to keep hoping that—someday—LimeWire LLC may comprehensively and effectively prevent and remediate inadvertent sharing. Consequently, civil/criminal referral letters should be sent to the both the U.S. Department of Justice and the state Attorneys General. These law-enforcement agencies possess the *civil* enforcement authority needed to *quickly* halt inadvertent sharing.[69] They also possess the *criminal* enforcement authority needed if an entity like LimeWire LLC really did

---

[66] Gorton Letter, *supra,* note 13, at 8.

[67] *See MGM Studios, Inc. v. Grokster, Ltd.,* 545 U.S. 913 (2005); *MGM Studios, Inc. v. Grokster, Ltd.,* 454 F. Supp. 2d 966 (2006).; *Universal Music Australia Pty Ltd v. Sharman License Holdings Ltd,* 2005 FCA 1242, *slip op.* at 132, ¶ 407 (Fed. Ct. of Australia Sept. 5, 2005).

[68] In effect, LimeWire blamed copyright owners for not suing users of file-sharing programs, and then blamed them when they did. *Compare Amicus* Brief of LimeWire, Inc., et al. at 5, *MGM Studios, Inc. v. Grokster, Ltd.,* Case Nos. 01-08541, 01-09923 SVW (PJWx) (C.D. Cal. Dec. 2, 2002) ("Plaintiffs can observe each and every file made available, find its location, and takewhatever remedial action would be appropriate under the Copyright Act."), *with* 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). (LimeWire's trade association claims, "[I]t's time for the RIAA's winged monkeys to fly back to the castle and leave the Munchkins alone.… [T]he record industry bullies should come out and fight us if they want, but leave the little guys alone.").

[69] The Racketeer-Influenced-And Corrupt-Organizations Act grants relevant civil-enforcement powers to the Department of Justice. *See* 18 U.S.C. § 1964. State consumer-protection acts generally provide powerful civil-enforcement powers to the Attorney General.

intend to trick users into "sharing" media files unintentionally—even if the predictable collateral damage would include family finances "shared" with thieves, national secrets "shared" with terrorists, and early-release cards granted to dangerous pedophiles.

In addition, *C*ongress should work with law-abiding technologists to revise H.R. 1319, The Informed P2P User's Act, so that another relevant federal law-enforcement agency—the Federal Trade Commission—will have the substantive and remedial authority needed to prevent malicious distributors of Prey-on-the-Weak file-sharing programs from sustaining piracy-based "business models" by bankrupting families, exploiting children, and empowering pedophiles.

Related PFF Publications

- Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform, Thomas Sydnor, John Knight, & Lee Hollaar, Progress on Point 14.22, October 2007.

The Progress & Freedom Foundation ■ 1444 Eye Street, NW ■ Suite 500 ■ Washington, DC 20005
202-289-8928 ■ mail@pff.org ■ www.pff.org

Testimony before the House Committee on Oversight and Government Reform

Robert Boback, CEO, Tiversa, Inc.

July 29, 2009

TIVERSA

Good morning Chairman Towns, Ranking Member Issa and Distinguished Members of the Committee.

My name is Robert Boback and I am the Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides security and intelligence services to help protect organizations from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

P2P file-sharing continues to be a major security risk and privacy issue. Today, I will provide a brief background on P2P networks, highlight the risks of inadvertent file sharing, provide examples of P2P file disclosures and the impact on consumers, businesses, government, the military and national security, and share our observations and recommendations.

Background: Peer-to-Peer Networks

The Internet is comprised essentially of four components: World Wide Web, Instant Messenger (IM), Email, and Peer-to-Peer networks. By many accounts, the largest of these by measure of consumption of overall bandwidth is Peer-to-Peer or P2P. This distinction is necessary to understand the security implications that we are presented with today as a result of both the enormity of the networks as well as the different security challenges that are presented by the networks.

P2P networks have been in existence for several years starting most notoriously with the introduction of Napster in the fall of 1999. The P2P networks have provided a gateway for users around the world to share digital content, most notably music, movies and software.

P2P networks are growing and dynamic. Since 2005, P2P networks have grown at the rate of over 20% (CAGR). Today, worldwide P2P networks may have over 20 million users at any point in time. P2P networks are ever-changing as users join and exit constantly. The number of P2P programs or "clients" has grown to over 225, with many having multiple versions in use. Additionally, many of the programs are open source and, accordingly, subject to modification as users see fit. P2P networks are a worldwide phenomenon with users across wide ranges of ages, educational backgrounds and incomes.

The use of P2P has evolved and is used by individuals worldwide for many different purposes including:

1 – Planned file sharing – its intended use.
2 – Searching for information with malicious intent – personal information used in identity theft; corporate information and trade secrets; and even military secrets and intelligence.
3 – Distribution and sharing of illegal information – Child pornography and information that could be used in terror activity.

Inadvertent File Disclosure

P2P networks continue to grow in size and popularity due to the extent of the content that is present and available on the networks, that in many cases, is not available from any other public source. In addition to movie and music files, millions of documents, that were not intended to be shared with others, are also available on these networks. It is this unintentional sharing that we refer to as inadvertent sharing or disclosure.

Inadvertent sharing happens when computer users mistakenly share more files than they had intended. For example, they may want to share only their music files or a large academic report, but instead expose all files on their computer's hard drive allowing other users to have access to their private or sensitive information. This can occur via several scenarios. These scenarios range from user error, access control issues (both authorized and unauthorized), intentional software developer deception, to malicious code dissemination.

"User error" scenario occurs when a user downloads a P2P software program without fully understanding the security ramifications of the selections made during the installation process. This scenario has been decreasing slightly in the past few years as many of the leading P2P clients have highlighted the security risks associated with sharing various types of files containing sensitive information.

"Access control" occurs most commonly when a child downloads P2P software program on his/her parents' computer. This may occur with or without the parents' knowledge or consent, however the sensitive or confidential information stored on that computer may become exposed publicly nonetheless.

"Intentional software developer deception" occurs when the P2P developers knowingly and intentionally scan and index any or all information during the installation process without the consent of the user. This practice was widely used a few years ago in an effort to populate the P2P networks with large amounts of content. The average user has no incentive to share any files with the other users on the network, confidential or not. The P2P developers recognized that this fact could cause a lack of content to be shared which would negatively impact the network itself. In recent years and in response to legislative intervention and awareness, most mainstream developers have discontinued this controversial tactic. However, there are over 225 P2P software programs that Tiversa has identified being used to access these networks. Many of these programs continue to surreptitiously index and share files in this fashion.

"Malicious code dissemination" occurs when identity thieves, hackers, fraudsters, and criminals embed malicious code ("worms") in a variety of files that appear innocuous. This scenario is extremely troubling as this malicious code can either force a system to reset its preconfigured security measures, despite the security-focused intentions of the P2P developers, or it can install an aggressive P2P program on a user's computer who may have never intended to install a P2P file sharing program. This scenario can expose even the most technologically advanced consumer or even an individual who has never intended to use P2P to identity theft or fraud. It can also lead to the inadvertent disclosure of sensitive work-related information that can inflict significant economic or brand damage to an organization and/or lead to the identity theft of customers, employees, or others.

The fact that P2P involves downloading of files from individuals that are unknown to the downloader allows the hacker to overcome the hurdle of getting users to download the worm. These criminals intentionally give the malicious code as the same name as highly sought after music, movie, and software downloads to ensure rapid and effective dissemination. Other criminals will use email attachments embedded with aggressive software that mimics P2P programs when installed. These worms will index and share all information on the victim's computer without any visibility to the victim. This code is very insidious as users cannot detect its presence on their systems. Current anti-virus programs typically do not detect the presence of such malicious software as it appears to the detection software as an intentionally-downloaded standard P2P software program. It is also important to note that firewalls and encryption do not address or protect the user from this type of disclosure.

These scenarios have resulted in millions of highly sensitive files affecting consumers, businesses large and small, the U.S. government, our financial infrastructure, national security, and even our troops being exposed daily to identity thieves, fraudsters, child predators, foreign intelligence organizations and terrorists worldwide.

Despite the tools that P2P network developers are incorporating into their software to avoid the inadvertent file sharing of private and classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem. Combine this with the fact that today's existing safeguards, such as data loss prevention, firewalls, encryption, port-scanning, policies, etc, simply do not effectively mitigate peer-to-peer file-sharing risk.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act highlighted the dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as CERT (Computer Emergency Response Team) and the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT's ST05-007-Risks of File Sharing Technology – Exposure of Sensitive or Personal Information clearly states:

> *"By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft."*

In July 2007, the House Committee on Oversight and Government Reform held a hearing on the very issue of the "Inadvertent Sharing via P2P Networks," during which many of the individuals that testified assured the Committee that this problem was being addressed or being remedied. Despite this recognition, most consumers and security experts at corporations worldwide have very little understanding of the information security risks caused by P2P. Most corporations believe that the current policies and existing security measures will protect their information – they will not.

Today, we will provide the Committee with concrete examples that show the extent of the security problems that exist on the P2P networks and the implications of sharing this type of information. During our testimony, we will provide the Committee with examples that illustrate the types of sensitive information available on P2P networks, provide examples of how identity thieves and others are actively searching for and using the information harvested from these networks, and offer our thoughts on actions to address the problem.

During our testimony today, we will show evidence that despite the numerous warnings and assurances by the developers and government agencies in previous hearings, the problem remains. In fact, we will also demonstrate the unprecedented increase in identity thieves using P2P software programs to harvest consumer information.

It is important to note that Tiversa believes strongly in the useful technology that is P2P. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the World Wide Web, it is not without its inherent risks.

Tiversa and its Technology

Beginning in 2003, Tiversa developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients. The technology has been designed, developed and implemented in a way that is transparent to the network; in a way that preserves the network's sustainability.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previously untraceable activity on the P2P network in one place to analyze searches and requests. While an individual user can only see a very small portion of a P2P file sharing network, Tiversa can see the P2P network in its entirety in real time. With this platform, Tiversa has processed as many as 1.6 billion P2P searches per day, more than the number of web searches entered into Google per day. This unique technology has led some industry experts (Information Week) to refer to Tiversa as the "Google of P2P."

Tiversa uses this technology to provide P2P security and intelligence services to businesses, consumers and law enforcement agencies. The following examples demonstrate how inadvertent breaches affect individual consumers, businesses, government, military and national security and are based on our unique perspective on P2P networks.

Examples: Inadvertent Disclosures on P2P

Consumers

Financial Fraud – From analysis of P2P searches, listed below is a small sampling of actual searches issued on P2P networks during a brief research window in March 2009. The term *credit card* was used as the filter criteria for the period.

- *2007 credit card numbers*
- *2008 batch of credit cards*
- *2008 credit card numbers*
- *a&l credit card*
- *aa credit card application*
- *abbey credit cards*
- *abbey national credit card*
- *ad credit card authorization*
- *april credit card information*
- *athens mba credit card payment*
- *atw 4m credit card application*
- *austins credit card info*
- *auth card credit*
- *authorization credit card*
- *authorization for credit card*
- *authorize net credit card*
- *bank and credit card informati*
- *bank credit card*
- *bank credit card information*
- *bank credits cards passwords*
- *bank numbers on credit cards*
- *bank of america credit cards*
- *bank of scotland credit card*
- *bank staffs credit cards only*
- *barnabys credit card personal*
- *bibby chase credit card*

As evidenced by the sampling above, it is clear to see that malicious individuals are issuing searches on P2P networks to gain access to consumer credit cards. Criminals will quickly use the information located to commit fraud using the stolen credit information. This fact was proven during our research with Dartmouth College and published in their subsequent report.

The term "tax return" is also highly sought after on P2P networks. During a live demonstration in January of this year for NBC's Today Show, Tiversa was able to locate and download over 275,000 tax returns from one brief search of the P2P. Many of these individuals have either saved an electronic copy of their tax return that they prepared themselves or have saved an electronic copy of their tax return that an accountant or professional tax office had prepared for them. There are also cases in which accountants and tax offices, themselves, inadvertently disclosed client tax returns.

It is a fact that identity thieves search for tax returns to primarily gain access to Social Security Numbers ("SSN"). According to a report on the black market, SSNs are worth approximately $35 each. This is up from approximately $8-$10 only a few short years ago. One plausible explanation for the rapid increase in black market pricing is that identity thieves are finding better ways to now monetize the stolen SSNs. This is a very important point. Our search data shows that thieves in fact employ a new degree of sophistication in cyber crime.

Identity thieves will also file an individual's tax return before the actual individual files the return. The thief will use a fabricated W-2, which can be printed using a number of programs, and will attempt to steal the phony refund that results from the fabricated return. When the victim then files his or her legitimate tax return, it will automatically be rejected by the IRS as "already filed." Eventually, the IRS will determine that the information, provided by the criminal on the W-2, doesn't match the records that it maintains. At this point, the criminal has most likely cashed the check from the fraud and has moved on to other victims leaving the initial victim to address the problem with the IRS. This is very costly and time consuming for both the victim and the IRS.

Stolen SSNs are also used by illegal aliens to gain employment in the United States. This crime has far reaching implications as well as placing a tremendous tax burden on the victim.

Medical Fraud – Medical information is also being targeted on P2P networks with alarming and increasing regularity. Listed below are some terms issued over the same period regarding medical information.

- *letter for medical bills*
- *letter for medical bills dr*
- *letter for medical bills etmc*
- *letter re medical bills 10th*
- *ltr client medical report*
- *ltr hjh rosimah medical*
- *ltr medical body4life*
- *ltr medical maternity portland*
- *ltr medical misc portland*
- *ltr orange medical head center*
- *ltr to valley medical*
- *lytec medical billing*
- *medical investigation*
- *medical journals password medical .txt*
- *medical abuce records*
- *medical abuse*
- *medical abuse records*
- *medical algoritms*
- *medical authorization*
- *medical authorization form*
- *medical authorization*
- *medical benefits*
- *medical benefits plan chart*
- *medical biliing*
- *medical biling*
- *medical bill*
- *medical biller resume*
- *medical billig software*
- *medical billing*
- *medical billing windows*

Identity thieves and fraudsters use medical information very similarly to financial information, but with much less scrutiny on behalf of law enforcement.

For example, if an identity thief were to download a consumer's medical insurance information, the thief would immediately have access to significant financial resources (in many cases medical insurance policies have limits set at $1 million or above). The criminal would most likely use the insurance card to buy online pharmaceuticals (predominantly Oxycontin, Viagra, or Percoset) which can be quickly sold for cash. This is a very difficult crime to detect as many consumers do not read Explanation of Benefit (EOB) forms sent from the insurance company, prolonging the criminal activity by delaying detection. Even consumers who do read the forms may not readily understand the diagnosis and treatment codes that are indicated on the forms. The victimization of the consumer continues when he or she attempts to appropriately use his or her insurance information for valid medical services only to be turned away or confronted with the suggestion of a potential prescription drug addiction.

User-issued P2P searches attempting to access financial, accounting, and medical information have risen 59.7% since September 2008. For the years of 2006 and 2007, the average annual rise in the search totaled just over 10%.

Child Predation – As if the aforementioned fraudulent activities were not enough to demonstrate the security implications of having personally identifiable information (PII) available to the public on these networks, the crimes can be even more heinous.

Tiversa works with federal, state, and local law enforcement agencies to address the rampant child pornography issues that permeate the P2P file sharing networks. The task is large and process is long however we continue to make progress in this ongoing fight. Presumably, child pornographers are using P2P to locate, download, and share sexually explicit videos

and pictures of small children because they feel that they cannot be caught on such a disparate network. Tiversa pioneered the research and tactics used to track and catch these individuals. We are also currently training all levels of law enforcement nationwide through the FBI LEEDA program and have been seeking to work more extensively with other law enforcement and prosecutorial organizations.

Tiversa has used its ability to locate available files and track individual's P2P network searches to document cases where child pornographers and predators are actively searching P2P networks for personal photos of children and others that may be stored on private computers. Once the photos are downloaded and viewed, these individuals will use the "Browse Host" function provided by the P2P software which allows the user to then view and download all additional information being shared from that computer. If personal photos are being shared, it is most likely that the computer will also be sharing other personal, private information such as a resume or tax return. This accompanying information can be used by the predator to locate the address, telephone, workplace, etc. of the potential victim. Individuals at Tiversa have directly assisted in the investigation of these specific types of cases.

Sources of the Breach – Many individuals at this point would consider themselves immune to these types of identity theft and fraud if they never used or downloaded P2P software. This is not an accurate assumption.

In research involving over 30,000 consumers, Tiversa found that 86.7% of the individuals whose information was found on the P2P networks, were breached by a third party. Many of these individuals had their information exposed by their doctors, lawyers, hospitals, accountants, employers, banks and financial institutions, payroll companies, etc. Organizations that had a right to have access to the information were predominantly the source of the breach.

In the 60 day research period (2/25-4/26/09), Tiversa downloaded 3,908,060 files that had been inadvertently exposed via P2P networks. This number is only comprised of Excel spreadsheets, Word documents, PDFs, Rich Text, Emails, and PST files. This number does not include any pictures, music, or movies. It is important to note that these files were only downloaded with general industry terms and client filters running. Many more exist on the network in a given period of time.

Corporations and businesses

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of specific search strings in this testimony would put these corporations at further risk. General search terms include company names in combination with "confidential," "executive," "payroll" and other terms clearly designed to identify files containing important or personal information. The Committee should note that the searches of this nature are every bit as aggressive and more specific than those for credit cards and medical information – the larger and better known a company and its brand, the greater the risks associated with the searches for these corporations.

Corporate information disclosed on P2P networks includes breached PII and personal health information (the basis for much of the personal information used in identity theft described above), intellectual property, strategic documents and business plans. We have identified disclosures of legal documents, performance reviews, Board minutes, merger and acquisition plans, plant physical security plans, network diagrams, user ID's and passwords. Specific examples of inadvertent disclosures are described below.

One Supplier affects Thousands – In one instance, we identified one small company with fewer than 12 employees that provides third party billing services to hospitals. An inadvertent disclosure on patients from three different hospitals by this company exposed personal health information (patient names, SSNs, diagnosis codes, physician names, and other information) involving:

- 20,245 Patients
- 266 Physicians
- 4,029 Employer Organizations
- 335 Insurance Providers

It is easy to see the criminal value of the information exposed in this single breach and the potential impact to a broad range of individuals, professionals and organizations.

Corporate secrets revealed – In another instance, Tiversa discovered the PST file of a high-ranking officer involved in the merger and acquisition area of a Fortune 100 company. The entire Microsoft Outlook information of this officer was exposed to the public:

- Entire calendar
- Schedule of conference calls with dial-in numbers and passcodes
- Business and personal contacts including names, e-mails, addresses, phone numbers, etc.
- Over 12,000 e-mails to and from the individual
- Over 400 e-mail attachments (documents, PowerPoints, spreadsheets, etc.) including:
  - Regional sales information
  - M&A business integration updates
  - Strategic business alliances
  - Revenues through acquisitions

In the wrong hands, this information could be used for individual profit from trading on "insider information" not formally reported by the company, or on a much larger scale to manipulate and undermine the credibility of the capital markets.

Government, the Military and National Security

This risk also extends to the military and to overall national security.

Troop PII exposed – Tiversa has documented the exposure of the PII of men and women in the Armed Forces with frightening regularity. Military families are prime targets for identity theft as the thieves are aware that the soldiers are probably not checking their statements or credit reports very closely due to the serious nature of the work that they are performing. We have seen the confidential information (SSNs, blood types, addresses, next of kin, etc.) of more than 200,000 of our troops.

Classified information searched for…and found – P2P networks also pose a national security risk. In monitoring the origin of the searches on the P2P networks regarding national security issues, it is clear that organized searching is occurring from various nations outside the United States to gain access to sensitive military information being disclosed in this manner.

Searches are directed at identifying and obtaining sensitive information on matters of security using terms such as:

- Classified
- Military classified
- Military confidential
- Top secret
- US Marines classified
- Restricted

Examples of information breaches emanating from P2P networks and known to the public are described below.

In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.

On April 22, 2009, the *Wall Street Journal* printed a front cover story reporting that former Pentagon officials had indicated that spies had downloaded plans for the $300B Joint Strike Fighter project. Highly sensitive information regarding the Joint Strike Fighter program was also discovered on P2P networks.

Recommendations

For several years, Tiversa's focus has been working with corporations and government agencies to mitigate P2P disclosures and risks. Based on our experience, we believe that there are steps that can help significantly decrease the likelihood of inadvertent disclosures and therefore increase the safety and protection of those most affected, the consumers. We humbly and respectfully provide the following recommendations for your consideration.

Increase Awareness of the Problem

Corporations are just becoming aware of the problem that the P2P poses to its information and data security. Individual consumers are even less prepared for the security threats that it poses. It is very difficult to protect against a threat that you are unaware of.

FTC – On the FTC's website on the page "About Identity Theft," there is not a single mention of P2P or file-sharing as an avenue for a criminal gaining access to a consumer's personal information. Of the 6 methods identified on the website, very few if any could ever result in the consistent production, let alone the magnitude, of PII like the P2P networks.

Clearly, victims of identity theft must be educated and notified that P2P could be the source of their stolen information.

SEC – Awareness should extend to corporations and government agencies as well. Corporations regularly breach personal information of individuals (employees, customers, etc.). With consumers increasingly being asked to provide PII to employers, banks, accountants, doctors, hospitals, and government agencies, the recipients of this PII must be knowledgeable in the threats that P2P can pose to the security of that information.

Corporations also disclose non-public information that could be used for individual profit or to manipulate or undermine the markets. P2P risks and vulnerabilities that lead to these disclosures should be addressed in the application of current laws (Sarbanes-Oxley, Gramm-Leach-Bliley, etc.).

Federal Data Breach Notification Standards

41 of the 50 states have now enacted some form of data breach notification law. However, the laws vary from state to state and, in our experience, are seldom respected or followed by organizations. In some cases, companies that seek to do the right thing are unfamiliar with the various laws that may apply to their situation or have difficulty in complying with the applicable laws.

Standardized breach laws should be enacted to provide guidelines for any organization, public or private, that houses consumer or customer PII in the event of a breach of the information. In this regard, we believe that P2P risks and vulnerabilities should be addressed in the application of current laws, and we support HR 2221 – the Data Accountability and Trust Act. This proposed legislation requires the establishment and implementation of policies and procedures for information security practices and includes notification and remediation provisions in instances of breach.

The breach laws will also need to be enforced. Many disclosing companies disregard the current state laws, if any, to the severe detriment of the consumer whose information was exposed.

Any breach involving the release of a consumer's SSN should include mandatory identity theft protection for that individual for a minimum of 5 years. The often reported 1 year of credit monitoring is completely inadequate remediation for a consumer whose SSN was breached. Identity thieves will wait for the credit monitoring to expire after the year provided to begin to attack the consumer. This is supported by actual files Tiversa has seen with expiry tags entered directly into the filename and meta-data.

Military Personnel & National Security Disclosures

DOD – The safety and identity of our men and women in uniform of Congress should be vigorously protected. Measures should be taken to safeguard personal information, and to monitor, detect and remediate any disclosures. For soldiers who have had their information disclosed, comprehensive identity theft protection services should be provided to prevent and guard against the use of the breached information.

DSS – P2P networks should be continuously monitored globally for the presence of any classified or confidential information disclosed by defense contractors or subcontractors that could directly or indirectly affect the safety or security our citizens.

Consumers

Tiversa also suggests the following recommendation for consumers:

Know Your PC (and who is using it) – Parents need to pay close attention to the actions of their children online, especially when the children are using a shared PC with the parents.

Just Ask! Consumers need to ask anyone who is requesting their PII (doctor, hospital, lawyer, banking institution, accountant, employer, etc.) what protections that the organization has in place to protect against inadvertent disclosures on the P2P networks.

Consider Identity Theft Protection Service – Organizations offer a wide variety of services to help with identity theft from credit monitoring to the more proactive placing of fraud alerts and black market monitoring. Consumers should select an ID theft protection service that offers proactive monitoring and remediation of P2P related disclosure.

Conclusion

In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, and private information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The Committee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of this powerful technology in the future.

Thank you for the opportunity to testify today.

TIVERSA.

144 Emeryville Drive
Suite 300
Cranberry Township
Pennsylvania 16066

(724) 940-9030 *office*
(724) 940-9033 *fax*
www.tiversa.com

"Inadvertent File Sharing over Peer-to-Peer Networks: How It Endangers Citizens and Jeopardizes National Security"
A Hearing before the House Committee on Oversight and Government Reform

Written Testimony of Thomas D. Sydnor II,
Senior Fellow and Director of the Center for the Study of Digital Property,
Progress & Freedom Foundation

July 29, 2009

Chairman Towns, Ranking Member Issa, and Members of the Committee on Oversight and Government Reform, I thank you for holding the Committee's *third* hearing on the needlessly persistent problem of inadvertent file-sharing. My name is Thomas D. Sydnor II. I am a Senior Fellow and the Director of the Center for the Study of Digital Property at the Progress and Freedom Foundation (PFF), a nonprofit, nonpartisan think tank founded in 1993 to study the effects of the digital revolution upon commerce and society.

"Inadvertent file-sharing" affects users of popular file-sharing programs used primarily to illegally copy and distribute popular music, movies and software. Predictably, many users of these programs are preteen or teenage children, so inadvertent sharing often affects not just the particular user of a program, but entire families and the employers of family members. Inadvertent sharing occurs when users of these programs end up distributing to potentially thousands of anonymous strangers files that they did not *intend* to publish to the world at large. Two different "types" of files can be inadvertently shared.

First, users may inadvertently distribute *downloaded* files that they acquired by downloading them from a file-sharing network. Users affected by this type of inadvertent sharing often become copyright infringers or distributors of pornography or child pornography. Second, users may inadvertently distribute *personal* files already stored on their personal computer or later created or acquired through some means other than downloading. Users affected by this type of inadvertent sharing often "share" hundreds or thousands of files that could end careers, facilitate identity theft, and turn the user into a high-volume infringer of the copyrights in *thousands* of lawfully acquired songs or videos.

I have now co-authored or authored three studies of the causes of inadvertent file-sharing, and I have testified about these studies before two Congressional Committees. In 2007, as an attorney-advisor in the Copyright Group of the United States Patent & Trademark Office, I co-authored *Filesharing Programs and "Technological Features to Induce Users to Share,"* a report which explained why inadvertent sharing had recurred long after its causes and consequences were thought to have been understood and remediated.[1] I also testified at this Committee's *second* hearing on inadvertent sharing in July of 2007.[2]

[1] Thomas D. Sydnor II, John Knight & Lee A. Hollaar, *Filesharing Programs and "Technological Features to Induce Users to Share"* (USPTO Mar. 2007) at http://www.uspto.gov/web/offices/dcom/olia/copyright/oir_report_on_inadvertent_sharing_v1012.pdf.

Later, I co-authored *Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform*, a paper which sought to correct and clarify misleading or inaccurate information provided to the Committee in 2007 by LimeWire LLC.[3] On May 5, 2009, I testified about inadvertent sharing during a legislative hearing before a Subcommittee of the House Committee on Energy and Commerce.[4] Most recently, in July of 2009, I authored *Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5*.[5] Accept as otherwise noted, below, these prior papers and testimony provide sources for the claims made below.

The problem of inadvertent sharing should have been detected and resolved long ago. For example, the developers of the file-sharing program Napster—by actually studying the contents of file-sharing networks—detected and avoided the problem as early as 2000. In 2001, the ground-breaking study *Free Riding on Gnutella* warned that distributors of file-sharing programs might deploy "technological features to induce users to share" because so few users were *intentionally* "sharing" popular files. In 2002, the now-famous study *Usability and Privacy: A Study of KaZaA P2P File-Sharing*, alerted even unobservant distributors of file-sharing programs to inadvertent sharing's consequences and causes.

Nevertheless, nine years later, inadvertent sharing remains a widespread and very dangerous problem. In late February of 2009, inadvertent file-sharing disclosed to Iran the plans for Marine One, President Obama's helicopter. Today Investigates also published a report on inadvertent file-sharing that revealed that the citizens of New York State alone were "sharing" over 150,000 tax returns over "peer-to-peer" file-sharing networks used mostly to pirate popular music and movies.[6] This report thus suggests that, nationally, over 2,000,000 tax returns were being inadvertently shared in February of 2009—an enormous data-security problem. Today Investigates also profiled the Bucci family, whose daughters, by misconfiguring the LimeWire file-sharing program, inadvertently "shared" their parents' tax returns with identity thieves who stole the family's tax refund.

To illustrate one reason why inadvertent sharing is still pervasive today—and can be expected to remain dangerously common in the future—I conducted an experiment this past weekend: I set up a test

---

[2] *See* Written Testimony of Thomas D. Sydnor II and Appendix A, *Hearing on Inadvertent File Sharing on Peer-to-Peer Networks Before the H. Comm. on Oversight and Government Reform,* 110th Cong. (July 24, 2007), at http://oversight.house.gov/story.asp?ID=1424.

[3] Thomas D. Sydnor II, John Knight & Lee A. Hollaar, *Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform* (PFF Oct. 2007) at http://www.pff.org/issues-pubs/pops/pop14.22inadvertentfilesharing.pdf.

[4] Prepared Statement of Thomas D. Sydnor II, *Legislative Hearing on… H.R. 1319 The Informed P2P User Act before the House Comm. on Energy and Commerce, Subcomm. on Commerce, Trade and Consumer Protection,* 111th Cong. at http://www.pff.org/issues-pubs/testimony/2009/090505_P2P_sydnor_testimony.pdf.

[5] Thomas D. Sydnor II, *Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5* (PFF July 2009) at http://www.pff.org/issues-pubs/pops/2009/pop16.14-inadvertent-file-sharing-reinvented-limewire-5.pdf.

[6] Today Investigates, *New warnings on cyber-thieves,* at http://today.msnbc.msn.com/id/26184891/vp/29405819%2329405819.

computer configured like my own family computer, which stores 16,798 personal documents, images, videos, and audio files in thousands of subfolders of a folder called *My Documents*.

After confirming that *no* version of LimeWire was installed upon this test computer, I then did something very dangerous: I downloaded the latest version of LimeWire 5, (version 5.2.8) and completed a "default" installation of the program. In other words, I clicked "Next," or accepted every default setting proposed by LimeWire; I did not change the "default" settings of LimeWire 5.2.8 in any way. Here were the results, enlarged for viewability:

In short, 16798 document, image, video, and audio files were automatically "shared" with tens of thousands of anonymous strangers *just by installing LimeWire 5.2.8*. Were this my actual family computer, my family would be sharing all of our work-related and personal documents, all of our scanned tax-related and identifying documents, many home movies, all of our family photos, and over 3,800 copyrighted audio files. This would likely ensure that my family would suffer one of three forms of financial ruin, (job loss, identity theft, or an infringement lawsuit). It would also expose my family and children to risks far worse than mere bankruptcy:

> [C]hild… predators are actively searching P2P networks for personal photos of children and others that may be stored on private computers…. [T]hese individuals will [then]… download all additional information being shared from that computer…. This accompanying information can be used by the predator to locate… the potential victim.[7]

This latter threat is neither hypothetical nor remote: *The Washington Post* reports that in Virginia alone federal investigators from the Internet Crimes Against Children Task Force were able to obtain child pornography "from nearly 20,000 private computers in the state…."[8]

No rationally designed computer program should inflict risks like these upon families *just by being installed*. Worse yet, LimeWire *also knows* that LimeWire 5.2.8 can cause inadvertent sharing for *other* reasons. Every version of LimeWire 5 released to the public—from LimeWire 5.1.1 to LimeWire 5.2.8,

---

[7] *See* Written Statement of Tiversa at 5, *Legislative Hearing on H.R. 2221 and H.R. 1319 Before the Subcomm. on Commerce, Trade and Consumer Protection of the H. Comm. On Energy and Commerce*, 111th Cong. (May 5, 2009). The term "predator" is a frighteningly apt description of some members of the LimeWire file-sharing "community." *See, e.g., United States v. Park,* 2008 U.S. Dist. LEXIS 19688, (D. Neb. March 13, 2008) (a LimeWire user shared videos of an adult raping a little girl "bound with a rope and being choked with a belt"); *United States v. O'Rourke,* 2006 U.S. Dist. LEXIS 1044 (D. Ariz. Jan. 12, 2006) (a LimeWire user was held to be a "danger to the community" because he allegedly shared many "extraordinarily abusive" images of "horrific child abuse" inflicted on "a very young girl, with hands bound and mouth gagged").

[8] Chris L. Jenkins, *Officials Find Child Pornography on 20,000 Va. Computers,* The Washington Post, VA03 (Apr. 10, 2008) (reporting on the results of a state-level report prepared by federal agents) at http://www.washingtonpost.com/wp-dyn/content/article/2008/04/08/AR2008040803930.html.

which was released late last Wednesday—has contained other "features" that LimeWire *knew* were unacceptably dangerous.

In short, the problem of inadvertent sharing has persisted for nine years because distributors of file-sharing programs like LimeWire LLC have repeatedly responded to even the most serious and well-documented concerns about inadvertent sharing with half-measures, misrepresentations, whitewash, and other conduct that, considered in its entirety, could strongly suggest bad faith—an *intent* to cause and perpetuate inadvertent sharing. If these concerns prove to be warranted, then the numerous breaches of national, military, commercial, and personal security that this Committee and others have repeatedly documented were probably nothing more—or less—than the acceptable "collateral damage" of schemes intended to trick users into sharing popular music and movies, the types of files that drive high volumes of traffic toward file-sharing networks.

Given this long history of repeated failure and potential wrongdoing, it would be absurd to, yet again, rely upon entities like LimeWire LLC to remediate inadvertent sharing. History suggests too well what the consequences of doing so could be: more breaches of national and military security; more needless damage to private enterprises that could otherwise drive economic recovery; more identity theft; more endangered children; more early-releases for dangerous pedophiles; and more needless lawsuits between copyright owners and American families.

Nevertheless, the measures needed to *comprehensively* remediate inadvertent sharing are neither mysterious nor complex—they simply are not compatible with the interests of companies, like LimeWire LCC, that still insist upon trying to build businesses based upon unlawful uses of their programs. Consequently, I would respectfully suggest that this Committee should now pursue a two-pronged remedial strategy that need not rely upon the competence and good faith of entities like LimeWire LLC.

First, I would respectfully suggest that the Committee should formally refer this matter to those law-enforcement agencies that *currently* possess both the civil enforcement authority needed to effect a complete and swift remediation of inadvertent sharing *and* the criminal enforcement authority that may be needed if some of the conduct described below proves to be as deliberate as if often seems to be. The U.S. Department of Justice possesses relevant criminal enforcement authority, and because criminal copyright infringement is a "predicate act," it also possesses potentially relevant expedited civil enforcement authority under the Racketeer Influenced and Corrupt Organizations Act (RICO).[9] The state attorneys generals have also been concerned about inadvertent sharing since 2004; they also possess not only adequate criminal enforcement authority, but even broader civil enforcement authority under their state consumer protection acts.

Second, and simultaneously, I would also respectfully suggest that the Committee should support efforts to amend and enact H.R. 1319, The Informed P2P User Act, bipartisan legislation now pending in the House Committee on Energy and Commerce. Granted, existing laws already provide the authority needed to send a blunt and powerful message that would deter distributors of piracy-adapted file-

[9] *See MGM Studios, Inc. v. Grokster, Ltd.,* 545 U.S. 913, 961 (2005) (Breyer, J., concurring) (noting that RICO could deter entities that intend to promote or cause widespread copyright infringement).

sharing programs from causing further inadvertent sharing or perpetuating that which they have already caused. Nevertheless, H.R. 1319 would target an intriguing "lighter-touch" approach toward the core problem underlying every incident of inadvertent sharing.

H.R. 1319 recognizes that the decision to publish a given file to the world at large is an extremely serious one that can implicate an array of state and federal civil and criminal laws—particularly if the file is to be published over a network as shadowy and lawless as the Gnutella file-sharing network to which programs like LimeWire connect. H.R. 1319 would thus grant to the Federal Trade Commission the additional remedial authority that the Commission needs in order to ensure that users of inherently dangerous programs like LimeWire never distribute *any* file *unless* they have received appropriate notice and then taken affirmative acts that clearly express their intent to "share" that file with anonymous strangers.

To understand the need for this two-pronged remedial strategy, it is critical to recall that this Committee, other agencies of the federal government, researchers, and security companies have long made extraordinary efforts to inform developers of programs like LimeWire about the causes and consequences of inadvertent sharing and given those developers repeated opportunities to remediate the problem voluntarily. Time and again, developers of such programs have failed to do so—and failed in ways suggestive of something worse than mere incompetence. Consider, for example, the following summary of *some* of LimeWire LLC's responses to this Committee's investigations of inadvertent sharing.

After the Committee's 2003 hearing on inadvertent sharing highlighted two features in file-sharing programs that were causing catastrophic inadvertent sharing, LimeWire and other distributors drafted a self-regulatory *Code of Conduct* prohibiting use of either feature—and then deployed both of them.

LimeWire inflicted the problem of inadvertent sharing upon its users—and itself—in the most effective way possible: it incorporated into its program "features" that had already been proven to cause catastrophic inadvertent sharing by computer-science research and this Committee. I have discussed LimeWire's 2002 to 2007 conduct in detail in *Filesharing Programs and "Technological Features to Induce Users to Share.*" Consequently, I want to focus here on one "feature" that may best illustrate the seeming blatant bad faith displayed by LimeWire LLC from 2003 to 2007.

A "search wizard," as that term is used here, is a subroutine that activates *only* the first time that a given file-sharing program is installed on a given computer. When activated, it scans the computer's hard drive(s) for "media files" and "recommends" that a new user should recursively share folders that the program's developers think that new users might want to share. Search-wizards actually deployed usually "recommended" that new users whose computers stored large music collections in subfolders of their *My Documents* folder should share their *My Documents* folder and all of its subfolders. Users accepting this "recommendation" would thus share almost all of their personal files: all of their personal and work-related documents, all of their scanned or faxed work-related or personal documents, all of their home videos and family photos, and—of course—all of the many thousands of copyrighted audio files in their collections of popular music.

In retrospect, the mere existence of search wizards seems inexplicable for two reasons. First, search wizards target vulnerable new users—and new users of file-sharing programs will tend to be preteen and teenage children. Second, it is simply absurd for *anyone* to have urged *children* to recursively share the *My Documents* folder of their family computer. No one who understood the consequences should agree to share all the files in their *My Documents* folder and all of its subfolders. Consequently, reasonable program developers could never have released programs that delivered such dangerous "recommendations" to vulnerable teenage and preteen children.

But distributors of popular file-sharing programs did just that. Search wizards were deployed in many such programs, and some distributors (like LimeWire LLC) actually *began* deploying search-wizards *after* their obvious consequences had been confirmed and condemned by computer-science research, by this Committee, and by the *Code of Conduct* developed by distributors of file-sharing programs including LimeWire LLC. The following search-wizard chronology makes this point:

> **June of 2002**: In *Usability and Privacy, A Study of KaZaA Peer-to-Peer Filesharing*, computer-science researchers from HP Labs conclude that two "features" in the KaZaA file-sharing program, including a search-wizard, were causing users to share so many sensitive files inadvertently that identity thieves had begun data-mining file-sharing networks for inadvertently shared credit-card numbers. Distributors responded by continuing to deploy search wizards.
>
> **June of 2003**: A year later, hearings on inadvertent sharing held by the House Committee on Oversight and Government Reform and the Senate Committee on the Judiciary caused the distributors of KaZaA to belatedly recognize *Usability and Privacy* as "intelligent research," and to promise to remove both of the dangerous features it had criticized.
>
> **July of 2003**: The distributors of KaZaA did remove the dangerous features condemned by *Usability and Privacy* and the hearings, but they did so in an almost inexplicable way: both features, including the search wizard were removed in a way that *perpetuated* all of the consequences of the catastrophic inadvertent sharing that they had already caused.
>
> **September of 2003**: The distributors of LimeWire and other programs responded to the Committee's hearing on *Usability and Privacy* by promulgating a self-regulatory *Code of Conduct* that should have precluded use of KaZaA-like search wizards
>
> **Fall of 2003**: Copyright owners begin suing users of file-sharing programs "sharing" hundreds or thousands of infringing files. Published research found that such enforcement caused most users to drastically reduce the number of files that they shared, but oddly, a few kept on sharing hundreds of infringing files—almost as if they did not realize that they were sharing files at all.
>
> **January of 2004** (approximately): The distributors of LimeWire deployed a KaZaA-like search-wizard in their program. Its share-*My-Documents* "recommendations" appeared automatically during a default installation of LimeWire.
>
> **August of 2004**: Predictably, LimeWire's aggressive search wizard quickly caused catastrophic inadvertent sharing. Consequently, a reporter from the Boston Globe soon asked LimeWire LLC why its users were sharing classified military data. A LimeWire executive blamed its search

wizard: "One possible weakness in LimeWire is a feature that automatically scans the user's hard drive, looking for files to be shared over the network. [The representative] said this feature can make it easy to expose private information by mistake." Nevertheless, LimeWire kept deploying the search wizard.

March of 2007: the United States Patent & Trademark Office published an empirical analysis of five popular file-sharing programs entitled *Filesharing Programs and Technological Features to Induce Users to Share*. It specifically criticized LimeWire for violating its own *Code of Conduct* by deploying a search wizard. LimeWire kept deploying its search wizard.

June of 2007: The House Committee on Oversight and Government Reform, following up on its own 2003 hearing and the USPTO report, asked LimeWire to explain why it was it was still deploying a search wizard. LimeWire declined to explain, but it did—finally—remove the search-wizard from its program. But like KaZaA in 2003, LimeWire removed the search wizard while *perpetuating* all inadvertent sharing it had previously caused.

Such conduct—which was part of a larger pattern of similar conduct—cannot be easily attributed to good faith, negligence or even gross recklessness. On balance—and absent the alternative explanation that LimeWire LLC has so far declined to provide—it seems more likely to reflect *deliberation*: an intent to deploy a known means of directing absurdly dangerous "recommendations" towards vulnerable persons in order to cause them to share files inadvertently.

After the Committee's 2007 hearing on inadvertent sharing allegedly alerted LimeWire to the dire and pervasive consequences of inadvertent sharing, it responded by, among other measures, deploying inadvertent-sharing warnings that seem to have been designed to fail.

Conduct like that described above ensured that in 2007, the Committee had to open its *second* investigation into the causes and consequences of inadvertent sharing. But this time, the Committee secured far more detailed testimony about the *consequences* of inadvertent sharing. That testimony left even Lime Group CEO Mark Gorton shocked by the results of LimeWire's reckless-at-best conduct:

> I had no idea that there was the amount of classified information out there or that there were people who are actively looking for that and looking for credit card information.
>
> I think I've always felt that it was inexperienced users who didn't know what they were doing. However, when you see documents coming from people who specialize in computer security about, you know, military documents, it really makes you think twice.…
>
> I absolutely want to do everything in my power to fight inadvertent file-sharing. And I am sorry to say that I didn't realize the scope of the problem….[10]

[10] *Inadvertent File-Sharing over Peer-to-Peer Networks: Hearing Before the H. Oversight and Gov. Reform Comm.,* 110th Cong., 114-15, 117 (July 24, 2007).

Nevertheless, after the 2007 hearing, LimeWire opted for a familiar response: it decided to "help" its *new* trade association, DCIA, draft a *new* set of "voluntary" industry-self regulations so that responsible implementation of these *new* self-regulations could, again, be declared to have made inadvertent sharing a mere urban myth—an increasingly outdated concern.

Consequently, for two reasons, little need be said about the half-measures that LimeWire adopted from mid-2007 to 2009 while it was allegedly drafting and implementing what would become the DCIA *Voluntary Best Practices for P2P File-Sharing Software Developers To Implement To Protect Users Against Inadvertently Sharing Personal or Sensitive Data,* (the "*VBPs"*) in what would become "LimeWire 5." First, the Marine One and Today Investigates reports alone suffice to prove the inadequacy of these measures. Second, whatever good these measures did is now largely irrelevant: LimeWire 5 actually eliminated most of these measures from more recent versions of the LimeWire program.

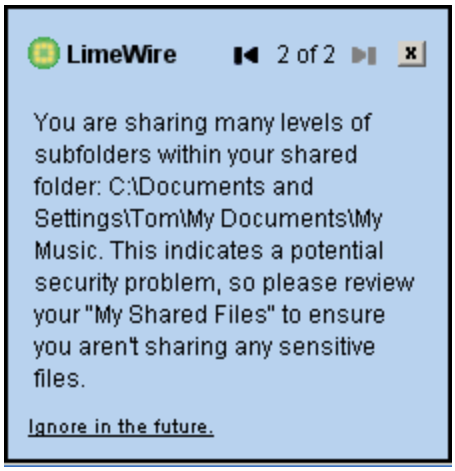
Nevertheless, one example may show why these many measures tended to fail.[11] For example, in the Lime Group CEO Mark Gorton's May 1, 2009 letter to the Committee (the "Gorton Letter"), LimeWire proudly explained that it incorporated into its "first major release following [Mr. Gorton's 2007] testimony" a new feature that would alert users to potential inadvertent sharing and help them remediate it by displaying a new you-are-sharing-too-many-files-or-folders warning:

> The third major change was designed to warn the use in the event an inordinate number of files were being shared, or a large number of folders were recursively shared, LimeWire displayed a warning telling the user that many files were being shared and giving the user the ability to go to their options menu and change this.

As LimeWire described it, this "warning" sounds like it should have been quite effective at alerting users to dangerous inadvertent sharing and helping them to remediate it. Nevertheless, subsequent events—like the Today Investigates report—reveal that it was actually a miserable failure.

And when you examine the delivery and appearance of this warning, the reasons for its miserable failure become clear. LimeWire "warned" its users that they were sharing too many files or folders by making a tiny little square full of 6-point type appear in the lower-right-hand corner of the screen and then automatically disappear seconds later:

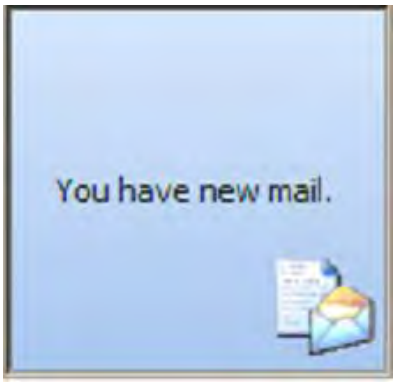
[11] I analyzed other problems with LimeWire 2007 warnings and remedial measures in my second co-authored paper on inadvertent sharing, *Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform.*



At first, this might *seem* like a thoughtlessly designed warning: someone managed to bury the lead—"**potential security problem**"—two-thirds of the way down a box full of jargon and small print. Moreover, note that the Gorton Letter misrepresented this warning's effects: it *never* gave users "the ability to go to their options menu and [correct potential inadvertent sharing]"—it gave them only the ability to disable the warning.

Nevertheless, the overall design of this warning is so bizarre as to suggest deliberation. Why cram the warning into a little square when the entire screen was available? Why make the little square appear in the bottom-right hand corner of the screen (and thus, in the bottom right-hand corner of the user's peripheral vision)? Why would a warning about a "potential security problem" disappear automatically? And why on Earth is the background *baby blue*—a color generally associated with neither LimeWire nor "security problem" warnings?

Nevertheless, a familiar source seems to have "inspired" the odd design of the LimeWire "security problem" warning. Many users of the versions of LimeWire that displayed this warning routinely received *another* type of notice. This notice was not meant to alert users to a "security problem"—merely to note a routine event that users would usually want to ignore. Consequently, these notices would appear frequently in a little baby-blue square in the lower right of the screen and then automatically disappear seconds later. They looked like this:



It is difficult to imagine that any entity acting in good faith could manage to create a "security-problem" warning that just happened to look and behave a lot like the "You have new mail" notifications that users would routinely vaguely perceive and ignore. It is even more difficult to imagine that any entity at all would engage in such conduct and then brag about it to this Committee during its *third* investigation of inadvertent sharing. LimeWire LLC must think that such acts speak to its good faith and commitment to remediating inadvertent sharing. So do I.

In short, as 2009 brought forth new disclosures like the Marine One and Today Investigates reports, any remaining claim that LimeWire LLC might have had to good faith rode upon the behavior of the new version of its program, "LimeWire 5," that was to implement DCIA's *Voluntary Best Practices—the latest* set of anti-inadvertent-sharing self-regulations promulgated by LimeWire's *latest* trade association.

But the result was a virtual re-run of 2003: once again, LimeWire 5 failed miserably to comply with the *DCIA* VBPs. Once again, both LimeWire and its trade association denounced and renounced a particular "feature" as *the* cause of inadvertent sharing—only to see its effects recreated in LimeWire 5.1, and the feature *itself* re-introduced in LimeWire 5.2.8, the latest version of LimeWire 5.

After the Committee opened its 2009 investigation, every version of LimeWire 5 has violated the DCIA *Voluntary Best Practices* and contained features that LimeWire LLC *knew* were dangerous.

I provided a detailed analysis of the behavior of what could be called "LimeWire 5.1" in my paper *Inadvertent File-Sharing Re-Invented: the Dangerous Design of LimeWire 5*. The following testimony thus summarizes major problems with LimeWire 5.1 and analyzes whether those, or other, major problems affect the latest version of LimeWire 5, LimeWire 5.2.8, which was released late last Wednesday.

The unpredictably and deliberately dangerous, *VBP*-violating design of LimeWire 5.1**:** My paper on LimeWire 5 identified an array of problems with the 5.1.1, .5.1.2, 5.1.3 and 5.14 versions that LimeWire distributed from early March of 2009 until July 22, 2009. Three of these problems can be summarized briefly.

First, these versions of LimeWire 5 are dangerously unpredictable programs because LimeWire 5 and previous versions of the LimeWire program do not "uninstall" completely. Consequently, if users—like the Bucci family profiled by Today Investigates—try to halt inadvertent sharing by removing or uninstalling a misconfigured copy of LimeWire from their computer, they unknowingly implant within it a ticking time-bomb. If any identical or later version of LimeWire is ever again installed on that computer, obscure files stored in a hidden folder *invisible* to the average user can cause the newly-installed version to *automatically* begin sharing *all* files shared by the previously uninstalled version. As a result—and particularly if a family computer is being used by more than one person—there is no way for ordinary computer users to determine what files LimeWire 5 may share *just by being installed.* It may not share any files. It may share all the document, image, video, and audio files in *My Documents* and its subfolders; it may share only some of those files, or it may do something even worse. Absent careful forensic analysis of the hidden folders and files on a given computer, there is no way to be sure.

Second, while DCIA relied upon data from LimeWire to declare LimeWire 5 the "poster child" for implementation of its *Voluntary Best* Practices, versions of LimeWire 5.1 appear to violate at least *eight* critical obligations imposed by the *VBPs*: (1) LimeWire 5.1 can share User-Originated Files by default; (2) it shares User-Originated Files without timely and conspicuous warnings; (3) it shares "Sensitive File Types" by default—like the image files that store entire collections of scanned financial documents and family photos; (4) it recursively shares *folders* by default; (5) it does not uninstall completely; (6) it does not make users of prior versions "reconfirm" their "sharing selections"; (7) it can "share" entire *networks* by recursively sharing *Documents and Settings*; and (8) it gives no "prominent warning" to users sharing more than 500 files.

Third, and worst of all, LimeWire 5.1 incorporated a new feature that it *knew* was hopelessly dangerous. One mistaken click on LimeWire 5.1's dangerously ambiguous "share all" feature can publish *all* of the audio, video, image, and documents files in a user's "Library." LimeWire's own website thus warned that a user's "Library" must <u>never</u> include "any folder… that contains personal information." But by default, LimeWire 5 will *automatically* include in a user's "Library" <u>all</u> of the documents, family photos, scanned documents, home movies and entire collections of popular music and movies stored in *My Documents* and its subfolders. This seemingly deliberate wrongdoing thus put millions of families one click away from multiple threats of financial ruin—or something worse.

<u>The unpredictably and deliberately dangerous, *VBP*-violating design of LimeWire 5.2.8</u>**:** the Committee may hear claims that the latest version of LimeWire 5, LimeWire 5.2.8, corrects many or all of the concerns expressed in my latest paper. Any such claims are 66% wrong and 100% misleading.

First, LimeWire 5.2.8 is still a dangerously unpredictable program. It will perpetuate any and all inadvertent sharing caused by both currently installed *and previously uninstalled* prior versions of LimeWire 5 and most earlier versions of the LimeWire program.

Second, LimeWire 5.2.8 still appears to violate most of the major substantive obligations imposed by the DCIA *VBPs*. Indeed, since LimeWire 5.2.8 will *perpetuate* all inadvertent sharing cause by LimeWire 5.1, it also appears to perpetuate *all* of the *VBP* violations described in my latest paper.

Third, while LimeWire 5.2.8 did eliminate the *new* Library-*My-Documents*/"Share-All" feature that LimeWire *knew* was dangerous, it replaced this *new* dangerous feature with a *old* feature that LimeWire also *knew* was dangerous: recursive sharing of folders.[12]

[12] The phrase "recursive sharing of folders" is actually a shorthand way to describe a more complex reality. Folders are data-management tools intended to present the files stored on the hard drive of a personal computer in a hierarchical structure so different kinds of files will be easier to find, manage and back-up. But the folder-structure on an ordinary personal computer was *never intended* to segregate a subset of the user's personal files that he or she might want to "share" with anonymous strangers. Nevertheless, earlier versions of LimeWire used folders (to quote the Gorton Letter) as a "shortcut for selecting many files and sharing them individually," even though folders are inherently ill-suited for that purpose. Worse yet, by default, most earlier versions of LimeWire would share folders *recursively*: in

Recall that LimeWire LLC and its trade association DCIA spent the spring of 2009 telling this Committee, Congress, and the public that *recursive sharing of folders* was a now-outdated feature that had been the root cause of most catastrophic inadvertent sharing:

> DCIA *VBPs*: "'Recursive Sharing' means the automatic sharing of subfolders of any parent folder designated for sharing.… Recursive Sharing shall be disabled by default…."
>
> DCIA Testimony to Congress: "[Inadvertent file-sharing is] an increasingly outdated concern over a very specific feature [recursive sharing of folders] of a small number of applications…."
>
> May 1, 2009 Gorton Letter: "LimeWire 5 did away with recursive sharing… did away with folder sharing…."

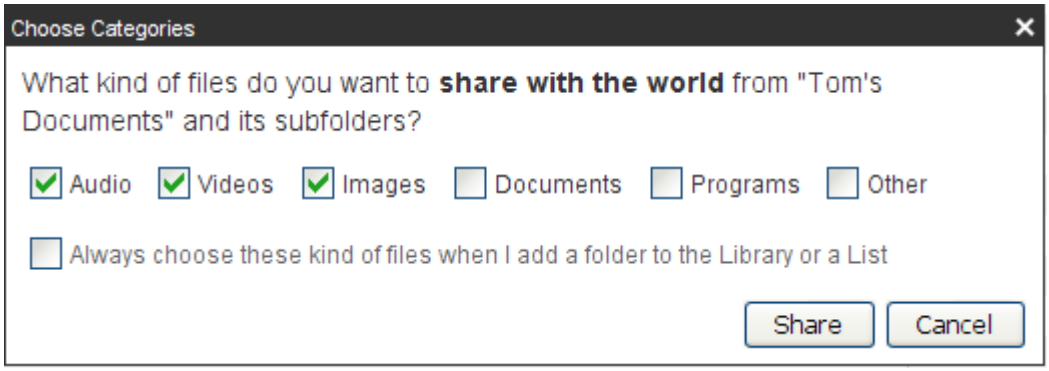
My most recent paper agreed that recursive sharing was an absurdly dangerous behavior, but it noted an equally dangerous flaw in the account of LimeWire 5 being offered by DCIA and LimeWire. LimeWire 5.1 *did still enable default recursive sharing of folders* during its installation-and-set-up process, but even after the program was installed and running a more serious problem remained: recursive sharing of folders was hopelessly dangerous because it made it far too easy for one mistake to "share" thousands of personal files inadvertently. Because LimeWire 5.1, by default, recursively loaded the contents of a user's *My Documents* folder into a "Library" that could be shared with one click of its ambiguous "Share all" button, it had re-created—in a slightly different way—the same conditions that made recursive sharing of folders so dangerous.

When confronted with the contradiction between its own website warnings, the default behavior of LimeWire 5.1, and the obvious defects in its "Share all" feature, LimeWire had little choice but to cease further deployment of this deplorable combination of features—though, once again, it has again chosen to perpetuate *any and all* inadvertent sharing that these features have already caused among the more than 50% of LimeWire users who were already using LimeWire 5.1.

Nevertheless, in LimeWire 5.2.8, the next general release after 5.1.4, LimeWire LLC did not really *remove* the library-*My Documents* and "Share all" features of LimeWire 5.1. Rather, LimeWire 5.2.8 *replaced* them with a familiar, tested substitute. As the following screenshot excerpt shows, LimeWire 5.2.8, *once again* has re-enabled *default recursive sharing of folders*:

---

other words if a user indicated that they wanted to share folder X, LimeWire would interpret that as a request to share all of the files stored in folder X *and* all of the files stored in all of the *subfolders, sub-subfolders, etc. of folder X*. Using this sort of *recursive sharing of folders* as a "shortcut for selecting many files and sharing them individually," ensured that one mistake could inadvertently share thousands or tens of thousands of a user's personal files.



The statement “and its subfolders” reveals what testing confirms: LimeWire 5.2.8 has re-enabled default recursive sharing of folders.

Indeed, preliminary testing suggest that the implementation of default recursive folder-sharing in LimeWire 5.2.8 may be more dangerously unbalanced that most implementations in prior versions of LimeWire. In LimeWire 5.2.8, it appears that while recursive folder-sharing will enable users to again make one mistake that shares thousands of personal files—even if those users were otherwise too unsophisticated to know how to select multiple files and apply an action to them. But should that happen, such LimeWire 5.2.8 users may have no means—other than file-by-file “unsharing”—to correct such all-too-predicable mistakes.

In conclusion, LimeWire *knew* that default recursive sharing of folders is hopelessly dangerous: both LimeWire and DCIA have so concluded, and those conclusions have been thoroughly validated by the years of empirical testing, on live human families, that LimeWire conducted while distributing “pre-LimeWire 5” versions of its program. Nevertheless, LimeWire *reinserted* default recursive folder-sharing into the latest version of its program, LimeWire 5.2.8.

Conduct like this—and the similar conduct described above and in my published papers and prior testimony on inadvertent sharing—lead me to conclude that the two-pronged, law-enforcement-based remedial approach that I have outlined, above, would be far more likely to protect the security of the our nation, our military, our economy, our families, our children, and even our copyright owners than any further reliance upon the competent, good-faith remediation of inadvertent sharing by entities like LimeWire LLC.

Prepared Statement of
Thomas D. Sydnor II,
Senior Fellow and Director for the Center for the Study of Digital Property,
Progress & Freedom Foundation

"Legislative Hearing on H.R. ___, the Data Accountability and Protection Act and H.R. 1319, the Informed P2P User Act"

Before the
Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection
United States House of Representatives
Washington, D.C.

May 5, 2009

Chairman Rush, Ranking Member Radanovich, and members of the Subcommittee, I am Tom Sydnor, a Senior Fellow and the Director of the Center for the Study of Digital Property at the Progress & Freedom Foundation, a non-profit research foundation dedicated to studying the public-policy implications of technology. I am also the lead author of two empirical studies that focus on the causes of what has been called "inadvertent file-sharing." Both studies seek to answer one simple question: "Why do so many users of certain types of 'peer-to-peer' file-sharing programs end up 'sharing' types of files that no informed user would ever deliberately 'share'?"

I would like to thank the Subcommittee for holding this hearing, and I would like to thank the sponsors of H.R. 1319, The Informed P2P User Act, for proposing a thoughtful and moderate solution to the serious and protracted problem of inadvertent file-sharing. My support for the Act is based upon my analysis of three critical questions that it seems to raise.

First, should Congress legislate to deter inadvertent sharing, or can Congress assume that inadvertent sharing will be remediated because distributors of file-sharing programs like LimeWire can be trusted to abide by the Voluntary Best Practices developed in mid-2008 by the Distributed Computing Industry Association? Here, I think that the answer is clear: "No": This approach was tried in 2003; multiple distributors violated their own self-regulatory *Code of Conduct* repeatedly, and the consequences were disastrous for consumers, for commerce and for the country.

Second, could the Act's substantive requirements improve upon existing legal mechanisms for deterring inadvertent sharing? Here, I think that the answer is "yes": the Informed P2P User Act improves upon existing law because its substantive requirements can narrowly and rather gently target the critical problem: because *certain* file-sharing programs are used almost exclusively for unlawful purposes, we should ensure that their users—many of whom are preteen or teenage children—must *once again* act deliberately before they "share" files that might be dangerous for them to distribute.

Third, can the Act's requirements be targeted narrowly toward the appropriate subset of the technologists who have deployed peer-to-peer networking technologies? In other words, should legislators again try to devise some definition of "peer-to-peer" that will target problematic conduct without needlessly burdening legitimate, law-abiding uses of this particular networking technology? Here, I think that the answer is "yes, but…."

The Subcommittee should attempt such efforts. In the past, such efforts have not succeeded, but given the gravity of the stakes, and the lessons taught by the Supreme Court's decision in the *Grokster* conclude, I believe that another attempt would be worthwhile. In particular, I believe that a combination of both technological and result-focused constraints might enable the Subcommittee and the sponsors of H.R. 1319 to devise a broadly acceptable compromise.

But because such efforts might not succeed, I believe that the Subcommittee might also wish to consider a back-up strategy. The Informed P2P User Act improves upon existing law because it narrowly and rather gently targets critical root causes of inadvertent sharing. Nevertheless, Congress has long provided federal law-enforcement agencies with both criminal and civil enforcement authority that, while neither gentle nor narrowly targeted, can surely punish and deter the worst of the abuses that distributors of certain file-sharing programs have—for far too long—inflicted upon children, families, lawful commerce, national security and the rule of law.

The Informed P2P User Act seeks to end years of inexcusable conduct by devising a precision instrument that would narrowly target root causes of inadvertent sharing. But if a precision instrument cannot be made broadly acceptable to law-abiding technologists and thoughtful consumer advocates, then the Committee could, instead, urge federal law enforcement agencies to use their existing hammers to send a message. And should this back-up strategy be accepted, and resort to it required, the rest of my testimony may suggest why the message to be sent must be both forcefully delivered and unequivocal in content.

Given my background, I believe that I may best assist the Subcommittee's legislative efforts by focusing the rest of my written testimony on the first of the three questions that outlined above. Last year, the Distributed Computing Industry Association (DCIA) published a set of Voluntary Best Practices (VBPs) that were intended to help developers of programs and services that use peer-to-peer technologies avoid causing inadvertent sharing. In recent weeks, DCIA's member company, LimeWire LLC, has been telling both the public and Congress that its implementation of the DCIA VBPs in the most recent versions of its program, LimeWire 5 "put the final nail in the coffin of inadvertent sharing of sensitive files."

Such reports could suggest that the Committee should forego resort to legislation and rely, instead, upon further implementation of "voluntary self-regulation" by distributors of file-sharing programs like LimeWire 5. For the following reasons, I cannot advise any Committee of Congress to make *another* attempt to rely on voluntary self-regulation by distributors of certain types of file-sharing programs.

Voluntary Self-Regulation Has Been and Should Be a Critical "First-Resort" Component of Sound Technology Policy.

I believe that voluntary self-regulation should be the policy option of first resort when we encounter problems relating to computer, software, and internet technologies. Simply put, innovation is an inherently uncertain process in which missteps and mistakes are inevitable. Were Congress and regulators to react to each misstep by imposing stringent, prescriptive laws and regulations, the innovation that could drive our Information-Age economy toward recovery could be seriously impeded by constraints that could quickly become outdated, ineffectual, or market-distorting.

But precisely because voluntary self-regulation must be central to our innovation policy, entities who pledge to voluntarily self-regulate must take their self-imposed duties seriously. Consequently, voluntary self-regulation has three important components: 1) credible self-regulators; 2) meaningful self-regulations; and 3) reasonable implementations of the self-regulations.

When the circumstances of this situation are compared against the requirements for viable self-regulation, none appear to be clearly satisfied: 1) one critical self-regulator seems to have repeatedly proven itself to be untrustworthy; 2) in critical respects the VBPs provide only vague or inappropriate guidance; and 3) the implementation of the VBP's by the distributors of the LimeWire file-sharing program seem to reflect flaws so serious as to—again—raise questions about the integrity of its implementation process.

Under such circumstances, those of us who favor voluntary self-regulation should concede that the only question remaining is which branch of the government should act, and how. I will address each of these concerns—credibility, regulations, and implementation—in that order.

Few potential self-regulators are less credible than LimeWire LLC: generally, questions about voluntary self-regulation arise only *after* a problem has occurred. Consequently, sound public policy dictates that even entities and industries that have made serious errors should be able to qualify as potentially viable self-regulators. Nevertheless, at some point, misconduct can become so seemingly culpable, so egregious, or so frequent as to preclude further rational reliance on self-regulation.

Some cases may present fine questions about whether these lines have been crossed. But this is not one of them. The entity whose behavior is probably most critical to the efficacy of the DCIA VBPs is LimeWire LLC. I have described in detail aspects of LimeWire's previous conduct in my two prior papers on inadvertent sharing. Today, I only wish to highlight one episode to illustrate a larger pattern of conduct that should tend to discredit this potential self regulator. As a result, I want to describe the history of the deployment of a feature called a "search wizard" in the file-sharing programs KaZaA and LimeWire.

A "search wizard," as that term is used here, activates only the first time that a given program is installed on a given computer. When activated, it scans a computer's hard drive(s) and "recommends" that the new user recursively share certain folders identified by the distributors of the program as folders that a new user might want to share. Search-wizards actually deployed

tended to "recommend" that new users should share all, or almost all, of the files in their "My Documents" folder and all of its subfolders. Users accepting this "recommendation" would thus share almost all of their personal files—including their entire music collection: all of the audio files ripped from purchased CDs.

In retrospect, the existence of search wizards seems difficult to explain for two reasons. First, search wizards target new users—and new users of file-sharing programs will tend to be preteen and teenage children. Second, a search wizard that urges children to recursively share the "My Documents" folder of the family computer seems inexcusable. No one who understood the probable consequences should agree to share all the files in their *My Documents* folder and all of its subfolders. Consequently reasonable program developers should never have released programs that delivered such "recommendations" to their most vulnerable users.

But they did. Search wizards were deployed in many popular file-sharing programs, and some distributors of some file-sharing programs (like LimeWire) actually *began* deploying search-wizards *after* their self-evident consequences had been confirmed and condemned by computer-science research, by both Houses of Congress, and by the *Code of Conduct* developed by distributors of file-sharing programs including LimeWire LLC. The following search-wizard chronology makes this point:

> **June of 2002**: In *Usability and Privacy, A Study of KaZaA Peer-to-Peer Filesharing*, computer-science researchers from HP Labs conclude that two "features" in the KaZaA file-sharing program, including a search-wizard, were causing users to share so many sensitive files inadvertently that identity thieves had begun data-mining file-sharing networks for inadvertently shared credit-card numbers. Distributors responded by continuing to deploy search wizards.
>
> **June of 2003**: A year later, hearings on inadvertent sharing held by the House Committee on Oversight and Government Reform and the Senate Committee on the Judiciary caused the distributors of KaZaA., (who were members of DCIA), to belatedly recognize *Usability and Privacy* as "intelligent research," and to promise to remove both of the dangerous features it had criticized.
>
> **July of 2003**: The distributors of KaZaA did remove the dangerous features condemned by *Usability and Privacy* and the hearings, but they did so in an almost inexplicable way: both features, including the search wizard were removed in a way that *perpetuated* all of the consequences of the catastrophic inadvertent sharing that they had already caused.
>
> **September of 2003**: The distributors of LimeWire and other programs responded to the congressional hearings on *Usability and Privacy* by promulgating a self-regulatory *Code of Conduct* that should have precluded use of KaZaA-like search wizards. They declared, "[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."
>
> **Fall of 2003**: Copyright owners begin suing users of file-sharing programs "sharing" hundreds or thousands of infringing files. Published research found that such enforcement caused most users to drastically reduce the number of files that they shared, but oddly, a few kept on sharing hundreds of infringing files—almost as if they did not realize that they were sharing files at all.

January of 2004 (approximately): The distributors of LimeWire deployed a KaZaA-like search-wizard in their program. Like the KaZaA search wizard, it tended to recommend that new users should share their "My Documents" folder and all of its subfolders. Unlike the KaZaA search wizard, its "recommendations" appeared automatically during a default installation of LimeWire.

August of 2004: Predictably, LimeWire's more aggressive search wizard quickly caused catastrophic inadvertent sharing. Consequently, a reporter from the Boston Globe soon asked LimeWire LLC why its users were sharing classified military data. A LimeWire representative cited its search wizard: "One possible weakness in LimeWire is a feature that automatically scan the user's hard drive, looking for files to be shared over the network. [The representative] said this feature can make it easy to expose private information by mistake." Nevertheless, LimeWire kept on deploying the search wizard.

March of 2007: the United States Patent & Trademark Office published an empirical analysis of five popular file-sharing programs entitled *Filesharing Programs and Technological Features to Induce Users to Share*. It specifically criticized LimeWire for violating its own *Code of Conduct* by deploying a search wizard. LimeWire kept on deploying its search wizard.

June of 2007: The House Committee on Oversight and Government Reform, following up on its own 2003 hearing and the USPTO report, asked LimeWire to explain why it was it had, and was still, deploying a search wizard. LimeWire declined to explain, but it did—finally—remove the search-wizard feature from its program. But like KaZaA in 2003, LimeWire removed the search wizard in a way that happened to *perpetuate* all inadvertent sharing it had previously caused.

I do not purport to see how the conduct described above—which was part of a larger pattern—can be easily attributed to good faith or even repeated negligence. Some might argue that it could reflect mere repeated recklessness. Nevertheless, at least to an outsider like me, it seems difficult to deny the possibility that it reflects the results of *deliberation*: an intent to deploy a known means of directing absurdly dangerous guidance towards a program's most vulnerable users in order to cause them to share files inadvertently.

Fortunately, for present purposes, debates about repeated-recklessness versus deliberate-wrongdoing are irrelevant. In either case, history has discredited LimeWire LLC as a viable self regulator: we conducted that experiment, and the results were disastrous and unequivocal.

Critical components of the DCIA VBPs are necessarily vague or ill-suited when applied to particular programs: in theory, sufficiently prescriptive Voluntary Best Practices might reduce concerns about the character of the entities that must implement them. But in practice, the DCIA VBPs should not do so. For example, DCIA or others may criticize the Informed P2P User Act because its *initial* version prescribes a set of principles applicable to *all* uses of peer-to-peer networking—from the most inherently unobjectionable to the most inevitably unlawful. But if so, the same critique applies even more forcefully to the *final* version of the DCIA VBPs: they also try to prescribe rules of conduct for applications so diverse that critical components of the resulting "best practices" inevitably suffer from one of two limitations.

First, some "best practices" simply lack meaningful content because no specific "practice" could be "best" as applied to the whole range of applications governed by the VBPs. For example, perhaps the most critical provision of the VBPs requires developers to disable sharing of "sensitive" files by default. Yet no meaningful definition of "sensitive is provided and none could be: the set of files that would be "sensitive" to share using a given program could vary enormously. On a "closed" network that will distributed only authorized, authenticated files, no file types might be "sensitive." On a network like Gnutella, there would appear to be few file types that would not tend to be potentially harmful to share.

Second, and conversely, some "best practices" may make no sense as applied to some programs. For example, the VBPs presume that files downloaded by a user of any file-sharing program are never "sensitive" and thus inevitably safe to "share" by default. As applied to a program like LimeWire, I am aware of no evidence that would suggest that it would be safe for a user to "share" the types of files that users typically download.

Neither of these limitations suggest that the DCIA VBPs reflect a dishonest attempt to redress inadvertent file sharing. But they do suggest that the utility of the VBPs will depend heavily upon the good faith and common sense of the entities implementing them. To an entity trying to act responsibly, the VBPs could provide useful guidance. But to a negligent, reckless or willful entity, the VBPs could provide loopholes and excuses. Consequently, it is important to examine how the VBPs were implemented by LimeWire LLC in LimeWire 5.

The implementation of the VBPs in LimeWire 5 actually *perpetuates* some of the worst inadvertent sharing of sensitive files caused by previous versions: DCIA has praised LimeWire 5 as a "poster child for compliance" with its VBPs. But LimeWire's "compliance" seems rather cynical. In effect, LimeWire concluded that the VBPs let it remediate those consequences of inadvertent sharing that were clearly hurting both LimeWire users *and LimeWire LLC*—but *perpetuate* those consequences of inadvertent sharing that hurt users, but potentially benefited LimeWire LLC.

Moreover, those convenient results should have followed only if LimeWire could have reasonably concluded that a family's digital photos, its home movies, its entire music collection, and all of its scanned documents, like tax returns, are not "Sensitive File Types" when broadcast over a Gnutella file-sharing network known to be used by identity thieves and pedophiles. Because those conclusions do not seem *reasonable*, serious problems seem to affect the implementation of the VBPs in LimeWire 5.

LimeWire LLC began promoting the availability and advantages of LimeWire 5 after alert reporters documented the latest debacle that that distributors of file-sharing programs had inflicted upon the public: a report by Today Investigates revealed that the residents of New York state alone were inadvertently sharing over 150,000 tax returns. This report also profiled the Bucci family—identity theft victims who had inadvertently "shared" their tax return because their preteen daughters had downloaded and misconfigured LimeWire.

LimeWire responded by assuring its users that upgrading to LimeWire 5 would halt inadvertent sharing without resort to the rash delete-LimeWire-right-now strategy used by the Bucci family:

> "[a LimeWire spokesperson] said, 'Our newest version, LimeWire 5.0, by default cannot share sensitive file types such as spreadsheets or documents. In fact, the software can not share any file or directory without explicit permission from the user."
>
> "With LimeWire 5, the latest version of the software, 'LimeWire has ensured the complete lockdown of the safety and security of LimeWire users, said [Lime Group CEO] Gorton.'"

Unfortunately, widely repeated statements like these appear to be potentially misleading. And worse yet, LimeWire LLC may have known that.

For example, consider the claim that LimeWire made to LimeWire-using families who happened to be mere *constituents* of U.S. Representative Edolphus Towns: "[LimeWire 5] can not share any file or directory without explicit permission from the user." But when making claims to the Representative himself—who happens to be the Chairman of the House Committee on Oversight and Government Reform—LimeWire *added* a critical caveat: "for new LimeWire users, LimeWire 5 does not share *any* file of *any* type without explicit permission from the user."

The Chairman and his constituents were thus told different stories about how LimeWire 5 affects its users. Ordinary families who might have deleted LimeWire could have concluded that if they upgraded to LimeWire 5, then "the software can not share any file or directory without explicit permission from the user." But the Chairman was told that such benefits would accrue *only* to brand new users of LimeWire 5—not to users of previous versions of LimeWire who upgraded to LimeWire 5.

So it is *almost* déjà vu all over again: in 2003, a DCIA member-company distributing the file-sharing program KaZaA "remediated" catastrophic inadvertent sharing by perpetuating its effects. In 2009, a DCIA member-company distributing the file-sharing program LimeWire "remediated" catastrophic inadvertent sharing by perpetuating *some of its effects*—the subset that could materially benefit the Gnutella file-sharing network, albeit at the expense of common sense and user safety. Consequently, were a family like the one profiled by Today Investigates to try to resolve their inadvertent file-sharing problem by upgrading to LimeWire 5, that family would probably keep "sharing" many files that are clearly "sensitive" within any reasonable definition of that term—perhaps even their tax returns.

To understand what has happened, and why it might have happened, one need only understand a bit about the harm that catastrophic inadvertent sharing can inflict upon families, and the potential benefits that it could confer upon the distributor of a file-sharing program used mostly to download unlawful copies of popular music, popular movies, and "adult" images.

When inadvertent sharing affects people like the family profiled by Today Investigates, disclosure of a tax return is almost surely just one symptom of a much broader problem. It is very unlikely that families "share" a tax return because an adult decided to store it in the hard-to-access default "Shared" folder created by programs like LimeWire. Consequently, the over

150,000 tax returns being inadvertently shared *in one state alone* are probably being shared along with *all* files that a family has stored on its home computer in its *My Documents* folder and all of its subfolders. In my 2007 testimony to the House Committee on Oversight and Government Reform, I explained what could happen to my family were a cousin or babysitter to inadvertently and recursively share the *My Documents* of our family computer:

> I would end up sharing bank statements; tax returns; passwords for investment accounts; scans of legal, medical, and financial records; all my family photos; my children's names, addresses, and Social Security numbers; and a scan of the sign that designates the car authorized to pick up my daughter from preschool. And I would also share over 3,000 copyrighted audio files. With one mistake, I could be set up for identity theft, an infringement lawsuit, or far worse.

Ironically, the files that could inflict the worst harm if "shared," (the image files that could endanger my children and the document files that could end my career), seem to confer no real benefits upon a distributor of a file-sharing program. As LimeGroup CEO Mark Gorton testified in 2007, the only two "major use[s]" of his program are downloading music and downloading movies. And he might have added, *popular* music and videos, because, as a LimeWire developer has noted: "here's modern p2p's dirty little secret: it's actually horrible at rare stuff." Moreover, in addition to these two "major" uses, there is also a third potentially material use: downloading image files. Most are probably "adult" images, but infringing images of the "box" art on popular CDs and DVDs are also traded.

Interestingly, when existing LimeWire users upgrade to LimeWire 5, the program will *perpetuate* any inadvertent sharing of at least three categories of files: audio files, video files, and image files. Moreover, actually *using* LimeWire 5 to download a file can also cause inadvertent sharing: by default, LimeWire 5 shares most downloaded files without any "express permission from the user." So LimeWire did not misstate the behavior of its program when it told Chairman Towns that "for new LimeWire users, LimeWire 5 does not share *any* file of *any* type without explicit permission from the user." But it did fail to note that this happy state probably ends when the average user downloads a file.

One can easily see why the interests of the developer of a Gnutella-based file-sharing program that had caused widespread, catastrophic inadvertent sharing would be served by "remediation" efforts that perpetuated all previously caused inadvertent sharing of *existing* media files and could cause future inadvertent sharing of *downloaded* media files. But for the following reasons, it is difficult to see why those should be the results of remediation efforts driven by an informed and genuine concern for the interests of users, their families and employers, and the public.

Image Files: As my 2007 testimony indicated, users who have inadvertently shared sensitive personal files tend to "share" two types of image files. First, they tend to share all of their family photos, and it is certainly not safe or responsible to "share" these over a file-sharing network frequented by pedophiles. Second, consumer copiers and scanners often save scanned files in image-file formats like .tff and .jpg. As a result, were a family affected by inadvertent sharing to have *scanned* tax records stored on its home computer, an upgrade to LimeWire 5 would merely perpetuate its exposure to the identity thieves now data-mining the Gnutella file-sharing network.

Nor is identity theft the worst potential consequence of perpetuating inadvertent sharing of media files. I thought that I had made this clear enough in my 2007 testimony when I described the potential consequences of inadvertent sharing to my family and concluded that we could be "set up for identity theft, an infringement lawsuit, *or something far worse*." Unfortunately, some program distributors seem to have missed the point.

So I let me be even clearer: when I said "or something far worse," I meant that inadvertent sharing of files on my family computer, (including home movies and image files like digital photos and scanned documents), could disclose identifying information about my children to LimeWire-using pedophiles. *See, e.g., United States v. Park,* 2008 U.S. Dist. LEXIS 19688, (D. Neb. March 13, 2008) (a LimeWire user shared videos of an adult raping a little girl "bound with a rope and being choked with a belt"); *United States v. O'Rourke,* 2006 U.S. Dist. LEXIS 1044 (D. Ariz. Jan. 12, 2006) (a LimeWire user was held to be a "danger to the community" because he allegedly shared many "extraordinarily abusive" images of "horrific child abuse" inflicted on "a very young girl, with hands bound and mouth gagged"); *United States v. Postel,* 524 F. Supp.2d 1120, 1123 (N.D. Iowa 2006) (a LimeWire user used shared child pornography to "groom" the girl that he molested for four years).

Sadly, these are risks that LimeWire 5 can perpetuate. Nevertheless, Lime Group CEO Mark Gorton has told the public and Congress that "LimeWire 5 put the final nail in the coffin of inadvertent sharing of sensitive files."

Video Files: Increasingly inexpensive and sophisticated camcorders and video-editing software ensure that many people now archive family movies on their home computers—and these files are not "safe" to "share" for the reasons set forth above. Moreover, to the extent that users also have copies of popular commercial films, these will tend to be copyrighted, and thus not safe to "share" over the Gnutella file-sharing network.

Audio Files: As my 2007 testimony indicated, users who have inadvertently shared sensitive personal files will also tend to be sharing entire music collections—potentially thousands of copyrighted audio files of popular music. These files generally cannot be legally or safely shared, and it is particularly dangerous to share an entire music collection because users sharing hundreds or thousands of audio files are those most likely to be targeted by copyright enforcement actions.

Downloaded Files: At first, early Gnutella-based file-sharing programs had "symmetrical" downloading and uploading capabilities: in other words, just as a user then had to take—and must still take—a voluntary, deliberate act in order to *download* a given file, a user also had to take a voluntary, deliberate act in order to *upload* (or "share") a given file over the Gnutella file-sharing network. Unfortunately, computer-science researchers studied the results and concluded that there was not enough "voluntary cooperation between users" and that developers would have to rely, instead upon "technological features to induce users to share." One of the "features" suggested was automatic sharing of files that users download. As a result, one *knowing* act, a download, can then trigger an *unknowing* act, an upload that could distribute the downloaded file to others.

That default—share downloaded files automatically—is still the default setting for most file types in LimeWire 5. And the problem with that default setting is revealed in the following 2008 testimony given in federal court by a LimeWire developer. He testified, under oath, that "meaningful" default settings are those "set by the programmers" that "make sense and are in the user's best interest."

Hence the problem: programs like LimeWire are used primarily to download infringing copies of media files that are *illegal* to re-distribute. Consequently, a reasonable LimeWire developer should not conclude that a default re-distribution feature is actually in the average user's "best interest." As a practical matter, it simply is not.

Worse yet, because LimeWire 5 still "shares" media files by default, (without any "explicit permission"), and because it perpetuates all prior inadvertent sharing of media files—it seems sure to compromise interests even more important than the federal civil rights called "copyrights" that helped the United States become the world's most successful producer and net exporter of expressive works. Sadly, those interests may include the federal government's ability to protect children from pedophiles.

And this is not a hypothesis. It is not an abstract could-be threat. It is not arm-waving speculation about a theoretical parade-of-horribles. It is a statement about what has happened and what is increasingly likely to happen again. And worst of all, though the facts set forth below were known to LimeWire LLC long before they were known to me, their obvious implications do not seem to be reflected in the design of LimeWire 5.

The design of file-sharing programs like LimeWire and network protocols like Gnutella just so happen to make them attractive to teenage and preteen children who do not want to get caught illegally "sharing" popular music and movies. But for similar reasons, such programs and networks are also attractive to pedophiles who do not want to get caught "sharing" illegal child pornography. As a result, pedophiles have gravitated to the Gnutella network, and a wave of file-sharing-related child-pornography prosecutions is now moving through the federal courts.

Worse yet, some of these defendants are not just alleged viewers of child pornography—they are alleged child predators. When federal prosecutors catch such defendants, they can, of course, charge them with possession of child pornography. But because possession is a rare strict-liability criminal offense, long jail terms are generally not imposed for a conviction.

Consequently, if prosecutors bring criminal charges against a LimeWire user who appears to be, as one court found, "a danger to the community," they may also charge a more serious crime: *knowing distribution* of child pornography. A knowing-distribution conviction can sequester dangerous predators from their potential victims for a long time—*but only if the prosecutor can prove beyond a reasonable doubt that the defendant knew that he was distributing media files containing child pornography.*

Predictably, the task of defending most file-sharers charged with knowing distribution of child pornography falls upon the federal public defenders who serve an essential role in our justice

system and have both a legal and ethical duty to vigorously defend their clients. And those public defenders have realized that inadvertent file-sharing provides a potential complete defense to a defendant charged with knowing distribution of child pornography.

As a result, LimeWire developers are no longer just writing code, they are also testifying in criminal child-pornography cases. Unfortunately, as the following testimony from a March 2008 trial shows, the design of the LimeWire program has ensured that the testimony of LimeWire employees can be as valuable to the defendant as to the prosecution:

> PROSECUTOR: Your Honor, I don't believe it is possible to share files inadvertently.
>
> ***
>
> THE COURT: … [D]oes your software make it possible make it possible for people to accidentally share personal files or sensitive data?
>
> LIMEWIRE DEVELOPER: Accidentally?
>
> THE COURT: Yes.
>
> LIMEWIRE DEVELOPER. Yes.

While such testimony did not prevent a conviction in this particular case, the difficulty of proving scienter in file-sharing child-pornography cases has already had consequences. For example, in *United States v. Park*, 2008 U.S. Dist. LEXIS 19688 (D. Neb. March 13, 2008), a defendant had used LimeWire to share, *inter alia*, a three-hour video depicting a little girl "bound with a rope and being choked with a belt by what appeared to be an adult male.'" Nevertheless, that defendant secured a reduced sentence because he "lacked an understanding of the software and thus … the knowledge to distribute the illegal wares that he possessed."

Consequently, for over 14 months, LimeWire LLC has known that unless LimeWire 5 comprehensively foreclosed *any* potential inadvertent sharing *even of mere media files*, it could compromise the ability of prosecutors to sequester dangerous pedophiles from their potential victims. Nevertheless, LimeWire LLC *chose* to design LimeWire 5 so that it would *perpetuate* all inadvertent sharing of all previously shared media files and *continue* to automatically "share" all media files that a user might download.

To conclude, I must note an important point: I do agree that the implementation of the DCIA VBPs reflected in at least *non-beta* versions of LimeWire 5 does seem to make *some* consequential changes that should significantly reduce *some types* of inadvertent file-sharing, including some long known to be very dangerous. These are improvements. Nevertheless, I cannot conclude that these improvements really do signal an overdue-but-now-genuine commitment to "user-safety-first" file sharing. Indeed, in some cases, they seem to reflect little more than the belated admission of the long obvious.

For example, in a May 1, 2009 letter to Chairman Towns of the House Committee on Oversight and Government Reform, Lime Wire LLC heaped glowing praise upon itself because LimeWire 5 now disallows sharing of document file-types by default. But this change can only be welcomed—not praised. After years of countless disasters, Lime Wire LLC has now belatedly conceded that which was obvious to *responsible* developers of file-sharing programs in the year 2000 and that which was *made obvious* to all others in 2002.

In 2000, lawyers who had misread the Supreme Court's famous *Sony* decision began giving developers of file-sharing programs the sort of bad advice later offered in the Electronic Frontier Foundation's infamous "whitepaper": "If your product is intended to work solely as a mechanism for copyright piracy, you're asking for legal trouble…. For example, if you're developing a file-sharing system or distributed search engine, support all file types, not just MP3 or Divx files."

Nevertheless such advice was rejected by the developers of the first popular file-sharing program, Napster. Its developers examined other services that had followed such advice and "often turned up documents from computers whose owners didn't realize that the material could be seen by others." This empirical research convinced Napster's developers that sharing document files by default would be "a big mistake." Joseph Mein, All the Rave 239 (2003). In 2002, computer-science research later praised by a DCIA member-company derived similar conclusions from more formal empirical analysis. *See* Nathaniel Good & Aaron Krekelberg, *Usability and Privacy: A Study of KaZaA Peer-to-Peer File Sharing*, (2003).

Consequently, Lime Wire's 2009 decision to stop sharing document files by default is welcome—and troubling. Tomorrow, a *new* security problem with file-sharing programs may arise—a problem whose deadly serious consequences and simple solution would be obvious to both responsible program distributors and computer scientists. Should this happen, would we again need to endure nine years of needless, recurring security disasters before LimeWire LLC grasped the problem, perceived its long-published solution, and implemented it?

Possibilities like this—combined with the other factors discussed above—require me to conclude that I would only undermine and discredit the cause of voluntary self-regulation were I to advise this Committee that it remains a viable option in this case.

I thank the Subcommittee and the sponsors of H.R. 1319 for their careful attention to these important issues, and I look forward to providing any further assistance that might be useful to the Subcommittee and the sponsors of H.R. 1319.

Appendix A to
the Testimony of Thomas D. Sydnor II,
Office of International Relations,
United States Patent and Trademark Office
July 24, 2007

The following five pages illustrate each of the five "features" discussed in the USPTO Report.

Redistribution Features

Description: By default, almost all filesharing programs will share all files that a user downloads from a filesharing network. Programs usually do this by creating a new, empty folder when they are installed; this folder has a name like "Shared" or "My Downloads." By default, this folder stores downloaded files, and all files in it are shared. So unless a user changes the default settings or physically moves downloaded files, all downloaded files will be shared.

Users may receive no or misleading information about redistribution features during a filesharing program's installation-and-setup process: Some programs, like eDonkey, do not inform users about redistribution during their installation. Other programs provide potentially misleading information: For example, the installation process of a 2003 version of Morpheus makes it look like *no* folder would be shared by default. But this version of Morpheus had a redistribution feature—the folder used to store downloaded files was shared by default.

Users may receive no or little information about sharing when a filesharing program is operating: Research shows that most users of filesharing programs do not want to share files from their computers; they only want to search for and download files shared by others. Some programs, like eDonkey, provide download-only users with no information about their shared files on their main interface. Other programs do provide very little information about sharing on the main interface. LimeWire, for example, provided *less* information about shared files on the main interface over time.

Search-Wizard Features

Description: A search wizard scans the hard drive of a user's computer and presents the user with a list of folders that the user might want to share with others. Sharing caused by search wizards is usually recursive: The user will share not only all files stored in a folder selected by the wizard, but also all files stored in any of its subfolders.

Problems: The problems with search wizards are evident in this screenshot of the results screen of a BearShare search wizard from 2005:

Wizards will "recommend" the sharing of folders that are inherently unsafe to share: This wizard recommends that the user share "My Documents." By default, almost all user-created files will be stored in this folder or its subfolders. It would never be wise to share "My Documents." But the wizard recommends that the user do so.

Wizards may not disclose recursive sharing: This wizard tells the user that the folder "My Documents" has been selected for sharing, but not that the *files* stored in this folder will be shared. More importantly, it does not disclose that this folder will be shared *recursively*: All of the hundreds of files stored in its scores of *subfolders* will also be shared.

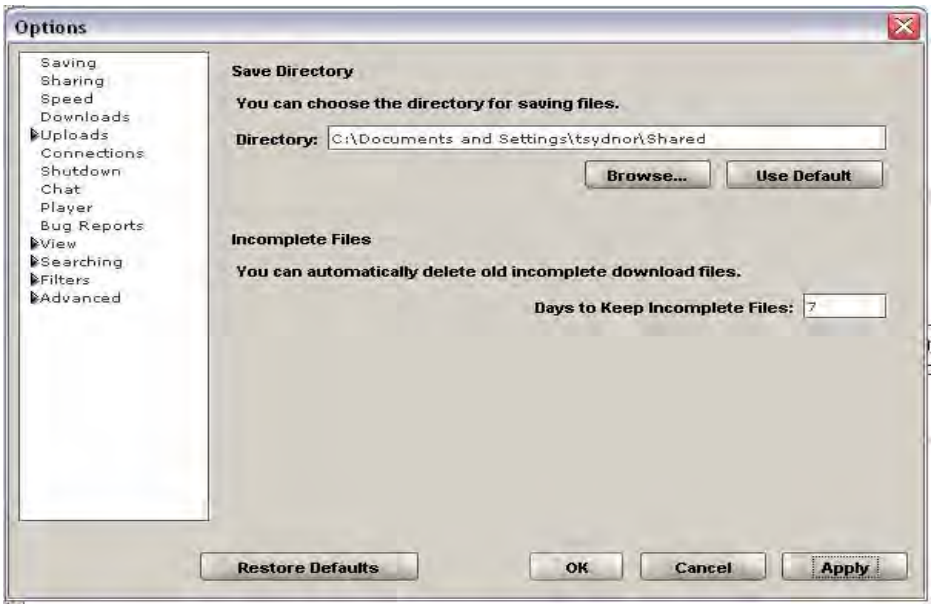
A user must have perfect information about the location of all his files and folders to respond rationally to a wizard's recommendations: *Usability and Privacy* reminded distributors that computer users are "notoriously bad" at remembering folder-subfolder structures and relationships. Unless users understand exactly how folders recommended for sharing relate to all other folders on their computers, they cannot evaluate the wizard's recommendation.

Wizards usually run during the installation-and-setup process, when the user will be most unfamiliar with the program and its potential effects: Users will encounter wizards when they are least familiar with a program and its capabilities—and thus most likely to defer to "recommendations" from its distributors.

Share-Folder Features

Description: When filesharing programs are installed, they create an empty folder, (usually called "Shared" or "Downloads"), that will store copies of downloaded files. A share-folder feature lets the user select another folder in which to store downloaded files, but it does so through an interface that fails to warn the user that existing files in the selected folder will be shared or that subfolders will be shared. Share-folder features usually cause recursive sharing: The program will share not only existing files stored in the selected folder, but also existing files stored in all subfolders of the selected folder.

Problems: The problems with share-folder features are evident in this screenshot of the Share-Folder feature in a 2004 version of LimeWire:



Nothing on this screen indicates that this feature will *share* files: Users are only told that they are selecting a "Save Directory" to store files downloaded from other users. They are not told that all files in this folder will be shared.

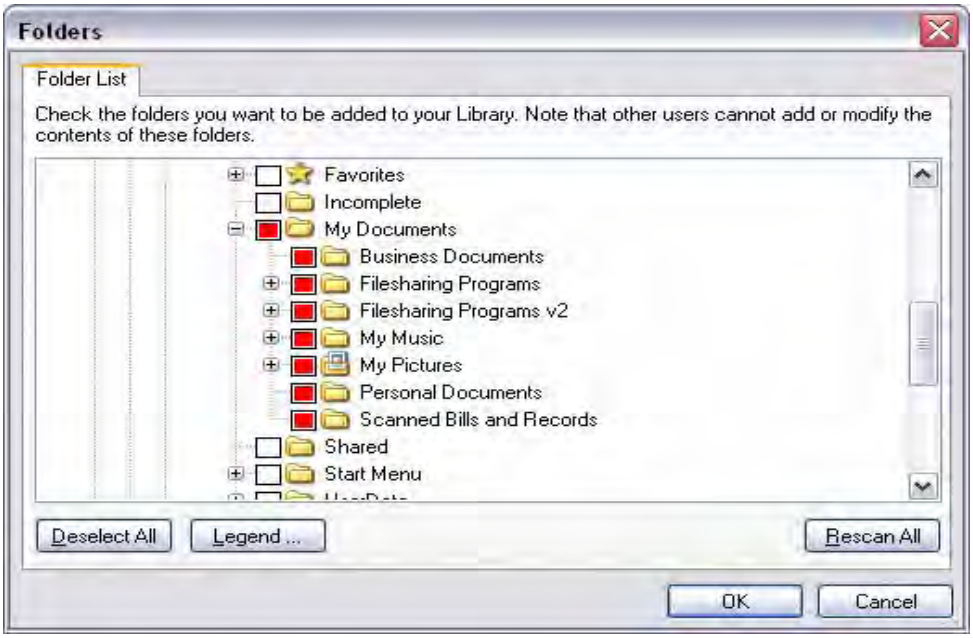
Recursive sharing is not disclosed: The share-folder feature also fails to disclose that the "Save Directory" will be shared recursively: The program will share not only all files stored in the folder selected as the "Save Directory," but also all files stored in all of its subfolders.

"Librarying" is not disclosed: This share-folder feature has a button labeled "Use Default." If the user has set the "Save Directory" to a folder that would not be safe to share, like "My My Music," pressing "Use Default" will reset the "Save Directory" to the special folder that LimeWire creates when it is installed. But the program still keep sharing "My Music" recursively, even though it is no longer the "Save Directory." We called this "librarying." In short, *every use of a librarying share-folder feature will cause the user to share more files and folders, never less.*

Partial-Uninstall Features

Description: If a user "uninstalls" most filesharing programs, (for example, by using the "Remove Program" function on the Control Panel in Microsoft Windows), these programs will appear to uninstall. But the process will leave behind a data file that will cause any subsequent installation of any version of the same program to automatically share all folders that were shared by the "uninstalled" version of the program.

Problems: The problems with partial-uninstall features are evident in the following screen shot, which shows the folders that were shared by default, without notice to the user, when a 2005 version of BearShare was installed on a computer on which no filesharing program was installed.



Thanks to a partial uninstall feature, this user is now sharing his "My Documents" folder recursively, by default, and with no notice.

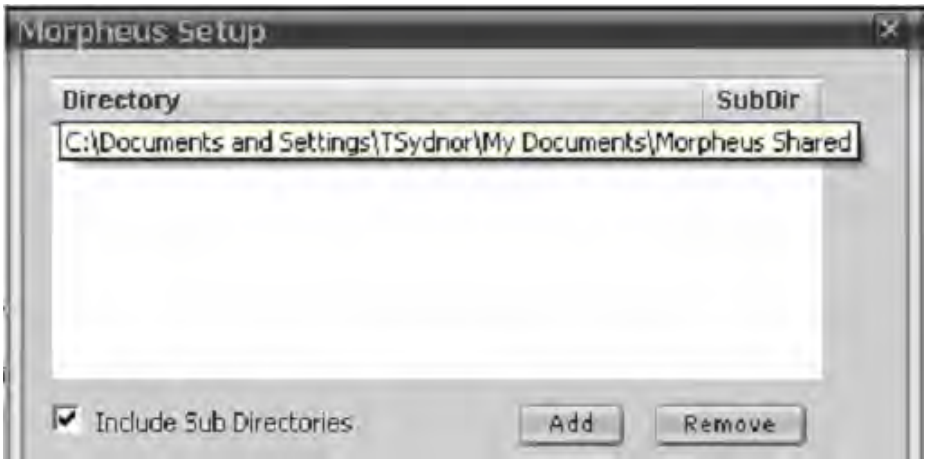
These features prevent users from correcting mistakes by removing the program: Users who discover that they are inadvertently sharing files might well try to correct their errors by removing the program and "starting over" with a new default installation. These features ensure that there is no starting over.

These features are particularly dangerous when more than one person uses a given computer: Users have been warned to avoid inadvertent sharing by using the "default" settings created when a filesharing program is installed. But when more than one person uses a computer, like a family computer, users have no way to know how a "default" installation of a filesharing program will behave.

Coerced-Sharing Features

Description: Coerced-sharing features make it more difficult for users to halt sharing caused by redistribution, search-wizard, share-folder and partial-uninstall features. Different programs achieve this different ways, but most coerced-sharing features ensure that users who try to stop sharing particular folders will fail while thinking that they have succeeded.

Problems: The problems with coerced sharing features are evident in the following two screenshots taken during the installation-and-setup process of a 2006 version of Morpheus:



Users who guess that this screen lists the folders that users will share might realize that Morpheus has a redistribution feature. These users might then try to halt sharing of downloaded files by selecting this folder and clicking the "Remove" button. If so, Morpheus will provide the following feedback on the effects of the users' actions:

The list of shared folders is now empty, so users would probably conclude that they will not share downloaded files because they have halted all sharing of all folders. But this would be wrong: The users' actions have had no effect; the folder that stores downloaded files will still be shared. This sort of misleading coerced-sharing feature also makes it more difficult for users to correct the effects of all the other features discussed above.

Comments of Thomas D. Sydnor II,
Director of the Center for the Study of Digital Property and Senior Fellow at
The Progress & Freedom Foundation
Before the
Intellectual Property Coordinator
Washington, D.C. 20554

In the Matter of	)
	)
Coordination and Strategic Planning of the	)
Federal Effort Against Intellectual Property	)
Infringement: Request of the Intellectual	)
Property Enforcement Coordinator	)
	)

COMMENTS of THOMAS D. SYDNOR II, SENIOR FELLOW AND DIRECTOR OF THE CENTER FOR THE STUDY OF DIGITAL PROPERTY AT THE PROGRESS & FREEDOM FOUNDATION

Thomas D. Sydnor II,
The Progress & Freedom Foundation
1444 Eye Street, NW, Suite 500
Washington, D.C. 20005
March 24, 2010

I. DISCUSSION.

These comments are filed on behalf of Thomas D. Sydnor II, Director of the Center for the Study of Digital Property and Senior Fellow at the Progress & Freedom Foundation, a § 501(c)(3) foundation dedicated to studying the digital revolution in communications technologies and its larger effects upon society. These comments are filed in my personal capacity, so they may not represent the views of the Progress & Freedom Foundation or any of its other Fellows, Board Members, employees, or contributors.

These comments will be deliberately brief. The Intellectual Property Enforcement Coordinator ("IPEC") should be commended for framing many highly relevant questions. In most cases, others are better situated than I to address most of them. Consequently, these comments will focus on two general policy questions arising from the questions posed in the IPEC's Request for Written Submissions ("RWS").

First, the RWS "seeks written submissions identifying threats to public health and safety posed by intellectual property infringement." The data-security company Tiversa, Inc., computer scientists, and I have extensively documented the causes and consequences of one set of such threats: the threats arising from inadvertent file-sharing by users of piracy-adapted "peer-to-peer" file-sharing programs like Grokster, Morpheus, KaZaA, some versions of Bearshare, and LimeWire.[1] Inadvertent file-sharing caused by these programs has created what the FTC has called "widespread" threats to national, military, corporate, and personal data security.[2] These threats have endangered American governments, soldiers, businesses, families, and children. These threats have repeatedly empowered, Iran, China, terrorists, identity thieves, and sadistic pedophiles seeking to evade prison or to select their next victim.

Second, the RWS asks commenters to "priorit[ize]" their most important proposals for achieving an array of IPR-related goals including "[d]isrupting and eliminating infringement networks in the U.S. and in other countries." One of the IPEC's priorities should be encouraging U.S. law-enforcement agencies to target the most harmful manifestations of mainstream Internet copyright piracy.

During the preceding Administration, federal law-enforcement agencies did an absolutely miserable job of standing up and opposing pervasive, threat-to-public-health-and-safety creating, violations of the

[1] As the term is used here, "piracy-adapted" file-sharing programs, protocols, and websites include those that happen to be—intentionally, knowingly, recklessly or negligently—well-suited to the needs of users who want to use them to infringe copyrights in popular music, movies, software, books and images. The modifier "piracy-adapted" is used to note that not all implementations of peer-to-peer file-sharing technologies are necessarily malign or likely to cause data-security problems.

[2] Federal Trade Commission, *Widespread Data Breaches Uncovered by FTC Probe,* (Feb. 22, 2010) at http://www.ftc.gov/opa/2010/02/p2palert.shtm.

federal civil rights—the copyrights—that have made American creators and creative industries the world's most successful commercial creators and net exporters of a vast array of expressive works. The IPEC should ensure that the same cannot be said about federal law-enforcement agencies during the Administration of President Obama.

A. Inadvertent file-sharing is a well-documented threat not only "to public health and safety posed by intellectual property infringement" in general, but also to the daughters of Presidents Obama and Bush.

The RWS "seeks written submissions identifying threats to public health and safety posed by intellectual property infringement." 75 Fed. Reg. at 8137. Such submissions must "include a detailed description of the threat, identify the source of the information substantiating the existence of that threat and provide a copy of or a citation to each such source." *Id.*

I have written and testified extensively about the causes of one such "threat to public health and safety posed by intellectual property infringement": inadvertent file-sharing. "Inadvertent file-sharing" occurs when users of piracy-adapted file-sharing programs like KaZaA, Grokster, Morpheus, and LimeWire end up "sharing" files that no sane adult would ever deliberately "share" with anonymous strangers.[3]

In the past, threats to public safety posed by intellectual property infringement rarely arose from copyright piracy. Indeed, such threats tended to arise only from the counterfeiting of certain types of physical goods, like electrical extension cords and pharmaceuticals or when violent criminal syndicates became involved in any type of IPR infringement, including copyright infringement.[4]

In short, a mere decade ago and absent the involvement of violent criminal syndicates, we might have safely laughed at anyone who suggested that the infringement of copyrights in, say, popular music—the distribution of unauthorized copies of the songs of Ms. Brittany Spears—could possibly create "threats to public health and safety…."

Today, no one is laughing. Distributors of file-sharing programs that are almost always used to infringe copyrights—programs like the Gnutella-protocol-base program LimeWire—have proven that in the Internet era, even the piracy of popular music and movies can create severe, enduring, documented threats to national, military, corporate, and personal data-security—not to mention copyrights and creative industries. Here are a few of the documented consequences of inadvertent file-sharing:

---

[3] . *See* Thomas D. Sydnor II, John Knight & Lee A. Hollaar, *Filesharing Programs and "Technological Features to Induce Users to Share"* (U.S. Patent & Trademark Office 2007) [hereinafter "*Filesharing Programs*"]; Thomas D. Sydnor II, John Knight & Lee A. Hollaar, *Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform* (PFF 2007) [hereinafter "*Revisited*"]; Thomas D. Sydnor II, *Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5* (PFF 2009) [hereinafter "*Re-Invented*"]. Citations and links to these studies and other relevant testimony and studies are provided in Appendix A.

[4] *See, e.g.,* Gregory F. Treverton, *et al*., *Film Piracy, Organized Crime and Terrrorism* (RAND Corp. 2009) at http://www.rand.org/pubs/monographs/2009/RAND_MG742.pdf.

- Inadvertent file-sharing disclosed information about the daughters of President Bush to a potential assassin who was apprehended mere miles away from the President's Crawford Ranch.

- Inadvertent file-sharing disclosed information about the escape routes and safe houses that were to be used by the First Lady and the daughters of President Obama.

- Inadvertent file-sharing disclosed information about President Obama's new Marine One helicopter to the Iranians and terabytes of data about the Joint Strike Fighter to the Chinese.

- Inadvertent file-sharing disclosed risk assessments that would tell terrorists how to attack American cities, like Chicago, in the way that would maximize the number of dead American civilians.

- Inadvertent file-sharing disclosed schematics of the Pentagon's secret computer backbone—complete with router addresses and passwords.

- Inadvertent file-sharing has disclosed hundreds of government documents classified "Secret."

- Inadvertent file-sharing has caused widespread breaches of corporate and personal security that have empowered identity theft, medical identity theft, pedophilia, and the distribution of child pornography.

My research into the causes of inadvertent sharing makes the root causes of these and other disasters painfully clear: distributors of piracy-adapted file-sharing programs counted on unsophisticated consumers and children to do all the dirty work of copying and distribution required to build a global piracy syndicates. But while it is not particularly difficult to encourage people to *download* files that they do not currently possess, it is very difficult to convince people to *upload* (or "share") files that they already possess when doing so imposes burdens and risks upon the uploader without any corresponding benefit.

Appendix A contains a detailed listing of sources documenting the causes and consequences of inadvertent file-sharing, and I have attached additional sources along with these Comments.

B. The IPEC's Highest Priorities Should Include Urging Federal Law-Enforcement Agencies to Bring the Moral Force of Federal Law Enforcement to Bear on the Architects of Mainstream Internet Piracy.

The RWS also asks commenters to "priorit[ize]" their most important proposals for achieving an array of IPR-related goals including "[d]isrupting and eliminating infringement networks in the U.S. and in other countries." 75 Fed. Reg. at 8137-38. I strongly commend the IPEC for making this request of commenters because it speaks eloquently to her deep understanding of the challenges inherent in the task before her.

In the space of a few decades, IPRs have become enormously important to a vast array of important American domestic and foreign interests—from information technology to agriculture. As a result, there are so many worthy tasks that the IPEC *could* do that the IPEC's most important task may be prioritizing the tasks that should be done *first*. The IPEC should thus be commended for asking commenters to acknowledge the realities confronting the IPEC and her staff.

The IPEC should thus prioritize efforts to encourage federal law-enforcement authorities, including the U.S. Department of Justice and the Federal Trade Commission, to bring the moral and practical authority of federal law-enforcement agencies to bear against the architects of "mainstream" Internet piracy. Unless and until federal law-enforcement agencies do so, the United States will have ever-diminishing credibility as a champion of intellectual-property rights.

To be clear: the IPEC and the Obama Administration have inherited this problem—they have not caused it. Nevertheless, it is a very serious problem that must be remedied if the United States is to retain its credibility as an international proponent of intellectual-property rights.

Consider where we are today. During the *Grokster* litigation, distributors of piracy-adapted file-sharing programs like Grokster, Morpheus and LimeWire strongly condemned copyright owners for failing to enforce their rights against the college students, teenagers and children who used their programs. But after such condemnation actually convinced judges that the distributors of such programs could not be liable just because they *intended* to profit from piracy by inducing children to do their dirty work, copyright owners did sue the individual users of such programs.[5]

And when the inevitable happened—when some of the most egregious infringers of copyrights using such programs turned out to be preteen children—then the same distributors of the same Grokster, Morpheus, and LimeWire programs publicly wept crocodile tears over the perfidy of the copyright owners who had done, well, exactly what the distributors Grokster, Morpheus, and LimeWire programs said that they should have done:

> [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.[6]

Predictably, when the resulting *Grokster* case got to the Supreme Court, the Defendants feared that the federal government might object to the cynical shell game that they had played with the federal civil

---

[5] Collections of these and other *Grokster* briefs are available at http://www.copyright.gov/docs/mgm/index.html or http://w2.eff.org/IP/P2P/MGM_v_Grokster/.

[6] 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).

rights of American artists and the safety of American children.[7] As a result, they cited fear of "criminal investigation" as their basis for refusing to let the United States Department of Justice review the litigation record that could have revealed their conduct. Nevertheless, the United States Supreme Court then unanimously found in the *Grokster* record "clear," "overwhelming" and "replete" evidence that the *Grokster* Defendants intended to induce users of their programs to infringe copyrights in order to create the largest global, for-profit copyright-piracy syndicates that the world has ever seen.[8] Subsequently, both the Department of Homeland Security and the U.S. Patent & Trademark Office would reveal that

And what, during the preceding Administration, did the U.S. Department of Justice and the Federal Trade Commission do in response? They did nothing. Absolutely nothing. Circumstances including the aftermath of the 9/11 attacks could explain such inaction, but only temporarily.

In short, the IPEC should strongly encourage federal law-enforcement agencies to take action against the most egregious and pervasive forms of Internet copyright piracy. New technologies should not obscure basic facts: nothing about the Internet generally or file-sharing programs in particular suggests that it should be easier today to convince informed adult consumers to bear all of the risks of direct liability for severe damages inherent in any widespread copyright-piracy operation. Consequentely, when that appears to be happening, reasonable federal law enforcement agencies should infer that some sort of fraud is being perpetrated and move to stop it—immediately. I will be happy to provide further supporting evidence to support this conclusion to any federal law-enforcement agency that might be interested.

In conclusion, I would like to thank the IPEC, the Office of Management and Budget and the Executive Office of the President for the opportunity to address these important issues.

[7] *See, supra,* n.5.
[8] *MGM Studios, Inc. v. Grokster, Ltd.,* 545 U.S. 913 (2005).

APPENDIX A

SOURCES ON INADVERTENT FILE-SHARING

HEARINGS AND TESTIMONY:

Overexposed: The Threats to Privacy and Security on Filesharing Networks: *Hearing Before the H. Comm. on Government Reform,* 108 Cong. (2003)
at http://www.access.gpo.gov/congress/house/pdf/108hrg/88016.pdf.

The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of Peer-to-Peer File-Sharing Networks?: *Hearing Before the S. Comm. on the Judiciary*, 108 Cong. (2003)
at http://www.gpo.gov/congress/senate/pdf/108hrg/91213.pdf.

Inadvertent File-Sharing Over Peer-to-Peer Networks: *Hearing Before the H. Comm. on Oversight and Government Reform,* 110 Cong. (2007)
at http://oversight.house.gov/index.php?option=com_content&task=view&id=2465&Itemid=2.

H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act: Hearing Before the Subcomm. On Commerce, Trade, and Consumer Protection (May 5, 2009) http://energycommerce.house.gov/index.php?option=com_content&view=article&id=1608:energy-and-commerce-subcommittee-legislative-hearing-on-hr-2221-the-data-accountability-and-trust-act-and-hr-1319-the-informed-p2p-user-act&catid=129:subcommittee-on-commerce-trade-and-consumer-protection&Itemid=70; *see also id.,* Prepared Statement of Thomas D. Sydnor II (May 5, 2009)
at http://www.pff.org/issues-pubs/testimony/2009/090505_P2P_sydnor_testimony.pdf; *id.* Prepared Statement of Robert Boback
at http://energycommerce.house.gov/Press_111/20090505/testimony_boback.pdf.

Inadvertent File Sharing over Peer-to-Peer Networks: How It Endangers Civilians and Jeopardizes National Security: *Hearing Before the H. Comm. on Oversight and Government Reform,* 111 Cong. (July 29, 2009) http://oversight.house.gov/index.php?option=com_content&task=view&id=2465&Itemid=2; *see also id.,* Written Testimony of Thomas D. Sydnor II (July 29, 2009) http://www.pff.org/issues-pubs/testimony/2009/090729-sydnor-testimony-p2p-inadvertent-filesharing.pdf; *id.,* Written Testimony of Mr. Robert Boback (July 29, 2009) http://groc.edgeboss.net/download/groc/transfer/testimony.of.mr.robert.boback.pdf.

Federal Trade Commission, *Widespread Data Breaches Uncovered by FTC Probe,* (Feb. 22, 2010)
at http://www.ftc.gov/opa/2010/02/p2palert.shtm

STUDIES:

Nathaniel S. Good & Aaron Krekelberg, *Usability and Privacy: A Study of KaZaA P2P File-Sharing* (2002) (causes) *reprinted in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, vol. 5, iss. 1 at pp. 137-144 http://www.hpl.hp.com/techreports/2002/HPL-2002-163.pdf

GAO, *Peer-to-Peer Networks Provide Ready Access to Child Pornography,* (Feb. 2003) at http://www.gao.gov/new.items/d03351.pdf.

Thomas D. Sydnor II, John Knight & Lee A. Hollaar, *Filesharing Programs and "Technological Features to Induce Users to Share"* (U.S. Patent & Trademark Office 2007) http://www.uspto.gov/web/offices/dcom/olia/copyright/oir_report_on_inadvertent_sharing_v1012.pdf

M. Eric Johnson, *Inadvertent Disclosure—Information Leaks in the Extended Enterprise* (WEIS 2007) http://weis2007.econinfosec.org/papers/43.pdf

Thomas D. Sydnor II, John Knight & Lee A. Hollaar, *Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform* (PFF 2007) http://www.pff.org/issues-pubs/pops/pop14.22inadvertentfilesharing.pdf

M. Eric Johnson, *The Evolution of the Peer-to-Peer File-Sharing Industry and the Risks to Users,* (Int'l Conf. on Sys. Sciences, 2008) http://csdl2.computer.org/comp/proceedings/hicss/2008/3075/00/30750383.pdf

Alexandre M. Mateus & Jon M. Pena, *Dimensions of P2P and Digital Piracy in a College Campus* (TPRC 2008) http://digitalcitizen.illinoisstate.edu/press_presentations/documents/mateus-peha-TPRC-paper.pdf

M. Eric Johnson, *Information Risk of Inadvertent Disclosure: An Analysis of File-Sharing Risk in the Financial Supply Chain,* 25 J. OF MAN. INF. SYS. 97-123 (Fall 2008) http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/JMIS08.pdf

M. Eric Johnson, *Data Hemorrhages in the Heath-Care Sector,* LECTURE NOTES IN COMPUTER SCIENCE (April 2009) http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/JohnsonHemorrhagesFC09Proceedingd.pdf

Thomas D. Sydnor II, *Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5* (PFF 2009) http://www.pff.org/issues-pubs/pops/2009/pop16.14-inadvertent-file-sharing-reinvented-limewire-5.pdf

SELECTED MEDIA REPORTS ON INADVERTENT FILE-SHARING

Department of Homeland Security, *Unauthorized Peer to Peer (P2P) Programs on Government Computers* (April 19, 2005) https://secure.infragard-ct.org/public/newsfiles/Unauthorized_Peer_to_Peer_(P2P)_Programs_on_Government_Computers__A

pril_19_2005_V6_0.pdf (warning, "Multiple organizations have ongoing investigations into disclosure of sensitive or classified material due to P2P.").

Today Investigates, *New warnings on cyber-thieves,* at http://today.msnbc.msn.com/id/26184891/vp/29405819%2329405819 (reporting on inadvertent sharing of over 150,000 tax returns in New York State alone, including the Bucci family's return, which was downloaded by an identity thief who used it to steal their refund).

Jaikumar Vijayan, *Leaked House Ethics document spreads on the Net via P2P*, ComputerWorld Security (Oct. 30, 2009), http://www.computerworld.com/s/article/9140154/Leaked_House_Ethics_document_spreads_on_the_Net_via_P2P.

Jaikumar Vijayan, *House bill seeking government P2P ban gets boost*, ComputerWorld Government (Oct. 5, 2009), http://www.computerworld.com/s/article/9138958/House_bill_seeking_government_P2P_ban_gets_boost (Tiversa found some 200 incidents of sensitive military documents being available on public peer-to-peer networks).

Jaikumar Vijayan, *Details on presidential motorcades, safe house for First Family, leak via P2P*, ComputerWorld Security (July 29, 2009), http://www.computerworld.com/s/article/9136053/Details_on_presidential_motorcades_safe_house_for_First_Family_leak_via_P2P.

Jaikumar Vijayan, *Update: Strike Fighter data was leaked on P2P network in 2005, security expert says*, ComputerWorld Security (May 5, 2009), http://www.computerworld.com/s/article/9132571/Update_Strike_Fighter_data_was_leaked_on_P2P_network_in_2005_security_expert_says_.

Jaikumar Vijayan, *Classified data on president's helicopter leaked via P2P, found on Iranian computer*, ComputerWorld Security (Mar. 2, 2009), http://www.computerworld.com/s/article/9128820/Classified_data_on_president_s_helicopter_leaked_via_P2P_found_on_Iranian_computer.

Jaikumar Vijayan, *Download music, share bank account info for free on P2P networks*, ComputerWorld Security (Jun. 12, 2007), http://www.computerworld.com/s/article/9024406/Download_music_share_bank_account_info_for_free_on_P2P_networks.

David Kravets, *Men Charged With Hijacking DOD Paychecks* (Dec. 9, 2009), http://www.wired.com/threatlevel/2009/12/military-paychecks-hijacked/ (Jeffrey Girandola and Kajohn Phommavong were indicted for using peer-to-peer networks LimeWire and BearShare to obtain inadvertently shared account information for a DOD online payroll system).

Angela Moscaritolo, *Army Special Forces document leaked on P2P network*, SC Magazine (Oct. 5, 2009), http://www.scmagazineus.com/army-special-forces-document-leaked-on-p2p-network/article/151309/ (A U.S. Army Special Forces document containing the names, Social Security

numbers, home phone numbers and home addresses of 463 soldiers as well as the names and ages of soldiers' spouses and children was found on a peer-to-peer network).

Declan McCullagh, *Congress: File Sharing Leaks Sensitive Government Data*, CBS News (July 29, 2009), http://www.cbsnews.com/blogs/2009/07/29/politics/politicalhotsheet/entry5195953.shtml ("Sensitive files including Secret Service safehouse locations, military rosters, and IRS tax returns can still be found on file-sharing networks, according to a report issued to a U.S. House of Representatives committee on Wednesday.")

Bob Brewin, *File-sharing networks used to uncover thousands of medical records,* nextgov (Feb. 27, 2009), http://www.nextgov.com/nextgov/ng_20090227_9147.php (A university professor was able to access medical records containing detailed personal data on physical and mental diagnoses, including one database containing records on 20,000 patients including Social Security numbers, insurance carriers, and diagnostic codes. The codes identified by name four patients infected with AIDS, the mental illnesses of 201 patients, and the cancer findings of 326 patients.)

Angela Moscaritolo, Medical data leakage rampant on P2P networks, SC Magazine (Feb. 11, 2009), http://www.scmagazineus.com/medical-data-leakage-rampant-on-p2p-networks/article/127216/.

Brian Krebs, *Justice Breyer Is Among Victims in Data Breach Caused by File Sharing*, The Washington Post (July 9, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/07/08/AR2008070802997.html (An employee of a McLean investment firm installed LimeWire on a company computer and inadvertently shared the names, dates of birth, and Social Security numbers of about 2,000 of the firm's clients, including Supreme Court Justice Breyer.).

Tim Wilson, *Army Hospital Breach May Be Result of P2P Leak,* DarkReading (Jun. 3, 2008), http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=211201106 (The names, Social Security numbers, birth dates, and other information on more than 1,000 patients at Walter Reed Hospital was inadvertently released, likely through a peer-to-peer network).

Avi Baumstein, *Our P2P Investigation Turns Up Business Data Galore*, InformationWeek (Mar. 17, 2008), http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=206903417 (Using LimeWire, a reporter easily finds confidential business documents, Social Security numbers, credit card numbers, bank passwords, Equifax credit reports, and a handful of tax returns).

Seattle indictment highlights risks of online file sharing, KOMOnews.com (Sep. 6, 2007), http://www.komonews.com/news/9622602.html (Gregory Thomas Kopiloff used LimeWire, SoulSeek, and other peer-to-peer programs to troll other computers for financial information, which he used to open credit cards and buy more than $73,000 worth of goods online).

ONE MONTH'S WORTH OF RECENT MEDIA REPORTS ON CHILD PORNOGRAPHY ON FILE-SHARING NETWORKS

FdL man guilty of child pornography possession, The Reporter (Dec. 31, 2009), http://www.fdlreporter.com/article/20091231/FON0101/912310436/1985/FONBusiness/FdL-

man-guilty-of-child-pornography-possession (Timothy S. Letz pleaded no contest to two counts of possession of child pornography for sharing child pornography files via a peer-to-peer network).

YMCA Worker Part Of International Porn Case, WSMV-TV (Jan. 1, 2010), http://www.wsmv.com/news/22105885/detail.html (Daniel Quail arrested after Canadian authorities arrested someone using the same peer-to-peer network as Quail and notified American authorities).

Part-time clown and Santa sentenced to 8 years on child pornography charges, Ethiopian Review (Dec. 24, 2009), http://www.ethiopianreview.com/news/7182 (August R. Billek caught after an Immigration and Customs Enforcement agent discovered what was later identified as Billek's computer distributing child pornography via a peer-to-peer network).

Paul Luce, *Child-pornography probe snares Marcus Hook man,* Daily Times (Dec. 11, 2009), http://www.delcotimes.com/articles/2009/12/11/news/doc4b21cb74b4567667059468.txt (David Michael Walton arrested after detectives browsed his shared files on a file-sharing network).

Logan man pleads guilty to child porn, The Herald-Dispatch (Dec. 11, 2009), http://www.herald-dispatch.com/news/x456828572/Logan-man-pleads-guilty-to-child-porn (Brian P. Cornell downloaded child pornograpy using the Internet and shared many of them through a peer-to-peer file sharing program).

Edward Van Embden, *Millville man pleads guilty to distributing child pornography*, Press of Atlantic City (Dec. 18, 2009), http://www.pressofatlanticcity.com/news/press/cumberland/article_cb8ef494-ec40-11de-8c4b-001cc4c03286.html ("Gary Gandy admitted to using a peer-to-peer file sharing service to download and distribute sexual images and videos involving children").

Amanda Terrebonne, *Paul Dixon, Michael Mammone arrested in Russellville on child porn charges*, Today's THV (Dec. 11, 2009), http://www.todaysthv.com/news/local/story.aspx?storyid=95795&catid=2 ("Police say Dixon said he had been downloading child pornography for over a year through Peer-to-Peer (P2P) networks and had accumulated about 30-50 videos showing boys as young as 10 engaged in sexually explicit conduct.").

Denise Yost, *Minister Sentenced For Distributing Child Porn*, NBC4i (Dec. 10, 2009), http://www2.nbc4i.com/cmh/news/crime/article/minister_sentenced_for_distributing_child_porn/28163/ (A FBI agent searching for people who wanted to share child pornography was contacted by Gary L. Kendall via a peer-to-peer file sharing site).

Man gets 15 years in child porn case, The Fayetteville Observer (Dec. 10, 2009), http://www.fayobserver.com/Articles/2009/12/10/959373 (Laurence David Clifton had videos depicting pre-pubescent children in sado-masochistic conduct and hundreds of other images of child pornography).

Eve Byron, *Helena man sentenced for collecting pornography images,* Independent Record (Dec. 12, 2009), http://www.helenair.com/news/local/article_54e8f066-e6e5-11de-bc00-001cc4c03286.html

(Jeremy Peterson admitted that he used LimeWire to download hundreds of videos and around 12,000 images of children who were clearly prepubescent, with some engaged in sadistic or masochistic abuse or other depictions of violence).

Jim Kouri, *Kiddie porn producer exploited his own relatives*, newjerseynewsroom.com (Dec. 16, 2009), http://www.newjerseynewsroom.com/nation/kiddie-porn-producer-exploited-his-own-relatives (Michael Joseph Gilbert possessed more than 6,000 images of child pornography, including images obtained from the Internet via peer-to-peer file sharing programs and of two young relatives that he admitted making sexually explicit videos of when they were as young as 5 and 6 years old).

Jason Trahan, *UT-Arlington graduate student arrested on child pornography charges*, The Dallas Morning News (Dec. 22, 2009), http://www.dallasnews.com/sharedcontent/dws/news/city/arlington/stories/122209dnmetgradporn.377cba6.html (Sheldon Fernandes was arrested after Immigration and Customs Enforcement agents got a tip that he was downloading child pornography from peer-to-peer networks and found more than 100 videos of children in sexual situations on his computer).

Nate Robson, *Couple accused of selling drugs*, The Citizen (Dec. 22, 2009), http://www.auburnpub.com/articles/2009/12/23/local_news/news06.txt (Brien Fredendall said he unknowingly download child pornography when he used LimeWire to download adult pornography).

South Charleston Man Sentenced on Drug Charges, The State Journal (Dec. 22, 2009), http://www.statejournal.com/story.cfm?func=viewstory&storyid=72360 (James Curtis Sorgman spent more than ten years downloading over 17,000 images and videos depicting the graphic sexual abuse of children, including infants using a peer-to-peer file sharing program).

From:	Tom Sydnor
To:	FN-OMB-IntellectualProperty
Subject:	Comments from Thomas D Sydnor II on IPEC Request for Written Submissions
Date:	Wednesday, March 24, 2010 5:01:08 PM
Attachments:	oir_report_on_inadvertent_sharing_v1012.pdf pop14.22inadvertentfilesharing.pdf pop16.14-inadvertent-file-sharing-reinvented-limewire-5.pdf HCOOGR_boback.pdf HCOOGR_sydnor_written_testimony.pdf HEC_testimony_sydnor_02.pdf HCOOGR_sydnor_test.pdf HCOOGR_sydnor_test_appA.pdf sydnor_IPEC_comments.doc