Copy protection

From Wikipedia, the free encyclopedia

Copy protection, also known as **content protection**, **copy prevention** and **copy restriction**, is any effort designed to prevent the reproduction of software, films, music, and other media, usually for copyright reasons.[1] Various methods have been devised to prevent reproduction so that companies will gain benefit from each person who obtains an authorized copy of their product. Unauthorized copying and distribution accounted for $2.4 billion in lost revenue in the United States alone in the 1990s,[2] and is assumed to be causing impact on revenues in the music and the game industry, leading to proposal of stricter copyright laws such as PIPA. Some methods of copy protection have also led to criticisms because it caused inconvenience for honest consumers, or it secretly installed additional or unwanted software to detect copying activities on the consumer's computer. Making copy protection effective while protecting consumer rights is still an ongoing problem with media publication.

Contents

Terminology

Media corporations have always used the term **copy protection**, but critics argue that the term tends to sway the public into identifying with the publishers, who favor restriction technologies, rather than with the users.[3] **Copy prevention** and **copy control** may be more neutral terms. "Copy protection" is a misnomer for some systems, because any number of copies can be made from an original and all of these copies will work, but only in one computer, or only with one dongle, or only with another device that cannot be easily copied.

The term is also often related to, and confused with, the concept of digital rights management. Digital rights management is a more general term because it includes all sorts of management of works, including copy restrictions. Copy protection may include measures that are not digital. A more appropriate term may be "technological protection measures" (TPMs),[4] which is often defined as the use of technological tools in order to restrict the use or access to a work.

Business rationale

Copy protection is most commonly found on videotapes, DVDs, computer software discs, video game discs and cartridges, audio CDs and some VCDs.

Many media formats are easy to copy using a machine, allowing consumers to distribute copies to their friends, a practice known as "casual copying".

Companies publish works under copy protection because they believe that the cost of implementing the copy protection will be less than the revenue produced by consumers who buy the product instead of acquiring it through casually copied media.

Opponents of copy protection argue that people who obtain free copies only use what they can get for free, and would not purchase their own copy if they were unable to obtain a free copy. Some even argue that free copies increase profit; people who receive a free copy of a music CD may then go and buy more of that band's music, which they would not have done otherwise.

Some publishers have avoided copy-protecting their products, on the theory that the resulting inconvenience to their users outweighs any benefit of frustrating "casual copying".

From the perspective of the end user, copy protection is always a cost. DRM and license managers sometimes fail, are inconvenient to use, and may not afford the user all of the legal use of the product he has purchased.

The term *copy protection* refers to the technology used to attempt to frustrate copying, and not to the legal remedies available to publishers or authors whose copyrights are violated. Software usage models range from node locking to floating licenses (where a fixed number licenses can be concurrently used across an enterprise), grid computing (where multiple computers function as one unit and so use a common license) and electronic licensing (where features can be purchased and activated online). The term *license management* refers to broad platforms which enable the specification, enforcement and tracking of software licenses. To safeguard copy protection and license management technologies themselves against tampering and hacking, software anti-tamper methods are used.

Floating licenses are also being referred to as *Indirect Licenses*, and are licenses that at the time they are issued, there is no actually user who will use them. That has some technical influence over some of their characteristics. *Direct Licenses* are issued after a certain user requires it. As an example, an activated Microsoft product, contains a *Direct License* which is locked to the PC where the product is installed.

From business standpoint, on the other hand, some services now try to monetize on additional services other than the media content so users can have better experience than simply obtaining the copied product.[5]

Technical challenges

From a technical standpoint, it would seem theoretically impossible to completely prevent users from making copies of the media they purchase, as long as a "writer" is available that can write to blank media. The basic technical fact is that all types of media require a "player" — a CD player, DVD player, videotape player, computer or video game console. The player has to be able to read the media in order to display it to a human. In turn, then, logically, a player could be built that first reads the media, and then writes out an exact copy of what was read, to the same type of media.

At a minimum, digital copy protection of non-interactive works is subject to the analog hole: regardless of any digital restrictions, if music can be heard by the human ear, it can also be recorded (at the very least, with a microphone and tape recorder); if a film can be viewed by the human eye, it can also be recorded (at the very least, with a video camera and recorder). In practice, almost-perfect copies can typically be made by tapping into the analog output of a player (e.g. the speaker output or headphone jacks) and, once redigitized into an unprotected form, duplicated indefinitely. Copying text-based content in this way is more tedious, but the same principle applies: if it can be printed or displayed, it can also be scanned and OCRed. With basic software and some patience, these techniques can be applied by a typical computer-literate user.

Since these basic technical facts exist, it follows that a determined individual will definitely succeed in copying any media, given enough time and resources. Media publishers understand this; copy protection is not intended to stop professional operations involved in the unauthorized mass duplication of media, but rather to stop "casual copying".

Copying of information goods which are downloaded (rather than being mass-duplicated as with physical media) can be inexpensively customized for each download, and thus restricted more effectively, in a process known as "traitor tracing". They can be encrypted in a fashion which is unique for each user's computer, and the decryption system can be made tamper-resistant.

Methods

For information on individual protection schemes and technologies, see List of copy protection schemes or relevant category page.

Computer software

Copy protection for computer software, especially for games, has been a long cat-and-mouse struggle between publishers and crackers. These were (and are) programmers who would defeat copy protection on software as a hobby, add their alias to the title screen, and then distribute the "cracked" product to the network of warez BBSes or Internet sites that specialized in distributing unauthorized copies of software.

Early ages

When computer software was still distributed in audio cassettes, audio copying was unreliable, while digital copying was time consuming. Software prices were comparable with audio cassette price.[2][6] To make digital copying more difficult, many programs used non-standard loading methods (loaders incompatible with standard BASIC loaders, or loaders that used different transfer speed.

Unauthorized software copying began to be a problem when floppy disks became the common storage media.[6] The ease of copying depended on the system; Jerry Pournelle wrote in *BYTE* in 1983 that "CP/M doesn't lend itself to copy protection" so its users "haven't been too worried" about it, while "Apple users, though, have always had the problem. So have those who used TRS-DOS, and I understand that MS-DOS has copy protection features".[7] Apple and Commodore 64 computers were extremely varied and creative because most of the floppy disk reading and writing was controlled by software (or firmware), not by hardware. The first copy protection was for cassette tapes and consisted of a loader at the beginning of the tape, which read a specially formatted section which followed.

The first protection of floppy disks consisted of changing the address marks, bit slip marks, data marks, or end of data marks for each sector. For example, Apple's standard sector markings were:

- **D5 AA 96** for the address mark. That was followed by track, sector, and checksum.
- **DE AA EB** concluded the address header with what are known as bit slip marks.
- **D5 AA AD** was used for the data mark and the end of data mark was another **DE AA EB**.

Changing any of these marks required fairly minimal changes to the software routines in Apple DOS which read and wrote the floppy disk, but produced a disk that could not be copied by any of the standard copiers, such as Apple's COPYA program. Some protection schemes used more complicated systems that changed the marks by track or even within a track.

1980s Locksmith

Pournelle disliked copy protection and, except for games, refused to review software that used it. He did not believe that it was useful, writing in 1983 that "For every copy protection scheme there's a hacker ready to defeat it. Most involve so-called nibble/nybble copiers, which try to analyze the original disk and then make a copy".[7] IBM's Don Estridge agreed: "I guarantee that whatever scheme you come up with will take less time to break than to think of it." While calling piracy "a threat to software development. It's going to dry up the software", he said "It's wrong to copy-protect programs ... There ought to be some way to stop [piracy] without creating products that are unusable."[8]

By 1980, the first 'nibble' copier, Locksmith, was introduced. These copiers reproduced copy protected floppy disks an entire track at a time, ignoring how the sectors were marked. This was harder to do than it sounds for two reasons: firstly, Apple disks did not use the index hole to mark the start of a track; their drives could not even detect the index hole. Tracks could thus start anywhere, but the copied track had to have this "write splice", which always caused some bits to be lost or duplicated due to speed variations, roughly in the same (unused for payload data) place as the original, or it would not work. Secondly, Apple used special "self-sync" bytes to achieve agreement between drive controller and computer about where any byte ended and the next one started on the disk. These bytes were written as normal data bytes followed by a slightly longer than normal pause, which was notoriously unreliable to detect on read-back; still, you had to get the self-sync bytes roughly right as without them being present in the right places, the copy would not work, and with them present in too many places, the track would not fit on the destination disk. Locksmith copied Apple II disks by taking advantage of the fact that these sync fields between sectors almost always consisted of a long string of FF (hex) bytes. It found the longest string of FFs, which usually occurred between the last and first sectors on each track, and began writing the track in the middle of that; also it assumed that any long string of FF bytes was a sync sequence and introduced the necessary short pauses after writing each of them to the copy. Ironically, Locksmith would not copy itself. The first Locksmith measured the distance between sector 1 of each track. Copy protection engineers quickly figured out what Locksmith was doing and began to use the same technique to defeat it. Locksmith countered by introducing the ability to reproduce track alignment and prevented itself from being copied by embedding a special sequence of nibbles, that if found, would stop the copy process. Henry Roberts (CTO of Nalpeiron (http://www.nalpeiron.com)), a graduate student in computer science at the University of South Carolina, reverse engineered Locksmith, found the sequence and distributed the information to some of the 7 or 8 people producing copy protection at the time.

For some time, Locksmith continued to defeat virtually all of the copy protection systems in existence. The next advance came from Henry Roberts' thesis on software copy protection, which devised a way of replacing Apple’s sync field of FFs with random appearing patterns of bytes. Because the graduate student had frequent copy protection discussions with Apple’s copy protection engineer, Apple developed a copy protection system which made use of this technique. Henry Roberts then wrote a competitive program to Locksmith, Back It UP. He devised several methods for defeating that, and ultimately a method was devised for reading self sync fields directly, regardless of what nibbles they contained. The back and forth struggle between copy protection engineers and nibble copiers continued until the Apple II became obsolete and was replaced by the IBM PC and its clones.

In 1989 Gilman Louie, head of Spectrum Holobyte, stated that copy protection added about $0.50 per copy to the cost of production of a game.[9]

1990s CD-R

Floppy disks were later displaced by CDs as the preferred method of distribution, with companies like Macrovision and Sony providing copy protection schemes that worked by writing data to places on the CD-ROM where a CD-R drive cannot normally write. Such a scheme had been used for the PlayStation and could not be circumvented easily without the use of a modchip.

For software publishers, a less expensive method of copy protection is to write the software so that it requires some evidence from the user that they have actually purchased the software, usually by asking a question that only a user with a software manual could answer (for example, "What is the 4th word on

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**