Compliance Report on Voluntary Best Practices By P2P File-Sharing Software Developers To Protect Users Against Inadvertently Sharing Personal or Sensitive Data

The DCIA-sponsored Inadvertent Sharing Protection Working Group (ISPG) announced its consumer protection program in July 2008, culminating a year of work among leading P2P companies along with US federal regulatory authorities. A document summarizing the program is posted on the DCIA website (Activities / ISPG).

In recent weeks, the DCIA has received 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.

There has been enormous progress on this important issue; and providing users of file-sharing programs with as safe and valuable an experience as possible remains a top industry priority.

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

It should be noted, too, that P2P 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 P2P network, which is disclosed to users clearly and conspicuously in advance. They do not share user-originated files by default.

100% of respondents also provide complete uninstallation of the P2P file-sharing software that is simple to do and explained in plain language (e.g., by using the standard “Add/Remove Program” functionality on Windows or its equivalent on other operating systems).

86% of respondents (all where 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.

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 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.

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 P2P 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.

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.

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%

(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.

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).

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 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%