

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

**“Legislative Hearing on H.R. ____, the Data Accountability and Protection Act and H.R.
1319, the Informed P2P User Act”**

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

May 5, 2009

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

June of 2002: In *Usability and Privacy, A Study of KaZaA Peer-to-Peer Filesharing*, computer-science researchers from HP Labs conclude that two “features” in the KaZaA file-sharing program, including a search-wizard, were causing users to share so many sensitive files inadvertently that identity thieves had begun data-mining file-sharing networks for inadvertently shared credit-card numbers. Distributors responded by continuing to deploy search wizards.

June of 2003: A year later, hearings on inadvertent sharing held by the House Committee on Oversight and Government Reform and the Senate Committee on the Judiciary caused the distributors of KaZaA., (who were members of DCIA), to belatedly recognize *Usability and Privacy* as “intelligent research,” and to promise to remove both of the dangerous features it had criticized.

July of 2003: The distributors of KaZaA did remove the dangerous features condemned by *Usability and Privacy* and the hearings, but they did so in an almost inexplicable way: both features, including the search wizard were removed in a way that *perpetuated* all of the consequences of the catastrophic inadvertent sharing that they had already caused.

September of 2003: The distributors of LimeWire and other programs responded to the congressional hearings on *Usability and Privacy* by promulgating a self-regulatory *Code of Conduct* that should have precluded use of KaZaA-like search wizards. They declared, “[Our] software and associated user instructions ... shall be designed to reasonably prevent the inadvertent designation of the content of the user’s ... principal data repository ... as material available to other users.”

Fall of 2003: Copyright owners begin suing users of file-sharing programs “sharing” hundreds or thousands of infringing files. Published research found that such enforcement caused most users to drastically reduce the number of files that they shared, but oddly, a few kept on sharing hundreds of infringing files—almost as if they did not realize that they were sharing files at all.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

“[a LimeWire spokesperson] said, ‘Our newest version, LimeWire 5.0, by default cannot share sensitive file types such as spreadsheets or documents. In fact, the software can not share any file or directory without explicit permission from the user.’”

“With LimeWire 5, the latest version of the software, ‘LimeWire has ensured the complete lockdown of the safety and security of LimeWire users, said [Lime Group CEO] Gorton.’”

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PROSECUTOR: Your Honor, I don't believe it is possible to share files inadvertently.

THE COURT: ... [D]oes your software make it possible make it possible for people to accidentally share personal files or sensitive data?

LIMEWIRE DEVELOPER: Accidentally?

THE COURT: Yes.

LIMEWIRE DEVELOPER. Yes.

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

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

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

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

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

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

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

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

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