CENTER FOR COPYRIGHT INFORMATION
AND
COPYRIGHT ALERT SYSTEM
FACT SHEET

The Center for Copyright Information is a new information center dedicated to educating the public about copyright and helping to implement an unprecedented and constructive effort to stop online content theft. Parents and other ISP subscribers will benefit from a new state of the art system of alerts -- similar to fraud alerts consumers receive about their credit card accounts -- that let them know when their Internet accounts have been identified as being misused for content theft.

This is important because most subscribers, once informed that content theft is illegal, will stop engaging in it and turn to one of the many legitimate entertainment options. Some subscribers – particularly parents or caregivers – are often not aware that their Internet accounts are being used for content theft. Other subscribers may be unaware that downloading and uploading copyrighted content from illicit sources is illegal. Because internet content providers and distributors believe subscribers have a right to know about the consequences of content theft, subscribers will be fully advised about possible consequences when their accounts have been identified as being involved in content theft.

- **Center for Copyright Information**: In 2011, the Center for Copyright Information will be formally opened. This newly formed Center will help educate consumers about content theft on the Internet. It will help them to understand the difference between lawful and unlawful online downloading and file sharing. It will inform them about the importance of copyright to content creators, millions of American jobs and the economy, and to them as consumers. The Center will also inform them about lawful ways to obtain movies and music online. The Center is being established jointly by the film, music, and television industries, in partnership with Internet Service Providers (ISPs) and will benefit from guidance from consumer advocates and technical experts.

- **Best Practices:** The Center will also help develop and confirm "best-practices" for a new system of progressive Copyright Alerts, similar to credit card fraud alerts, which will alert Internet subscribers when potential content theft is identified on their Internet accounts.

- **Common Framework**: Until now, there hasn't been a common framework of best practices for alerting Internet subscribers about possible content theft. Today, many ISPs forward subscribers notifications that they receive from content owners about alleged content theft – generally by email. The Center will help establish this common framework for alerting subscribers, protecting copyrighted content and promoting access to legal online content.

- **Subscriber Right to Know:** Internet content providers and distributors believe that subscribers have a right to know when their Internet accounts are being used for content theft, or if they are otherwise unwittingly downloading or distributing files that are subject to copyright protection, because that illegal activity could expose them to legal liability and other consequences under the Terms of Service (TOS), Acceptable Use Policy (AUP) or other policies (hereinafter referred to as "published policies") of their ISP. Online content theft can also expose a family's home network and the computers that are connected to it to dangerous viruses, spyware and identity theft. P2P applications are particularly risky because they can make accessible to other P2P users all of the information on a consumer's computer, including a consumer's bank account numbers, tax returns, or sensitive health information.

- **Alerts:** Copyright Alerts will provide a thoughtful and effective system to educate Internet subscribers about copyright, advise them about the consequences of inadvertent or purposeful content theft, ensure that they are aware of the many sources of legal content and deter those who receive repeated alerts from allowing their accounts to be used for content theft. Data suggests[1] that most users (up to 70%) would stop content theft once alerted that it is occurring, that it is illegal and that there are consequences associated with continuing to engage in it. We anticipate that very few subscribers, after having received multiple alerts, will persist (or allow others to persist) in the content theft, and that most will instead turn to one of the many legitimate entertainment options. This system consists of multiple (at least five) alerts:

    - **<u>First Alert</u>**: In response to a notice from a copyright owner, an ISP will send an online alert to a subscriber, such as an email, notifying the subscriber that his/her account may have been misused for content theft, that content theft is illegal and a violation of published policies, and that

[1] This data represents of an average of the following surveys: Ifop. "*Les Français et le Téléchargement Illégal*", snep (2009): France; Synovate. "*Movie File Sharing Amongst Young New Zealanders*", NZFACT (2009): NZ; Norstat A.S. "*Survey Regarding Norwegians' Music Habits on the Internet*", Ifpi and GramArt (2009): Norway; and Entertainment Media Research. "*2009 Digital Entertainment Survey*", Wiggin (2009): UK

consequences could result from any such conduct. This first alert will also direct the subscriber to educational resources which will (i) help him/her to check the security of his/her computer and any Wifi network, (ii) provide explanatory steps which will help to avoid content theft in the future and (iii) provide information about the abundant sources of lawful music, film and TV content.

- **Second Alert**: If the alleged activity persists despite the receipt of the first alert, the subscriber may get a second similar alert that will underscore the educational messages, or the ISP may – in its discretion – proceed to the next alert.

- **Third Alert**: If the subscriber's account again appears to have been used for content theft, he/she will receive another alert, much like the initial alerts. However, this alert will provide a conspicuous mechanism (a click-through pop-up notice, landing page, or similar mechanism) asking the subscriber to acknowledge receipt of this alert. This is designed to ensure that the subscriber is aware of the third copyright alert – and reminds the subscriber that content theft conducted through their account could lead to consequences under the law and published policies.

- **Fourth Alert**: If the subscriber's account again appears to have been used for content theft, the subscriber will receive yet another alert that again requires the subscriber to acknowledge receipt.

- **Fifth Alert**: If the subscriber's account again appears to have been used for content theft, the ISP will send yet another alert. At this time, the ISP may take one of several steps, specified in its published policies, reasonably calculated to stop future content theft. These steps, referred to as "Mitigation Measures," may include, for example: temporary reductions of Internet speeds, redirection to a landing page until the subscriber contacts the ISP to discuss the matter or reviews and responds to some educational information about copyright, or other measures that the ISP may deem necessary to help resolve the matter. ISPs are not obligated to impose any Mitigation Measure which would disable or be reasonably likely to disable the subscriber's voice telephone service (including the ability to call 911), e-mail account, or any security or health service (such as home security or medical monitoring). The use of the mitigation measure is waivable by the ISP at this point.

- **Sixth Alert**: Whether or not the ISP has previously waived the Mitigation Measure, if the subscriber's account again appears to have been used for content theft, the ISP will send another alert and will implement a Mitigation Measure as described above. As described above, it's likely that very few subscribers who after having received multiple alerts, will persist (or allow others to persist) in the content theft.

- **No Requirement of Termination:** This alert system does not, in any circumstance, require the ISP to terminate an Internet subscriber's account. However, section 512 of the Digital Millennium Copyright Act requires that the ISPs have in place a termination policy for repeat copyright infringers as a condition of availing themselves of the Act's "safe harbor" provision. That is why subscribers have a right to know if it has been alleged that content theft is taking place on their accounts, and a right to respond. As provided under current law, copyright owners may also seek remedies directly against the owner of an Internet account based on evidence they may collect.

- **Independent Review**: Before a Mitigation Measure is imposed, an Internet subscriber may request independent review to invalidate the alert and avoid any Mitigation Measure on the basis that the online activity in question is lawful or that the subscriber's account was identified in error. To request an independent review and avoid spurious claims, there is a $35 filing fee, which is waivable by the independent reviewer. This is a non-exclusive alternative, and subscribers retain the right to challenge any action in a court of law. The independent reviewer will have access to expert advice on copyright law.

- **Contrary to Some Press Reports, This is not "Three Strikes":** This creates no new laws or formal legal procedures and it does not require account suspension or termination. It simply sets in place a common "best practices" framework to give Internet subscribers the information they need about content theft, and how to avoid the legal exposure and security risks that content theft can create for them.

- **Privacy:** There is no mechanism enabling Content Owners to "figure out" which specific Subscriber account is involved in an alleged infringement – and at no time will ISPs share Internet subscribers' personal information (name, address, etc.) with anyone else (including the Content Owners) except pursuant to a properly issued subpoena or court order. None of the data exchanged between Content Owners and ISPs will include any personal information about subscribers.

- **Preservation of Essential Services:** ISPs are not required to impose any Mitigation Measure that will disable or be reasonably likely to disable the subscriber's voice telephone service (including the ability to call 911), email, or any security or health service (such as home security or medical monitoring).