

# Infragistics Corporation Response to

## Department of Commerce United States Patent and Trademark Office “Request for Written Comments on Technological Protection Systems for Digitized Copyrighted Works”

Presenting



**InTether**

File Security Series

**USPTO Question:** What technological protection systems have been implemented, are available for implementation, or are proposed to be developed to protect digitized copyrighted works and prevent infringement, including any upgradeable and self-repairing systems?

**Summary Response:** The Problem of Securing Copyrighted Materials is a challenge. While the ability to create, store, and use intellectual property via the internet has enabled organizations to conduct distance learning in a more efficient, timely and global manner, it has also put today's copyright owners at great risk. Each and every day, digital files that contain copyrighted works flow freely inside and outside of mediated instructional activities. Section 107 of the copyright law allows for redistribution of materials for teaching purposes inside of the classroom setting. However, when digital files go unprotected and are distributed at will, they represent a huge liability and can materially damage the owner of the intellectual property.

### **A. Infraworks Introduces InTether File Security Series**

Infraworks solves this significant and costly problem with its InTether™ File Security Series. The Company's patented security applications protect digital files as they are shared and used throughout their lifecycle. Infraworks is a leading enterprise file security software company that provides customers with the software and services they need to protect intellectual property stored and distributed in digital files. Our security solutions protect files from the time they are created until the time they are deleted ... even while they are in use.

Infraworks' InTether is intended to secure copyrighted works while in digital format. Sharing information has a positive and a negative aspect. The positive aspect is the distribution of knowledge. The negative aspect is losing control of the knowledge. This happens in two ways. First, the owner who distributes it cannot be certain that it will not be re-distributed. Second, the owner cannot be certain of proper and timely disposal. Without that assurance, sharing digital copyrighted materials becomes a threat to the creator of the material. With the assurance that copyrighted materials will not be illicitly re-distributed, modify, copy or printed, and will be destroyed at the end of life date, sharing will no longer put the owners of copyrighted materials at risk. InTether allows the dominant computing platform, the Wintel machine, to be used for distributing information while assuring a high degree of control over re-distribution and disposal.

InTether is the most secure method of sharing information available today. The patented InTether security technology enables organizations to create and share digital files of any type with intended recipients while keeping the files and data protected from misuse. By deploying InTether solutions, you gain complete control over the access, distribution and use of your copyrighted files in their electronic form. Infraworks provides a full selection of solutions that are tailored to the specific file-sharing model that you have chosen to implement.

Infraworks has developed the InTether File Security Series, which includes:

**InTether Server** – enables organizations to dynamically secure and distribute digital files over the web. **InTether SecureCD** – allows organizations to instantly secure and distribute content on CD-ROMs. **InTether Desktop** – enables content owners to share and secure digital files sent via email.

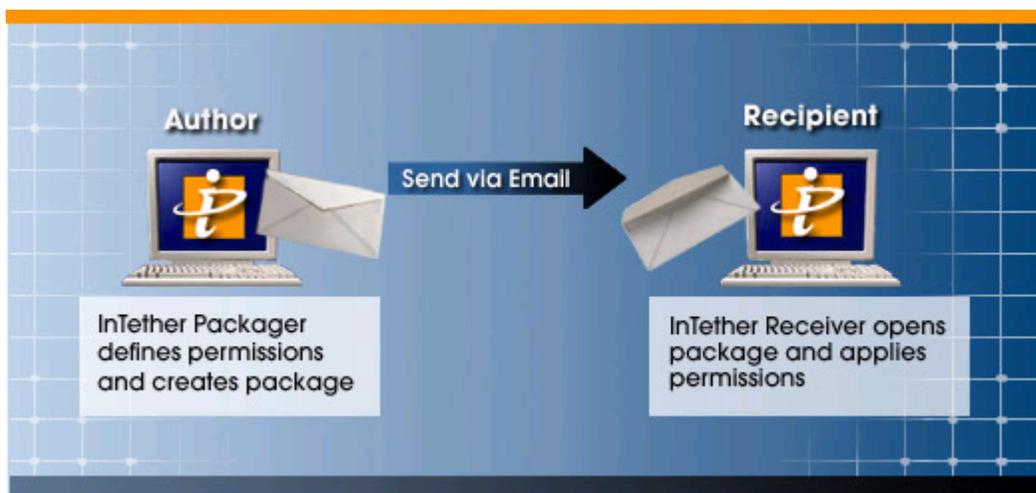
InTether Credentials pertaining to Federal criteria include:

- In Testing for Common Criteria – COACT, INC.
- SPOCK Validated (report available)
- NSTL Tested

## B. How Does InTether Work?

### InTether Components

At the heart of all of the InTether File Security Series (IFSS) are two components, InTether Packager and InTether Receiver. The InTether Packager is a core element of the IFSS product suite. It is incorporated in each of the above listed products. The InTether Receiver is a freely available application that can easily be distributed and is responsible for controlling the use of secured files on the recipient's PC. The InTether Receiver also enforces a set of usage permissions that are defined by the owner of the original files. This includes automatically removing the secured files when the permissions have expired.



### The Packager

The InTether Packager is a standard application that allows users to select a file or a file, assign specific usage permissions, and then generate an encrypted package that can be delivered through email, the web or CD.

InTether Packager allows the file owner to set the following permissions for recipients:

**Activation Date** - A file cannot be accessed prior to this specified date

**Deletion Date** - The date in which the file will be removed from a recipients machine

**Read Time** - Designate an amount of time in which a file can be used.

**Password** - Assign an extra security level by attaching a password for access to individual files

**Include InTether ID** - Lock files to individual computers to prevent unauthorized redistribution.

## **The Receiver**

The InTether Receiver is a client-side application that performs five key functions.

- Extracts the secured file and permissions and saves them to the secured area
- Controls access to the file and enforces the assigned permissions
- Creates a secure, protected environment on the client computer
- Removes the data upon expiration
- Generates and secures the InTether ID

InTether contains active security elements designed to detect and defend against attempts to violate the usage permissions. The Receiver is a one-time install, and can be used to access InTether secured files regardless of the source. Upon installation, an InTether ID is generated that is unique to each Receiver and each computer. The Receiver is distributed automatically and supplied by the InTether Server and InTether SecureCD and is available for download free at [www.infraworks.com](http://www.infraworks.com).

**USPTO Question:** What systems have been developed, are being developed, or are proposed to be developed in private voluntary industry-led entities through an open broad-based consensus process?

**Summary Response:** Infracore has included information in this section describing alternative security products (encryption, digital watermarking, proprietary readers, and DRM) and noting their challenges. Additionally we have highlighted the fact that InTether requires no change in Business process, is file format independent, and requires no data conversion, which is critical to content owners, universities and students. Lastly, no security is complete without data destruction, which is highlighted in this section as well.

### **Failed attempts at Protecting Copyrighted Material**

To date, nearly all attempts to protect digital property have relied on asymmetric encryption technology and are designed around a Digital Rights Management (DRM) concept where a set of public and private keys are used to exchange digital information in an encrypted form from the provider's web site to the recipient's PC. Initial forms of this technology supplied the decrypted file to the target PC application. Since the data was vulnerable to access during this exchange, second-generation DRM systems have embedded the data's decryption into the target application.

Although this has improved the robustness of these solutions, it has not solved the issue of accessing digital information in its un-encrypted form. The information is vulnerable once the file has been opened and while the application is using it. Any recipient accessing the digital information must also have an application that supports the decryption. Since each DRM solution is different, the applications on each end must support each other's format(s). Files can only be distributed in the format that the specific DRM-enabled application supports. This could require the sender to support multiple DRM solutions and multiple formats in order to be compatible with the target application.

Regardless of the specific DRM chosen, once the content has been accessed and the permissions have been exhausted, the access key is disabled. **The content remains on the PC of the recipient until they physically remove it from their hard drive.** This leaves the file freely available for the computer user to analyze it and try to recover a decrypted copy. In the past, DRM solutions have fallen victim to this Achilles heel.

**Digital watermarking** is another form of security used for copyright protection. It inserts copyright information into the digital object without a loss of quality. Watermarking does not provide any copy protection and does not limit the access to copyrighted material and/or inhibit the copy process itself. InTether allows the owner of copyrighted materials to protect the data after it is on the authorized recipient's computer through automatic enforcement of permissions determined by the owner. One key advantage of InTether is the ability to distribute digital files with confidence and eliminate theft and misuse of digital files by authorized recipients.

Other copyright security solutions, such as Microsoft Reader and Adobe Acrobat Reader, **require the copyrighted files to be converted into proprietary file formats** (.lit and .pdf respectively). File conversions require costly outsourcing or content owners must purchase proprietary conversions software packages to convert the files. Either method is inefficient and does not provide security from misuse by the authorized recipient. InTether allows content owners to share copyrighted materials in their native file formats while still offering in-use security.

**InTether** technology provides a method for securing and delivering files via the web. Furthermore, backend integration can be easily accomplished with an existing transaction system to allow the sale of copyrighted, downloaded files. The security is virtually transparent to the end user. The end user will receive one dialog box that summarizes the permissions associated with the file that is about to be downloaded. Otherwise, the secure file will appear in the native application associated with the file and behave exactly as the permissions set on the file dictate.

No security solution is complete if it does not have the ability to automatically **remove the data at the end of the data's lifecycle**. Infragistics Corporation owns the patent to remove the data from the recipient's machine at a time predetermined by the data owner prior to sharing the copyrighted material.

**USPTO Question:** Consistent with the types of information requested by Congress, please provide any additional comments on technological protection systems to protect digitized copyrighted works and prevent infringement.

**Response Summary:** Infracore would like to close with the following.

There are two dilemmas facing digitized copyrighted material. The first is the protection of that material from indiscriminate, uncontrolled reproduction, which would render intellectual property commercially valueless. The second dilemma is the retention of the principle of fair use, without which intellectual ferment is impossible. In the pre-digital world, there were natural barriers to indiscriminate reproduction and natural bridges to fair use. The challenge to the digital world is to recreate technologically the barriers and bridges that have traditionally existed.

InTether is a powerful technology for controlling reproduction and redistribution. It also has implicit in it, technology for enabling fair use. In future versions of InTether, such as our Workgroup release, InTether will be introducing a variety of permissions that will allow recipients of copyrighted material to reproduce - with appropriate permissions - all or part of material that they have received. InTether will enable the fair use that is one of the imperatives behind our patent tradition.