



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.

Congress 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 Hemorrhages in the Health-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 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.*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.

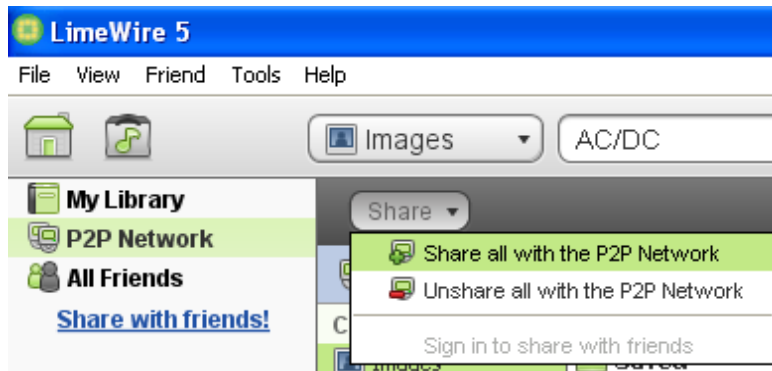
²⁰ Gorton Letter, *supra* note 13, at 6.

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.

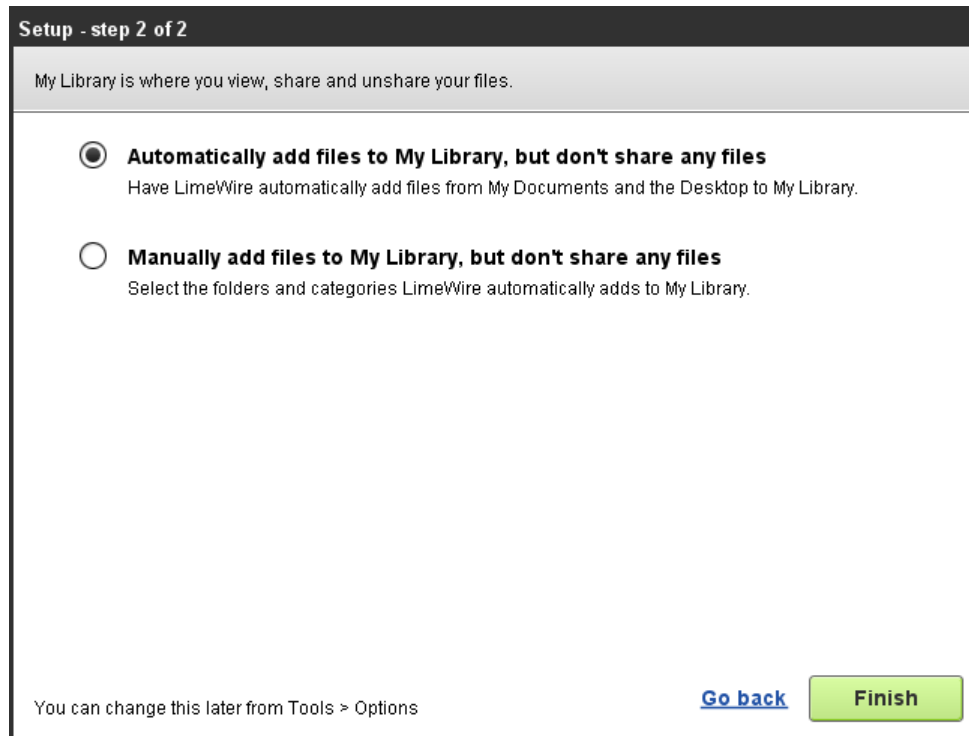
Over time, most LimeWire 5 users may make either or both of these errors. But to understand the *consequences* of such errors, one must understand what users of LimeWire 5 *may not* understand—the types and the locations of the files that a default installation LimeWire 5 will *automatically* load into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

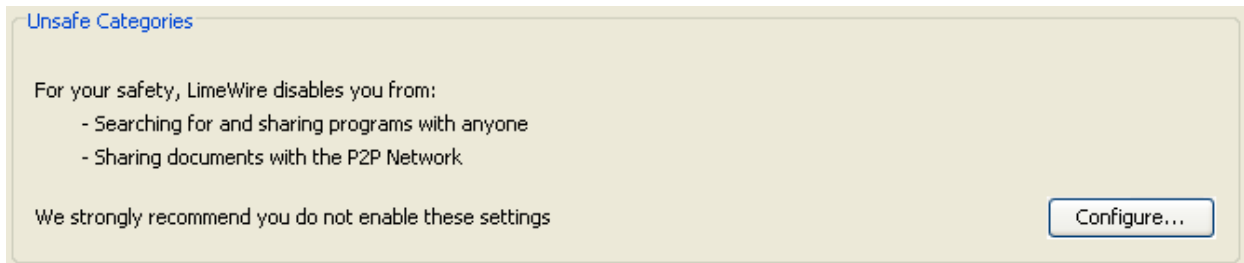
3. Users can *reasonably* disregard LimeWire 5's "warnings" and enable document-sharing.

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.

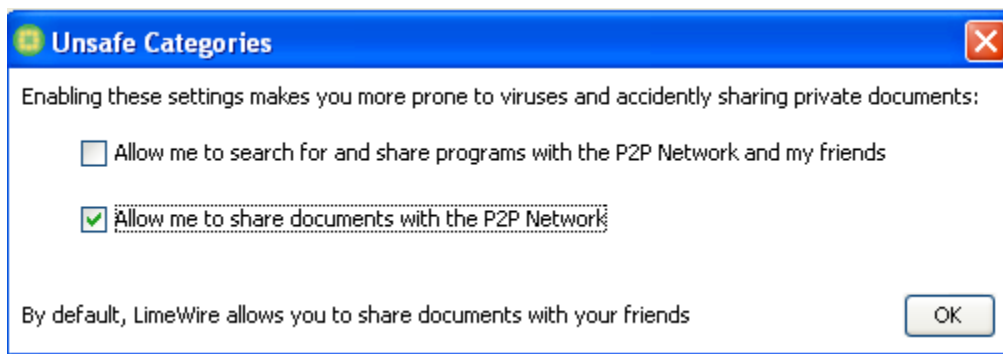
It has always been clear that almost all users of prior versions of LimeWire who inadvertently shared hundreds of personal files did so because *they had changed* "default settings." Consequently, history suggests that—over time—LimeWire 5's "default settings" will *not* determine how many of its users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

Sharing 1,244 files

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 *VBP*s 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 *VBP*s, 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 *VBP*s 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 *VBP*s 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 version 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, Congress 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 is a market-oriented think tank that studies the digital revolution and its implications for public policy. Its mission is to educate policymakers, opinion leaders and the public about issues associated with technological change, based on a philosophy of limited government, free markets and civil liberties.

Established in 1993, PFF is a private, non-profit, non-partisan research organization supported by tax-deductible donations from corporations, foundations and individuals. The views expressed here are those of the authors, and do not necessarily represent the views of PFF, its Board of Directors, officers or staff.

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