



# Digital Content Locks

## *Introduction*

Media publishers place locks on digital content with the objective of controlling secondary uses, often in the name of impeding copyright infringement. These locks restrict what people can and cannot do with the media and hardware they have legitimately purchased. These locks are variously called digital locks, Digital Rights Management (DRM), or Technological Protection Measures (TPMs).

DRM is one of several ways IP owners try to use software not only to enforce IP rights, but to also control add-on innovation and competition. Proponents of stronger intellectual property enforcement are pushing for provisions that make it difficult or illegal to break the locks on content, even if the end use is lawful. Unfortunately, these provisions have helped to further entrench copyright controls and many content producers have misused them to chill competition, free speech, and fair use.

## *Policy Background*

Countries that have signed onto various bilateral and regional trade agreements with the US are obligated to implement their own anti-circumvention laws. However, unlike the WCT and WPPT, which allow countries more flexibility in implementing anti-circumvention laws consistent with their national copyright exceptions, the recent free trade agreements require far broader anti-circumvention laws that mirror the US's Digital Millennium Copyright Act (DMCA). In that lurks the danger that foreign and domestic DRM-using companies will be able to chill academic research, punish home-grown innovators and entrepreneurs, and cover their misdeeds with the assistance of the public's tax-funded courts and police system.

In the US, the DMCA prohibits circumventing DRM used to protect copyrighted works. Trade agreements, like ACTA, TPP, and the last 10 bilateral free trade agreements with the US have exported this DMCA framework on digital locks to other countries. National policy choices on DRM can have significant impact on a wide range of areas (specific examples listed below). 12 years of the US DMCA show that overbroad DRM policies harm important public policy interests outside the copyright sphere.

At the outset, the music industry took the lead on using DRM to, for example, limit their customer's ability to play the music they had purchased on unapproved devices. Since then, DRM on music has mostly disappeared, but it is widely used in other forms of content such as video, mobile devices, e-books, and video games.

## ***Anti-Circumvention Provisions***

Anti-circumvention provisions are laws that forbid the making, distribution, and use of technologies that allow people to "circumvent," or break DRM used to lock down copyrighted works. These provisions are harmful to consumers, undermine competition and innovation, and unnecessarily preempt users' fair uses of copyrighted content, all the while making no appreciable dent in "digital piracy." Nonetheless, IP owners are working hard to put even stronger legal restrictions in place to entrench this system, and are effectively attempting to make every day uses of content illegal.

In the US, the DMCA does authorize a process for seeking exemptions for breaking digital locks for specific lawful purposes. In practice, however, there are many significant barriers to obtaining and maintaining such exemptions. Moreover, even if circumvention is legal under some specific circumstances, in a majority of jurisdictions the creation and distribution of technologies, resources, and tools to break those locks are illegal. Since most people do not know how to develop these tools themselves, DRM continues to be a barrier for people who do not have the time or the ability to work out a method to free the content for fair uses themselves.

Some proposed international agreements and initiatives would require criminal penalties for the removal or alteration of DRM, or if someone is caught distributing a method of circumventing locks. Further, some provisions included in the same legal instrument limit the number of lawful uses that can be allowed.

## ***Examples of Uses and Communities Impacted***

The following are some specific examples of the types of problems that DRM creates, especially when it is paired with laws that forbid breaking encryption under most circumstances:

- Consumer rights
  - DRM can prevent e-books from being read on unapproved e-book readers, shared with friends, or donated to a library.
  - DRM can prevent films or other audiovisual content on a disc from being copied onto a portable media player or other device with no disc drive.
  - DRM enhances barriers on smart-phones, preventing certain applications from being installed and/or impeding consumers' ability to switch service providers.
- Visually impaired community
  - DRM can prevent the blind and visually impaired from changing content formats so as to make material more accessible, such as freeing the content to use text-to-speech software.
- Education
  - Film professors, media studies educators, and students may not be able to show or use film/audiovisual clips for educational purposes.
- Security research
  - Anti-circumvention laws can prevent security researchers from circumventing digital locks in order to conduct research on a device.
  - Security experts may not publicize or publish legitimate encryption research for fear of being held liable for circumventing the encryption methods they study.

- Innovation
  - DRM can and has been used to block aftermarket competition, such as laser printer toner cartridges, garage door openers, and computer maintenance services.
  - Major phone manufacturers and providers have used DRM to try to tie devices to their own proprietary software and services.

### ***EFF's Position***

Since DRM control all access to a copyrighted work, including access for lawful, non copyright-infringing purposes, a legal ban on circumventing DRM would give rights holders a new right of controlling access to copyrighted works that is separate from and potentially unconnected to the enumerated copyrights contemplated under the Berne Convention, the WCT, and the WPPT. Thus, a legal prohibition on circumventing access control TPMs could effectively override the traditional boundaries of copyright law.

EFF's stance is quite clear: DRM is harmful to consumers, it undermines competition and innovation, and unnecessarily restricts users' fair uses of copyrighted content—all the while making no appreciable dent in "digital piracy." Anti-circumvention laws, like the DMCA, that make it illegal to break the DRM, which make the DRM problem much worse.