

FAQ's
on
The Center for Copyright Information
And
Copyright Alert System

1. How significant is online content theft?

- Content theft is estimated to cost the U.S. economy \$58 billion, 373,000 American jobs and \$16 billion in lost employee earnings every year, and to cost federal, state and local governments \$2.6 billion each year in lost tax revenue. However, data suggests¹ 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. A new educational center and system of alerts – similar to credit card fraud alerts – will help address this problem. The alerts will let subscribers know when their accounts have been identified for possible content theft, advise subscribers of the serious consequences associated with it, and encourage them to stop it from occurring again.

2. What is the Center for Copyright Information?

- The Center for Copyright Information (“CCI”) will focus on educating subscribers about the importance of copyright protection and lawful ways to obtain movies and music online. The Center will also help to develop and confirm “best-practices” for a new system of progressive Copyright Alerts, similar to credit card fraud alerts, which will alert subscribers when potential content theft is identified on their Internet accounts. 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 by consumer advocates and technical experts serving on its advisory committee or providing other expert services.

3. What are Copyright Alerts?

- Copyright Alerts are part of a thoughtful and effective system to educate subscribers about copyright, advise them about the consequences of inadvertent or intentional online content theft, and deter those who receive repeated alerts from allowing their accounts to be used for content theft. Alerts will be progressive, in the sense that successive alerts will reinforce the seriousness of content theft and

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*”, Wiggins (2009): UK

inform the recipient how to address the activity that is precipitating the alerts. For users who repeatedly fail to respond to alerts, the alerts will inform them of steps that will be taken to mitigate the ongoing content theft.

- Under this system, an ISP, in response to a notice from a copyright holder, will send an alert to a subscriber notifying the subscriber that his/her account may have been misused for online content theft, that content theft is illegal and a violation of the Terms of Service (TOS), Acceptable Use Policy (AUP) or other policies of their ISP (hereinafter referred to as “published policies”), and that consequences could result from any such conduct. Today, when fraud is detected on a consumer’s credit card account, the credit card company notifies the consumer by an email, a text message or a phone call. These alerts are intended to be similar to credit card fraud alerts.
- Subsequent alerts may include notifications in the form of pop-ups or redirection to a special page displaying the alert. Failure to respond to these alerts will lead to additional steps designed to ensure that the account comes into compliance. These steps, referred to as “Mitigation Measures,” might 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. These steps will only be taken after multiple alerts and a failure by the subscriber to respond. This system consists of at least five alerts.
- Data suggests that most users 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.

4. Why do subscribers need to get Copyright Alerts about alleged online content theft?

- Subscribers may not know that their Internet account is being used for possibly illegal purposes that could expose them to legal liability and other consequences under published policies of the ISP. Online content theft also can expose a family’s home network and the computers that are connected to it to dangerous viruses, spyware and identity theft. Today, many ISPs forward notifications to their subscribers that they receive from content owners about alleged content theft – generally by email. Until now, however, there has not been a common framework of “best practices” for effectively alerting subscribers, protecting copyrighted content and promoting access to legal online content.

Also, many Internet subscribers may be unfamiliar with the concept of copyright and the consequences of content theft. Subscribers may not be aware that family

members and others who have access to their Internet accounts may be engaged in content theft; for example, a parent or caregiver may not know that a child is illegally downloading music and movies. Also, some subscribers may not realize that their home network is insufficiently secured and that, for example, unauthorized individuals may be using their wireless network to engage in content theft. In some cases, subscribers may know that content theft is illegal and a violation of published policies, but believe they are immune from any exposure or consequences. The system of Copyright Alerts is intended to ensure that subscribers get this critical information in easily understandable ways with clear guidance on what they can do to address the problem.

5. What happens the first time a subscriber's account appears to have been used for online content theft?

- An ISP, in response to a notice from a copyright holder, will send an alert to a subscriber notifying the subscriber that his/her account may have been misused for online content theft, that content theft is illegal and a violation of the published policies of the ISP, and that consequences could result from any such conduct.

6. What happens if the subscriber's account again appears to have been used for online content theft?

- If the alleged content theft 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.

7. What happens if the subscriber's account again appears to have been used for online content theft after being sent educational alerts?

- If the alleged content theft persists after educational alerts are sent, then an additional alert will be sent which will include a conspicuous mechanism (such as a click-through pop-up notice, landing page, or other mechanism) asking the subscriber to acknowledge receipt of the alert. This is designed to ensure that the subscriber is aware of the copyright alert – and reminds the subscriber that content theft conducted through their account could lead to consequences under the law and published policies.
- If, after this alert asking for acknowledgment, the subscriber's account again appears to have been used in connection with online content theft, the subscriber will be sent yet another alert that again will require the subscriber to acknowledge receipt.

8. What if after acknowledging receipt of these Copyright Alerts (as many as four at this point) the subscriber's account still appears to be engaged in online content theft?

- If, after these educational and acknowledgment alerts, the subscriber's account still appears to be engaged in content theft, the ISP will send yet another alert. At this time, the ISP may take one of several steps, referred to as "Mitigation Measures" reasonably calculated to stop future content theft. These 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 (as specified in published policies) that the ISP may deem necessary to help resolve the matter. ISPs are not required 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 ISP may also waive the Mitigation Measure. Any and all steps an ISP may take will be specified by their published policies.

9. What if after this alert, the subscriber's account appears to persist in online content theft?

- If, after this latest alert, the subscriber's account still appears to be engaged in content theft, the ISP will send yet another alert and will implement a Mitigation Measure as described above. We anticipate that very few subscribers, after repeated alerts, will persist (or allow others to persist) in the content theft.

10. Is termination of the subscriber's account part of this program?

- No. This alert system does not, in any circumstance, require the ISP to terminate a subscriber account. This alert system is intended to notify and educate the subscriber. 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. This 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. Because the vast majority of subscribers observe copyright laws as a matter of course, and the participating ISPs and content companies believe that even more will do so if the Copyright Alert system is effective, it is reasonable to expect that very few subscribers will ever face this situation.

11. What if the subscriber believes that he or she is not engaged in copyright infringement?

- Before a Mitigation Measure is imposed, a subscriber may request independent review. To request an independent review, there is a \$35 filing fee, which is

waivable. This is a non-exclusive procedure, and any subscriber may choose to challenge any action in a court of law.

12. How does Independent Review work?

- A qualified, independent entity, separate from the Center for Copyright Information, will be engaged to establish and operate the Independent Review mechanism. Under this system, before a Mitigation Measure is imposed, a 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 (e.g. protected by fair use or authorized by the owner of the copyrighted material) or that the subscriber's account was identified in error. This is a non-exclusive alternative, and subscribers retain the right to challenge any action in a court of law. An independent reviewer will have access to expert advice on copyright law.

13. How is this different than what is done today to advise consumers?

- Many ISPs currently forward to subscribers notifications that they receive from content owners about alleged content theft – generally by email. Until now, however, there has not been a common framework of “best practices” for effectively alerting subscribers, protecting copyrighted content and promoting access to legal online content. A shared system of best practices will help to better ensure that a subscriber fully understands allegations of content theft and what they can do to address it.
- The Center for Copyright Information provides a new consumer-focused resource for copyright-related education.
- This system also provides a first-of-its-kind independent review alternative for subscribers to seek review of allegations by content owners of content theft using the Internet subscriber's account.

14. How is this different than international examples such as “Three Strikes” laws?

- Contrary to some press reports, this program is unlike so-called “three strikes” as it creates no new laws or formal legal procedures, nor does this system require account suspension or termination. Rather, it is a voluntary cooperative effort among ISPs and leading U.S. content providers. Neither the copyright owners nor the ISPs will take any new actions that are not already authorized under existing law. The goal is to enhance awareness and deter content theft through education and constructive communications, and direct subscribers to legitimate sources of content.

15. How do ISPs and content companies know who downloaded a pirated movie or song?

- Content companies don't know who downloaded and shared a pirated movie or song. When files are distributed on the Internet over peer-to-peer (P2P) networks, the IP address associated with the subscriber's account is visible by design to other users on the network. Leading technology companies have developed state-of-the-art software that participates in these P2P networks to identify pirated film, TV and music content and the IP addresses associated with the illegal distribution of that content. Content owners provide these IP addresses to ISPs along with additional information about the uploaded file. The ISP is then able to associate the IP address with the account on their network, and can forward the alert to that subscriber. It is important to note that ISPs never provide any personally identifiable information to copyright holders – as part of the alert process or for any other reason -- without a properly issued subpoena or court order.

16. How will this system of Copyright Alerts change the online experience for most Internet subscribers?

- Since most subscribers do not download or upload pirated content, the vast majority of subscribers likely will never see a Copyright Alert. However, when subscribers' accounts have been identified as being involved in content theft, subscribers are likely to receive one or more Copyright Alerts.

17. Is the purpose of this program to punish subscribers who download pirated movies and music?

- No. The purpose is to educate subscribers about copyright and the many sources of legal content, as well as to help them guard against the risks and consequences associated with content theft. When subscribers repeatedly fail to respond to alerts, ISPs will impose Mitigation Measures, the purpose of which is to educate and stop the alleged content theft in question, not to punish. No ISP wants to lose a customer or see a customer face legal trouble based on a misunderstanding, so the alert system provides every opportunity to set the record straight. As noted above, only a small fraction of all subscribers are likely to ever face a Mitigation Measure due to their online activity – they are far more likely to address the problem based on the initial alerts. It has been found that notification programs are most effective when subscribers truly understand that there are consequences associated with content theft. The number-one goal of content owners and ISPs is to encourage subscribers to enjoy all the legal content they want from legitimate sources.

18. Is there a blacklist?

- No. At no time will ISPs share subscribers' personal information (name, address, etc.) with anyone else (including the content owners or other ISPs) except pursuant to a properly issued subpoena or court order. All information provided to copyright holders is in a form that guarantees anonymity. The Center for

Copyright Information will work very closely with privacy and consumer advocates to enhance methods of protecting subscriber privacy every step of the way.

19. Isn't this just about ISPs trying to reduce online traffic?

- No. The fastest-growing segment of web traffic is legal online content that subscribers will be encouraged to use. Access to lawful content services is expanding rapidly, and ISPs are seeing more households add broadband service and TV service at the same time. According to Nielsen, the number of households with both a broadband connection and a home television subscription increased in the last year from 61% to 66% of households.

20. Isn't content theft driven by the fact that consumers can't get legal movies and music online?

- Vastly more music, movies, and TV shows are available online from legitimate sources than ever before. MOG, Pandora, Rhapsody, Amazon MP3, Napster and Vevo are just a few examples of growing businesses delivering music to consumers digitally. Apple's iTunes is virtually ubiquitous. Cable, phone and satellite companies are offering "TV Everywhere"-type services. Web based services from Netflix, Amazon and Apple TV are booming – in fact, Netflix is now one of the largest video distributors in America today with more than 20 million customers, and it offers nearly 20,000 streaming content titles to consumers. The boom in smartphones and tablets has put digital music, TV and film in the pocket of most Americans. There are many legitimate options for consumers who want their movies, TV shows and music online and on the go.

21. Does this system require mandatory filtering of web traffic?

- No. The process of identifying potential online content theft is described above. It is in place and has been the basis for consumer notices for several years. As has been the case with earlier notices, alerts are triggered only when an ISP receives a notice from a copyright holder or its representative. There is no filtering or monitoring of any user accounts. There is no caching of "click data." The ISP matches the IP address identified by the copyright holder with a subscriber account, and then forwards a Copyright Alert to the subscriber account as described above. No ISPs will share any personally identifiable information with another ISP or with a copyright owner, unless required to do so by properly issued subpoenas or court orders.

22. What are the risks of peer-to-peer file sharing ("P2P")?

- In addition to exposure from violating copyright law and published policies, viruses, malware and spyware described above, the use of P2P applications can expose a consumer's bank account numbers, tax returns, and sensitive health information to other P2P users.