

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

May 5, 2009

Dear Chairman Rush and Ranking Member Radanovich:

Thank you for holding this important and timely hearing on issues related to H.R. 2221 "The Data Accountability and Trust Act" and H.R. 1319 "The Informed P2P User Act." We greatly appreciate your leadership and that of your colleagues serving on the Subcommittee on Commerce, Trade, and Consumer Protection. We are grateful for this opportunity to share the Distributed Computing Industry Association's ([www.DCIA.info](http://www.DCIA.info)) perspective on this critical industry and consumer issue.

### **Introduction to P2P and File Sharing**

The Distributed Computing Industry Association (DCIA) is a non-profit trade organization focused on peer-to-peer (P2P), cloud computing, file-sharing, and related distributed computing technologies.

Our mission is to foster commercial development of these technologies, which are still in their infancy relative to more mature and established Internet-based offerings – so that their benefits can be realized by all participants in the distribution chain, including content rights holders and Internet service providers (ISPs).

The DCIA conducts working groups and special projects, such as the P2P Digital Watermark Working Group (PDWG), P3P Working Group, (P3PWG), P4P Working Group (P4PWG), Consumer Disclosures Working Group (CDWG), P2P PATROL, P2P Revenue Engine (P2PRE), and, most relevant to today's hearing, the Inadvertent Sharing Protection Working Group (ISPG), which we will discuss in more detail.

The DCIA also publishes the weekly online newsletter DCINFO, maintains a searchable database tracing industry history from 2003 with more than 5,000 articles and papers, and conducts several conferences annually focusing on current issues affecting commercial advancement of the technologies we advocate.

We currently have one-hundred twenty-five (125) Member companies, including P2P, cloud computing, file-sharing, and social networking software developers and distributors, Internet service providers (ISPs), content rights holders, and service-and-support companies. An alphabetical list of our Member companies with links to their respective websites can be found on the home-page of our primary site, [www.dcia.info](http://www.dcia.info).

Wikipedia defines a P2P computer network as using "diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

than conventional centralized resources where a relatively low number of servers provide the core value to a service or application."

With the old server-client approach, every download required a separate session – between the machine hosting the content and each device receiving it. Especially for large rich media files and entertainment content compilations, this represented an expensive methodology and inefficient use of network resources. P2P brought a way to replicate broadcast economics, where content providers incur virtually no incremental expense – as files are transmitted from one to a thousand or literally millions of users.

With P2P, every user on the network joins in a kind of online cooperative – sharing storage, bandwidth, communication, and even viral marketing – to very efficiently distribute content.

P2P is unique because of this decentralized approach and low-to-no overhead. In essence, P2P affords rights holders minimal hosting and transport costs, plus infinitely scalable capacity, limited only by the size of the user network.

P2P industry players include BitTorrent, the most widely used protocol, now with an enterprise solution and many derivatives; eDonkey, which ceased commercial operation, but has remained popular as the open-source eMule; Bearshare, which despite the company's acquisition by iMesh has also remained popular as a standalone program; LimeWire, a widely-used open-P2P program now integrating a LimeWire Store and new Lime Engine; and Kontiki, spun-off last year by VeriSign and currently used in several major enterprise deployments, including Wells Fargo, GM, and Coca-Cola.

Examples of new and emerging P2P services are Damaka, FrostWire, GigaTribe, Grooveshark, Itiva, LittleShoot, mBit, MyBloop, Ooma, Pownce, Raketu, RedSwoosh, SlapVid, Swapper, Twango, Vudu, and Yoomba... to name a few.

2007 was the year when peer-to-peer television (P2PTV) finally arrived as a huge breakthrough for digital video, the first video-centric offering to take advantage of P2P distribution technology in cooperation with a multitude of partners. Examples include the now Flash-based client-less solution Joost; an online movie festival and customized channels on Babelgum; TV stations now in European market trials at Zattoo; an open-P2P video service, backed by Time Warner called VeohTV; a hybrid client-player, Miro; and our newest Member in this space, TVU Networks.

China has been a pioneer of P2PTV with services like PPLive, PPStream, QQlive, UUsee, Vakaka, and Xunlei – where the cost savings of P2P have brought television to millions of unserved viewers.

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

2008 was the year of cloud computing or peer-assisted hybrid-P2P content delivery networks. These incredibly sophisticated platforms give rights holders enormous flexibility in managing online delivery of their copyrighted works. Cost, speed, and access terms-and-conditions can each be precisely controlled. Downloads to play in real-time, downloads to play later, and live streaming can all be supported with the unprecedented advantages of P2P. Leading examples in this category are Abacast, Pando Networks, CloudShield, Octoshape, GridNetworks, Solid State, Ignite Technologies, and Velocix.

Since 2000, P2P has grown into the dominant Internet traffic generator. Velocix reported that, by 2005, P2P surpassed web traffic as a major part of the value proposition for broadband access. Due to relative file-size, video now represents 65% of P2P volume, music 11%, and software-and-games 24%.

Sandvine likewise reports that P2P currently accounts for the largest aggregate share of bandwidth utilization by category. And given the asymmetrical structure of most broadband networks, this is especially striking on the upstream side.

MultiMedia Intelligence sees P2P traffic growing by 400% in the next five years, from 1.6 to 8 petabytes per month, with licensed P2P growing at ten times that rate as authorized offerings come into their own; and new advancements, such as P4P and hybrid services, take hold.

Insight Research projects that the worldwide market for P2P and file-sharing will surpass \$28 billion per year in revenue for carriers and ISPs over the next three years.

P2P-based companies generate income in a number of ways. We have traditional media business models for P2P; such as QTRAX with ad-supported music; iMesh with subscription sales; Vuze with paid downloads; and now Spotify with all three – plus P2P streaming.

P2P telephony with Skype, created 2.6 billion dollars for investors when acquired by eBay. Other examples include premium content delivery from Pando, digital rights management from BuyDRM, client filtering from Audible Magic, payment services from Clickshare and Javien, interactive advertising from Ultramercial and HIRO-Media, super-distribution patents from Digital Containers, spoofing and marketing from MediaSentry – just acquired by MediaDefender, interdiction from Friend Media and BayTSP, and P2P measurement from BigChampagne.

The DCIA believes collaboration among three groups is essential for success in the P2P marketplace: Content, with rights holders for music, movies, and games; Operations,

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

with P2P software developers and distributors; and Platform, with ISPs, plus service-and-support companies.

Therefore our Member companies include leading P2Ps like BitTorrent, Kontiki, Pando, and LimeWire; progressive entertainment firms like Nettwerk Music Group, ROK Entertainment, and PlayFirst games; and major platform companies like AT&T, Cisco Systems, and Verizon.

We also have many up-and-comers like Oversi, Abacast, PeerApp, ARTISTdirect, Brand Asset Digital, CUGate, Altnet, Raketu, and RightsFlow, cable and international ISPs like Comcast and Telefonica, as well as global consulting firms KPMG and FTI.

Most important for the purposes of this 2009 hearing is that we distinguish between P2P and file sharing.

P2P has evolved in the eight years since Napster first brought the term-of-art "P2P File Sharing" to prominence – and notoriety – to the point that P2P now encompasses many more technologies than file sharing, most of which do not deserve the negative connotations of copyright infringement and consumer risks that are still associated with rudimentary file-sharing functionality.

Fully licensed ad-supported P2P, subscription P2P, paid download P2P; commercial enterprise P2P, P2PTV, hybrid P2P CDNs, and live P2P streaming that are increasingly prominent as we reach the end of the first decade of this century deserve to be separated in terms of regulatory considerations from the narrow sub-set of functionality associated with file sharing per se.

DCIA Member companies increasingly use P2P technologies for the delivery of licensed entertainment and/or corporate communications content where rights-holders, rather than end-users, introduce files and/or live streams for online redistribution.

We strongly urge the subcommittee to apply the term "File Sharing" (without the P2P prefix) to its proposed legislation, as a more precise, current, and accurate descriptor.

### **Relevant Background**

By way of introduction, we respectfully call your attention to our related letter of July 18, 2007 to the U.S. House of Representatives Committee on Oversight and Government Reform:

We commend you for your leadership in conducting a Hearing scheduled for July 24th to explore potential privacy and security concerns associated with the use of

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

P2P file-sharing programs, and greatly appreciate the opportunity to comment on this important issue.

The DCIA has taken several steps to address such matters since our inception in 2003 and continues to seek further advances. We have worked closely with the Federal Trade Commission (FTC) on this and related issues. We have also provided witnesses and testimony for previous Congressional Hearings that in part addressed this subject.

We were particularly impressed with your report entitled “File-Sharing Programs and Peer-to-Peer Networks: Privacy and Security Risks.” The DCIA is also familiar with the March 2007 Patent and Trademark Office (PTO) report and the more recent correspondence between the Committee and two leading US-based P2P software developers and distributors regarding consumer disclosures, default settings, recursive sharing, un-installation procedures, etc.

As we suggested to the PTO in March, please allow us to offer the Committee the DCIA’s professional assistance in accelerating adoption of technological advances and related business practices to further protect P2P users against inadvertent sharing of private data.

In our view, because of both the technical complexity and relatively fast-moving innovation in this area, a federally mandated and closely monitored private sector initiative, rather than even the best intentioned legislative measure, will produce the most beneficial effect to the public and to government agencies whose sensitive and confidential information must be protected as a matter of national security.

We currently conduct several working groups tackling a number of issues, including consumer security concerns, such as the inadvertent sharing of files. These working groups can extend beyond our Membership as needed to ensure that the output of their work is widely adopted on a voluntary basis across the distributed computing industry.

The DCIA is willing to create a new working group or to charge an existing one with responding to the concerns that the PTO report has uncovered as may be more precisely delineated during your upcoming Hearing. We look forward to working with the Committee in a productive manner on these issues in a way that will significantly benefit all of your constituencies.

We will contact your offices to follow-up after the Hearing. Thank you very much for your continued interest in our developing industry.

## **Formation of the ISPG**

Following up on the above referenced hearing, within weeks the DCIA established a new working group called the Inadvertent Sharing Protection Working Group (ISPG)

Over a period of the next several months, the DCIA recruited participants among leading P2P file-sharing companies and other representatives of the technology sector with relevant expertise and engaged with FTC staff to address issues associated with inadvertent sharing of personal and sensitive data by users of file-sharing software applications.

This process began by providing an overview and detailed demonstrations for FTC staff of how current major file-sharing software applications work in terms of users uploading files for redistribution via user networks.

It continued through an iterative process involving private sector and federal regulatory participants to develop a program for voluntary best practices for file-sharing software developers to implement to protect users against inadvertently sharing personal or sensitive data.

A document summarizing the program was completed by ISPG participants and posted on the DCIA website at [www.dcia.info/activities/ispvg/inadvertentsharingprotection.pdf](http://www.dcia.info/activities/ispvg/inadvertentsharingprotection.pdf) in July 2008.

In publicly announcing the program, the DCIA expressed gratitude for the participation of industry-leading companies in a collaborative process with regulatory agency representatives that resulted in an excellent work product.

We noted that while adoption would be a voluntary decision to be made by each company on an individual basis, we were confident of wide acceptance, and would not only encourage, but also monitor compliance.

The summary document begins with a glossary defining terms specifically related to subject matter concerns, such as “recursive sharing,” “sensitive file type,” and “user-originated file,” as well as protective measures, such as “affirmative step.”

It then outlines seven steps that are required to be in compliance with the program. These include 1) default settings, 2) file-sharing controls, 3) shared-folder configurations, 4) user-error protections, 5) sensitive-file-type restrictions, 6) file-sharing status communications, and 7) developer principles.

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

The developer principles for file-sharing software applications address feature disablement, uninstallation, new-version upgrades, and file-sharing settings.

Finally, the document includes an eighth optional step for added consumer protection that relates to inactive states of the file-sharing application (fully disconnected from the user network and running in the background).

At the time of the program's announcement, leading file-sharing application LimeWire's CEO George Searle said, "LimeWire is committed to providing a great file-sharing product that people love to use and that provides for their personal safety. We have actively participated in key developmental aspects of this program and believe it will help protect users from the inadvertent sharing of personal or sensitive information."

Top commercial P2P software provider Kontiki's President Eric Armstrong added, "Kontiki, which offers secure peer-assisted content delivery technology, supports the provisions of this program. We believe this DCIA initiative will be valuable to users and creators of software for redistribution of user-originated content."

Major P2P content delivery solutions provider Pando Networks' CEO Robert Levitan concluded, "At Pando Networks, we believe users should always be in control of any P2P application on their desktop. We support this effort that will benefit the entire industry by advancing consumer safety in the large and growing P2P marketplace."

## **ISPG Program**

Following is the verbatim ISPG Program of Voluntary Best Practices for [P2P] File-Sharing Software Developers to Implement to Protect Users against Inadvertently Sharing Personal or Sensitive Data. (Note that brackets around uses of the term P2P indicate our recommended deletions).

### **DEFINITIONS:**

(1) "Affirmative Step" means an action that requires the user to select a non-default choice presented by the application's user interface.

(2) "Recursive Sharing" means the automatic sharing of subfolders of any parent folder designated for sharing.

(3) "Sensitive File Types" means file types which are known to be associated with personal or sensitive data, for example, those with file extensions such as .doc or .xls in Windows Office, .pdf in Adobe, or the equivalent in other software programs.

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

(4) “Sensitive Folders” are those often used to store personal or sensitive data, for example, the “My Documents” folder in Windows or the equivalent on another operating system.

(5) “Shared Folder” means a folder that is designated, at the point of installation, for users to store files that other users of the respective file-sharing network can download from the user’s computer.

(6) “User-Originated Files” means any files stored on a user’s computer prior to installation of the file-sharing application and any files subsequently stored on a user’s computer that a user has not downloaded from the respective file-sharing network.

**REQUIRED – TO BE CONSIDERED IN COMPLIANCE**

(1) An application’s default settings for file sharing at the point of software installation: may permit redistribution of files the user subsequently downloads from the respective [P2P] network if this behavior has been disclosed to users clearly and conspicuously in advance; and shall not share User-Originated Files.

(A) 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 risks of inadvertent sharing of personal or sensitive data.

(B) There shall be a simple way for the user to disable the file-sharing functionality altogether by using controls provided in a designated share settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to disable the file-sharing functionality shall be clear, timely, and conspicuous.

(2) There shall be a simple way for the user to stop sharing any folder, subfolder, or file that is being shared by using controls provided in a designated share settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to stop the sharing of any folder, subfolder, or file shall be clear, timely, and conspicuous.

(3) The Shared Folder shall not contain any User-Originated Files at the point of initial installation of the [P2P] software. The user must place User-Originated Files and pre-existing folders in the Shared Folder individually. The user must take Affirmative Steps to share additional folders.

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

- (A) Recursive Sharing shall be disabled by default and may be enabled only after the user takes Affirmative Steps.
- (B) The user must have clear and precise options to control Recursive Sharing if a user enables it. All subfolders that are going to be shared should be conspicuously noted, for the user to review and confirm.
- (4) For User-Originated Files that are made available for distribution by taking the Affirmative Steps outlined above, additional protection shall be provided against known instances of potentially-harmful user error.
- (A) To share the entire contents of a Sensitive Folder, the user must take Affirmative Steps and be given clear, timely, and conspicuous warnings that the selected folder may contain sensitive or personal files.
- (B) Any attempt to share a complete drive (e.g., the “C” or “D” drive, a network drive, or external drive) or a user-specific system folder (e.g., a “Documents and Settings” folder in Windows) must be prevented.
- (5) When the default setting for file sharing has been changed by the user to permit distribution of User-Originated Files in accordance with the foregoing requirements, files with Sensitive File Types shall not be permitted to be distributed via the [P2P] network.
- (A) The user must take Affirmative Steps to change the default settings to enable sharing of files with Sensitive File Types.
- (B) There shall be a simple way for the user to stop sharing files with Sensitive File Types by using controls provided in a designated share settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to stop sharing Sensitive File Types shall be clear, timely and conspicuous.
- (6) The user shall be presented with a clear and conspicuous communications (e.g., on all screens) specifying the number of files being shared. The user shall be shown a prominent warning when a large number of files or folders are shared.
- (A) If a large number of files is shared (e.g., greater than 500), a warning shall be shown to the user. This warning shall contain options to reduce the number of shared files.

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

(B) If a large number of subfolders is shared (e.g., greater than 4), a warning shall be shown to the user. This warning shall contain options to reduce the number of shared folders.

(7) Developers shall also implement the following principles:

(A) Disabling of file-sharing features, including but not limited to those outlined above, shall be simple to do and explained in plain language, with consistent terminology (i.e., terms such as “Default Setting,” “File Extension,” “Recursive Sharing,” and “Shared Folder” shall always have the same meaning whenever used in communications from the P2P file sharing software provider).

(B) Complete uninstallation of the [P2P] file-sharing software also shall be simple to do and explained in plain language (e.g., by using the standard “Add/Remove Program” functionality on Windows or its equivalent on other operating systems).

(C) [P2P] file-sharing software developers shall make best efforts to ensure that as many users of their applications as possible upgrade to the new versions of their software, which contain the features outlined above, as soon as they are commercially available (i.e., after successfully completing beta testing). 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, consistent with the foregoing requirements, before Sensitive Folders are shared and users must take Affirmative Steps to continue sharing Sensitive Folders and their subfolders. By default, Sensitive File Types shall not be permitted to be distributed via the [P2P] network.

(D) When the user subsequently chooses to upgrade to a different or newer version of the [P2P] file-sharing software, or to reinstall the same version of the software, either (a) if the software upgrade or reinstallation does not materially affect other user-controllable settings (including aspects of the user-interface and share settings addressed in this document), then it shall not change the file-sharing settings previously chosen by the user; or (b) if the software upgrade or reinstallation does materially change or require user-controllable settings to be reset, then it shall require file sharing settings to be reset by the user as described above. If the upgrade or reinstallation uses the previously set file-sharing settings, the application shall warn users that those settings will be used, remind the user that changes to those settings can be made in the designated area in the software, and warn users if Sensitive Folders or Sensitive File Types are being shared.

OPTIONAL – FOR ADDED CONSUMER PROTECTION

(8) When the user chooses no longer to use the [P2P] file-sharing software in a given online session, the user shall be presented with a choice of either i.) turning the software completely off (i.e., fully disconnecting from the [P2P] network); or ii.) having the software continue to run in the background (i.e., still contributing resources to the [P2P] network to help facilitate content redistribution).

(A) There shall be a simple way for the user to fully disconnect from the [P2P] network by using controls provided in a designated area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to fully disconnect from the [P2P] network shall be clear, timely, and conspicuous.

(B) When the [P2P] file-sharing software is in use and running in the background, the application shall clearly alert the user that the software is still running (e.g., in the “System Tray” on Windows or its equivalent on another operating system).

## **ISPG Compliance**

In August 2008, the DCIA announced that compliance monitoring would begin in December 2008 to allow software developers reasonable time to introduce required elements of the new ISPG program into their upcoming upgrades and new releases.

Monitoring began as scheduled and resulted in the completion of compliance report submissions from top brands that use P2P for downloading, live streaming, open-environment sharing, and corporate intranet deployments, and to distribute both user-generated and professionally produced content.

Specifically, seven (7) leading P2P program developers and distributors submitted detailed reports in February 2009, which were provided to FTC staff.

In March 2009, the DCIA prepared and submitted a summary report noting that there had been very significant progress on this important issue; and that providing users of file-sharing programs with as safe and valuable an experience as possible remained a top industry priority.

We also noted that, in addition, DCIA Member companies increasingly use P2P technologies for the delivery of licensed entertainment and/or corporate communications content where rights-holders, rather than end-users, introduce files and/or live streams for online redistribution.

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

Following is a summary analysis of the ISPG compliance report submissions followed by the data tables upon which this analysis was based.

It should be noted, too, that software implementations of the popular BitTorrent protocol typically require users to conduct a deliberate conversion process from whatever native file-format their content is in to a torrent file before it can be shared, thus minimizing this risk of user error.

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 user network, which is disclosed to users clearly and conspicuously in advance. They do not share user-originated files by default. Some, like LimeWire, by default do not even permit this sort of redistribution where the download was of a document file type.

100% of respondents also provide complete uninstallation of the P2P or 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 or its equivalent on other operating systems).

100% of respondents for whom this principle is applicable now offer a simple way for the user to stop sharing any folder, subfolder, or file that is being shared by using controls provided in a designated share-settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to stop the sharing of any folder, subfolder, or file are clear, timely, and conspicuous.

A similar number of respondents make best efforts to ensure that as many users of their applications as possible upgrade to the new versions of their software that contain these safety features. And during such upgrades, great care is taken regarding both the file-sharing settings themselves and communications regarding them.

Five times more respondents comply than do not with the user being presented a clear and conspicuous communications (e.g., on all screens) specifying the number of files being shared. Users are also shown prominent warnings when a large number of files or folders are shared.

Where this principle is applicable, which was for the majority of respondents, four times more respondents than not offer additional protection against known instances of potentially-harmful user error.

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

These include requiring that a user must take affirmative steps to share the entire contents of a sensitive folder, and be given clear, timely, and conspicuous warnings that the selected folder may contain sensitive or personal files; and that any attempt to share a complete drive (e.g., the “C” or “D” drive, a network drive, or external drive) or a user-specific system folder (e.g., a “Documents and Settings” folder in Windows) must be prevented.

Furthermore, in each of the 57% of cases where applicable, 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 include clear, timely, and conspicuous plain-language warnings about the risks of inadvertent sharing of personal or sensitive data.

A similar number provide a simple way for the user to disable the file-sharing functionality altogether by using controls provided in a designated share settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to disable the file-sharing functionality are clear, timely, and conspicuous.

For those respondents whose services include a shared folder, none now contain any user-originated files at the point of initial installation of the software. The user must place user-originated files and pre-existing folders in the shared folder individually. The user must take affirmative steps to share additional folders.

Recursive sharing has been disabled by default and may be enabled only after the user takes affirmative steps in all but 14% of applicable instances. For the non-complying applications, this is expected to be addressed in upcoming new releases. The same ratios apply to users having clear and precise options to control recursive sharing if a user enables it. All subfolders that are going to be shared shall be conspicuously noted for the user to review and confirm.

At this point, an even number of respondents, where the following principle applies, comply with not permitting sensitive files to be distributed by the user network when the default setting for file sharing has been changed by the user to permit distribution of user-originated files in accordance with the foregoing requirements.

Results were similar for providing a simple way for the user to stop sharing files with sensitive file types by using controls provided in a designated share-settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface, and with instructions on how to stop sharing sensitive file types that are clear, timely and conspicuous.

U.S. House of Representatives Committee on Energy and Commerce  
 Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
 Testimony of Marty Lafferty  
 CEO, Distributed Computing Industry Association (DCIA)

Fewer currently require users to take affirmative steps to change the default settings to enable sharing of files with sensitive file types. We will continue to closely examine this critical area.

**Data Tables**

- (1) An application’s default settings for file sharing at the point of software installation: may permit redistribution of files the user subsequently downloads from the respective [P2P] network if this behavior has been disclosed to users clearly and conspicuously in advance; and shall not share User-Originated Files.

Percentage of Respondents Complying: 100%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 0%
---	---	---

- (A) 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 risks of inadvertent sharing of personal or sensitive data.

Percentage of Respondents Complying: 57%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 43%
--	---	--

- (B) There shall be a simple way for the user to disable the file-sharing functionality altogether by using controls provided in a designated share-settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to disable the file-sharing functionality shall be clear, timely, and conspicuous.

Percentage of Respondents Complying: 57%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 43%
--	---	--

- (2) There shall be a simple way for the user to stop sharing any folder, subfolder, or file that is being shared by using controls provided in a designated share-settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to stop the sharing of any folder, subfolder, or file shall be clear, timely, and conspicuous.

U.S. House of Representatives Committee on Energy and Commerce  
 Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
 Testimony of Marty Lafferty  
 CEO, Distributed Computing Industry Association (DCIA)

Percentage of Respondents Complying: 86%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 14%
--	---	--

(3) The Shared Folder shall not contain any User-Originated Files at the point of initial installation of the [P2P] software. The user must place User-Originated Files and pre-existing folders in the Shared Folder individually. The user must take Affirmative Steps to share additional folders.

Percentage of Respondents Complying: 57%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 43%
--	---	--

(A) Recursive Sharing shall be disabled by default and may be enabled only after the user takes Affirmative Steps.

Percentage of Respondents Complying: 29%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 57%
--	--	--

(B) The user must have clear and precise options to control Recursive Sharing if a user enables it. All subfolders that are going to be shared should be conspicuously noted, for the user to review and confirm.

Percentage of Respondents Complying: 29%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 57%
--	--	--

(4) For User-Originated Files that are made available for distribution by taking the Affirmative Steps outlined above, additional protection shall be provided against known instances of potentially-harmful user error.

Percentage of Respondents Complying: 57%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 29%
--	--	--

U.S. House of Representatives Committee on Energy and Commerce  
 Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
 Testimony of Marty Lafferty  
 CEO, Distributed Computing Industry Association (DCIA)

(A) To share the entire contents of a Sensitive Folder, the user must take Affirmative Steps and be given clear, timely, and conspicuous warnings that the selected folder may contain sensitive or personal files.

Percentage of Respondents Complying: 43%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 43%
--	--	--

(B) Any attempt to share a complete drive (e.g., the “C” or “D” drive, a network drive, or external drive) or a user-specific system folder (e.g., a “Documents and Settings” folder in Windows) must be prevented.

Percentage of Respondents Complying: 57%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 29%
--	--	--

(5) When the default setting for file sharing has been changed by the user to permit distribution of User-Originated Files in accordance with the foregoing requirements, files with Sensitive File Types shall not be permitted to be distributed via the [P2P] network.

Percentage of Respondents Complying: 29%	Percentage of Respondents Not Complying: 29%	Percentage of Respondents with Principle Inapplicable: 43%
--	--	--

(A) The user must take Affirmative Steps to change the default settings to enable sharing of files with Sensitive File Types.

Percentage of Respondents Complying: 14%	Percentage of Respondents Not Complying: 29%	Percentage of Respondents with Principle Inapplicable: 57%
--	--	--

(B) There shall be a simple way for the user to stop sharing files with Sensitive File Types by using controls provided in a designated share-settings control area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to stop sharing Sensitive File Types shall be clear, timely and conspicuous.

U.S. House of Representatives Committee on Energy and Commerce  
 Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
 Testimony of Marty Lafferty  
 CEO, Distributed Computing Industry Association (DCIA)

Percentage of Respondents Complying: 29%	Percentage of Respondents Not Complying: 29%	Percentage of Respondents with Principle Inapplicable: 43%
--	--	--

- (6) The user shall be presented with a clear and conspicuous communications (e.g., on all screens) specifying the number of files being shared. The user shall be shown a prominent warning when a large number of files or folders are shared.

Percentage of Respondents Complying: 71%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 14%
--	--	--

- (A) If a large number of files is shared (e.g., greater than 500), a warning shall be shown to the user. This warning shall contain options to reduce the number of shared files.

Percentage of Respondents Complying: 0%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 100%
---	---	---

- (B) If a large number of subfolders is shared (e.g., greater than 4), a warning shall be shown to the user. This warning shall contain options to reduce the number of shared folders.

Percentage of Respondents Complying: 0%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 100%
---	---	---

- (7) Developers shall also implement the following principles:

- (A) Disabling of file-sharing features, including but not limited to those outlined above, shall be simple to do and explained in plain language, with consistent terminology (i.e., terms such as “Default Setting,” “File Extension,” “Recursive Sharing,” and “Shared Folder” shall always have the same meaning whenever used in communications from the [P2P] file-sharing software provider).

U.S. House of Representatives Committee on Energy and Commerce  
 Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
 Testimony of Marty Lafferty  
 CEO, Distributed Computing Industry Association (DCIA)

Percentage of Respondents Complying: 14%	Percentage of Respondents Not Complying: 14%	Percentage of Respondents with Principle Inapplicable: 71%
--	--	--

(B) Complete uninstallation of the [P2P] file-sharing software also shall be simple to do and explained in plain language (e.g., by using the standard “Add/Remove Program” functionality on Windows or its equivalent on other operating systems).

Percentage of Respondents Complying: 100%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 0%
---	---	---

(C) [P2P] file-sharing software developers shall make best efforts to ensure that as many users of their applications as possible upgrade to the new versions of their software, which contain the features outlined above, as soon as they are commercially available (i.e., after successfully completing beta testing). 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, consistent with the foregoing requirements, before Sensitive Folders are shared and users must take Affirmative Steps to continue sharing Sensitive Folders and their subfolders. By default, Sensitive File Types shall not be permitted to be distributed via the [P2P] network.

Percentage of Respondents Complying: 86%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 14%
--	---	--

(D) When the user subsequently chooses to upgrade to a different or newer version of the [P2P] file-sharing software, or to reinstall the same version of the software, either (a) if the software upgrade or reinstallation does not materially affect other user-controllable settings (including aspects of the user-interface and share settings addressed in this document), then it shall not change the file-sharing settings previously chosen by the user; or (b) if the software upgrade or reinstallation does materially change or require user-controllable settings to be reset, then it shall require file-sharing settings to be reset by the user as described above. If the upgrade or reinstallation uses the previously set file-sharing settings, the application shall warn users that those settings will be used, remind the user that changes to those settings

U.S. House of Representatives Committee on Energy and Commerce  
 Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
 Testimony of Marty Lafferty  
 CEO, Distributed Computing Industry Association (DCIA)

can be made in the designated area in the software, and warn users if Sensitive Folders or Sensitive File Types are being shared.

Percentage of Respondents Complying: 86%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 14%
--	---	--

OPTIONAL – FOR ADDED CONSUMER PROTECTION

(8) When the user chooses no longer to use the [P2P] file-sharing software in a given online session, the user shall be presented with a choice of either i.) turning the software completely off (i.e., fully disconnecting from the [P2P] network); or ii.) having the software continue to run in the background (i.e., still contributing resources to the [P2P] network to help facilitate content redistribution).

Percentage of Respondents Complying: 43%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 57%
--	---	--

(A) There shall be a simple way for the user to fully disconnect from the [P2P] network by using controls provided in a designated area of the software that is easy to access (e.g., with a single click) from any screen in the user interface. Instructions on how to fully disconnect from the [P2P] network shall be clear, timely, and conspicuous.

Percentage of Respondents Complying: 29%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 71%
--	---	--

(B) When the [P2P] file-sharing software is in use and running in the background, the application shall clearly alert the user that the software is still running (e.g., in the “System Tray” on Windows or its equivalent on another operating system).

Percentage of Respondents Complying: 29%	Percentage of Respondents Not Complying: 0%	Percentage of Respondents with Principle Inapplicable: 71%
--	---	--

## **Compliance Report Follow Up**

After submitting the compliance report summary, there were two follow-up items based on FTC staff review of the compliance reports.

One related to a company that had not yet eliminated recursive sharing in its default mode. In March 2009, the CEO of this company committed that in the subsequent version of this software that by default sharing would not be recursive.

The other related to a separate company that in the FTC staff's view had not adequately complied with Sections 1 and 7(C) and (D).

The DCIA engaged with senior management and technology leaders at this company to address these outstanding compliance issues as expeditiously as possible, resulting in the company's commitment to make changes in the subsequent release of its software scheduled for June 2009.

In April 2009, the company made the following additional commitment:

Please see the descriptions below regarding the outstanding ISPG Voluntary Best Practices fulfillment issues identified by the FTC [Sections 1, 7(C), 7(D)]. Where noted, the specific comments below indicate intended functionality for the next version of our software, the beta of which will be released in June as we originally committed, which is the soonest that this can reasonably be accomplished given our internal technical resources and the non-consumer-facing changes necessary for their implementation.

However, the Company will be able to integrate the notification discussed regarding the Voluntary Best Practice Section (1) within 3-5 weeks of the date of this letter, sooner than our original commitment.

By way of overview, in all instances dealing with sensitive file types (including but not limited to .doc, .wpd, .pdf, .exc.) our software by default does not share these types of files with the [P2P] network, even if they were shared in the prior version of our software. Period. This change was initiated with the current version of our software. This version will not share sensitive file types no matter whether these document file types exist in a folder that a user elects to share with the [P2P] network, no matter whether a user shared these sensitive file types previously in the prior version of our software, and no matter whether a user is using our software's library to manage his/her personal files. Sharing sensitive file types with the entire [P2P] network is only possible if a user changes his/her settings

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

by going to Tools -> Options -> Security -> and clicking Configure under the category of “Unsafe Categories” and disregards the following warning: “We strongly recommend you do not enable these settings.” Should a user continue beyond this point, he/she then has to affirmatively “check” a box stating “Allow me to share documents with the [P2P] Network” and then click “O.K.”, and then disregard the following warning: “Enabling these settings makes you more prone to viruses and accidentally sharing private documents.”

Following is more information about the changes designed to protect users against inadvertently sharing personal or sensitive data.

Current version of our software and beyond - General foundational changes:

1. By default (see 3 below regarding changing default settings), if a user tries to share a sensitive file type with the [P2P] Network, our software will not let him/her do it even if the file was previously shared in the prior version. This will be the case even if that user previously shared that file, and it will apply no matter where that user stored or stores the file on his/her computer or whether or not that file is managed by the user in his/her library.

2. By default, if a user shares a folder containing sensitive file types, our software will not share the sensitive file.

3. In order to share sensitive file types, a user must affirmatively undertake the following: go to Tools -> Options -> Security -> and click Configure under the category of “Unsafe Categories” and disregard for the following warning: “We strongly recommend you do not enable these settings.” If the user elects to continue, in the “Configure” section, he/she must then check the box “Allow me to share documents with the [P2P] Network,” and then click “O.K.”, and then disregard the following warning: “Enabling these settings makes you more prone to viruses and accidentally sharing private documents.”

a. NOTE: changing this setting will still not share users' documents and will not automatically share any sensitive file types, rather it merely allows users to share them if they affirmatively elect to share a particular file at a later point in time.

Regarding the ISPG Voluntary Best Practices fulfillment issues -

Voluntary Best Practice Section 1 – for release within 3-5 weeks

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

1. To begin, mere installation and activation of our software will not result in the receipt or sharing of files with other users of our software without further affirmative steps taken by the user.
2. Effective on the beta release of the next version of our software, during the first-launch following installation the user will be told that files downloaded from the [P2P] network will be shared automatically with the [P2P] network and how to change this setting.

Voluntary Best Practice Sections 7(C), 7(D) – for June release.

1. Beginning with the current version of our software and for all versions thereafter, our software by default does not share sensitive file types. Even if they were shared previously in the prior or earlier version of our software, the current version “un-shares” ALL sensitive file types.
2. As our software loads a user's library, if it finds any sensitive file types being shared, a warning of such will be given to the user along with instructions on how to disable sharing the sensitive file type.
3. In the event a user (1) was using an earlier sub-version of our current major release, AND (2) affirmatively changed his/her setting in that version to allow sharing of sensitive file types AND (3) affirmatively chose to share a specific file or files of this type (because merely enabling the sharing of sensitive file types does not automatically share such files, rather the user must choose specific files to share), our software will display a notification substantially similar to this: “You are sharing a sensitive file type and doing this can lead to identity theft. Click here to stop sharing sensitive file types and prevent this from happening.”

## **H.R. 1319**

In April 2009, Subcommittee staff invited the DCIA to participate in redrafting the subject proposed legislation. We agreed to do so and formed a DCIA Member company subgroup of interested parties to conduct this work.

This process is now underway and the DCIA would be glad to coordinate this work with Subcommittee staff.

Our basic principles in undertaking this redraft were to seek to help improve the language of the measure by making it more specific to user behavior and software functionality, and to express its provisions more precisely and in plain language.

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

Among our greatest concerns was that the bill as drafted would have unintended consequences that would make some of the most advanced implementations of P2P, which involve licensed content distributors, uncompetitive.

For example, even those that don't include a user-generated content (UGC) component still cause the user's computer to seed files. And because the proposed legislation applies to the use of the user's bandwidth without their knowledge, it could apply to almost any application that relies on distributed computing.

We believe the proposed legislation was precipitated by an increasingly outdated concern over a very specific feature of a small number of applications, some of which no longer exist.

Our Member companies and ISPG participants, specifically those that rely on P2P technologies, no longer have that feature – recursive sharing of sensitive file types – or are in the process of phasing it out.

The present bill goes way beyond that specific concern, however, and would appear to apply to additional functionality and technologies that have nothing to do with recursive file sharing.

Applying the requirements of the bill to all these products, services, and companies is unnecessary and would be burdensome and counter-productive. The problem the bill is intended to address is limited to a small number of companies, and these are the ones to which the ISPG best practices already apply.

To the extent that legitimate consumer concerns persist in the area that the bill is meant to address, we strongly believe they can best be handled by ongoing self-regulation under the oversight of the appropriate federal authority that we have initiated with the ISPG.

Nevertheless to meet our commitment to Subcommittee staff to work on a redraft, certain of the changes our sub-group is considering are to more precisely define the file-sharing user error to be prevented by means of the contemplated legislative safeguards.

This includes a narrower description of the inadvertent making available of sensitive or personal information on a computer through the use of file-sharing software applications.

We are further seeking to define the sensitive file types that should be covered by a precisely targeted measure.

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

We are also attempting to address the practical realities of timing as well as content for optimally effective consumer-protecting notices and obtaining of informed consent at various stages in the accessing, installing, and activation of such software and its various modes of functionality, and relevant differences for various genres of content.

Regarding the uninstallation provisions, our sub-group is also reviewing this language against previously developed consumer disclosure guidelines as well as generally established practices for best-of-class related software applications, again taking into account multiple modes of file-sharing software operation and functionality that should be under the clear control of the user.

We have requested legal counsel to review the proposed enforcement regime and provide advice to the sub-group.

It is likely that the defined terms would be substantially changed as a result of the above work effort, and the list slightly expanded to include such additional items as the file-sharing function itself, which involves searching, discovery, and copying of files.

It would also need to involve such essential file-sharing software application defining terms as shared directory, data files versus streaming content, etc.

## **CONCLUSION**

Based on the demonstrated success to date of the ISPG in putting in place a system for effective self regulation, the potential harm of unintended consequences from overbroad impact of a bill of this sort, and the fundamental principle that legislation should embolden technological advancement rather than hinder it, the DCIA and our Member companies are opposed to the passage of this legislation.

The bill would likely unnecessarily burden U.S.-based technology firms with compliance with an innovation-freezing measure, while being unenforceable against overseas firms whose software is available to U.S. consumers. Of great concern to us is how this bill might stifle yet undeveloped new and potentially very useful and valuable software applications.

Our legal review up to this point suggests that no matter the changes in the bill's construction, no matter any amount of rewording, it will still not only stifle its purported target from possible improvements that would better address the problem the bill intends to address, but it will also potentially still apply to any type of data transmitting software, including Internet applications, desktop applications, e-mail applications,

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

instant messaging (IM), cloud computing, social networks, fully licensed P2P deployments, hybrid peer-assisted CDNs, etc.

The foregoing summarizes some of the very real difficulties in trying to develop legislation such as this.

Rather than an overly broad, outdated, and potentially stifling legal measure, we believe that the Subcommittee's acknowledgment and formalization of requirements for compliance with the ISPG's self-regulatory process will be more effective in achieving the stated purpose that the bill is intended to accomplish.

As we noted previously, because of both the technical complexity and relatively fast-moving innovation in this area, a federally mandated and closely monitored private sector initiative, rather than even the best intentioned legislative measure, will produce the most beneficial effect to the public and to government agencies whose sensitive and confidential information must be protected as a matter of national security.

Nonetheless, the DCIA and our Member companies will continue to review the bill in an effort to find a way to reconstruct it as requested to achieve the Subcommittee's goals.

If the Subcommittee chooses to move the bill forward, we will be there to aid in the redrafting process and to help the Subcommittee address opposition to the bill.

On the other hand, the DCIA has committed to industry self-regulation through the ISPG to address the subject matter of this bill, and is making substantial progress.

As a further commitment, the DCIA is willing to charge our existing ISPG with responding to additional concerns that may be raised today, and as may be more precisely delineated by Subcommittee staff following up on the hearing. We look forward to working with the Subcommittee in a productive manner on these issues in a way that will significantly benefit all of your constituencies.

Thank you very much for your continued interest in our developing industry.

Respectfully,

Martin C. Lafferty  
Chief Executive Officer  
Distributed Computing Industry Association (DCIA)

Attachment: Testimony of DCIA Member Company Solid State Networks

U.S. House of Representatives Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection – Legislative Hearing on H.R. 2221 and H.R. 1319  
Testimony of Marty Lafferty  
CEO, Distributed Computing Industry Association (DCIA)

Cc: Subcommittee on Commerce, Trade, and Consumer Protection

The Honorable John Barrow  
The Honorable Bruce L. Braley  
The Honorable G. K. Butterfield  
The Honorable Kathy Castor  
The Honorable Diana DeGette  
The Honorable Phil Gingrey  
The Honorable Charles A. Gonzalez  
The Honorable Bart Gordon  
The Honorable Gene Green  
The Honorable Mary Bono Mack  
The Honorable Jim Matheson  
The Honorable Doris O. Matsui  
The Honorable Tim Murphy  
The Honorable Sue Wilkins Myrick  
The Honorable Frank Pallone, Jr.  
The Honorable Joseph R. Pitts  
The Honorable John P. Sarbanes  
The Honorable Steve Scalise  
The Honorable Jan Schakowsky  
The Honorable Zachary T. Space  
The Honorable Cliff Stearns  
The Honorable Bart Stupak  
The Honorable John Sullivan  
The Honorable Betty Sutton  
The Honorable Lee Terry  
The Honorable Anthony D. Weiner  
The Honorable Ed Whitfield  
The Honorable Joe Barton (ex officio)  
The Honorable John D. Dingell (ex officio)  
The Honorable Henry A. Waxman, CA (ex officio)