

“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 LLC, 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 it 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 general 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.

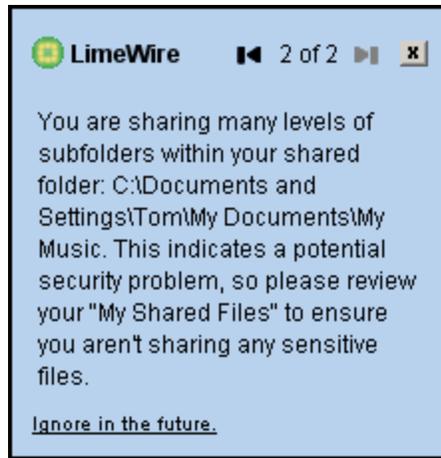
Nevertheless, one example may show why these many measures tended to fail.¹¹ For example, in the Lime Group CEO Mark Gorton’s May 1, 2009 letter to the Committee (the “Gorton Letter”), LimeWire proudly explained that it incorporated into its “first major release following [Mr. Gorton’s 2007] testimony” 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:

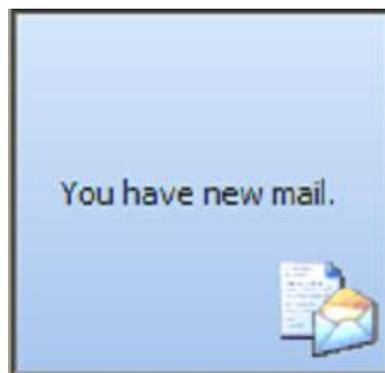
¹¹ I analyzed other problems with LimeWire 2007 warnings and remedial measures in my second co-authored paper on inadvertent sharing, *Inadvertent Filesharing Revisited: Assessing LimeWire’s Responses to the Committee on Oversight and Government Reform*.



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 5.1.4 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 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.

The unpredictably and deliberately dangerous, VBP-violating design of LimeWire 5.2.8: 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....”

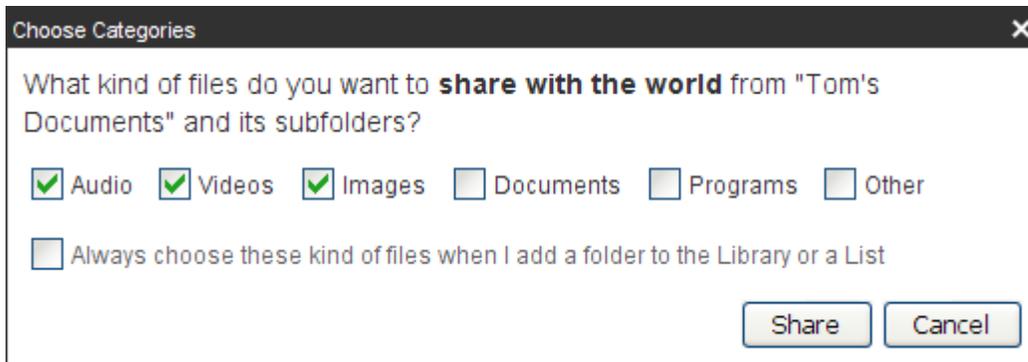
May 1, 2009 Gorton Letter: “LimeWire 5 did away with recursive sharing... did away with folder sharing....”

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 than 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-predictable 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.