Legally Speaking

Anti-Circumvention Rules Limit Reverse Engineering

Considering some of the requested exceptions to technical protection mechanisms.

Until the U.S. Congress passed the Digital Millennium Copyright Act (DMCA) in 1998, reverse engineering of computer programs and other digital works was widely regarded as lawful in the U.S. The DMCA changed the law because the entertainment industry feared clever hackers could and would bypass technical protection measures (TPMs) that the industry planned to use to protect their copyrighted works from unauthorized copying and dissemination. The industry persuaded Congress to make it illegal to circumvent TPMs and to make or offer circumvention tools to the public.

Circumvention of TPMs is, of course, a form of reverse engineering. This activity is now illegal not only in the U.S., but also in most of the rest of the world unless there is a special exception that permits circumvention_reverse engineering for specific purposes under specific conditions.

The DMCA rules, for instance, include exceptions for law enforcement, intelligence, and national security purposes, for making software interoperable, and for encryption and computer security research under certain conditions.

In response to expressions of concern that the anti-circumvention rules might have detrimental effects on the ability to make fair and otherwise lawful uses of technically protected digital content, Congress created a triennial rulemaking process that enables affected persons to request special exceptions to the anti-circumvention rules to engage in specified legitimate activities that TPMs are thwarting.

In November 2014, the Copyright Office received more than 40 proposals for special exceptions to the DMCA anti-circumvention rules. In February 2015, the Office received detailed comments explaining the rationales for the proposed exceptions. In March, opponents had the opportunity to express their objections to the proposed exceptions. In late May, the Office held hearings to allow proponents to offer further arguments in support of proposed exemptions and opponents to rebut those arguments. Thereafter the Copyright Office will review the record, hold some hearings, and ultimately issue rules that will either grant or deny the requested exceptions. This column provides an overview of the requested exceptions and delves into some proposals that may be of interest to computing professionals.

Overview of Submissions

 Approximately half of the proposed exceptions aim to enable interoperability with devices or software that the anti-circumvention rules arguably makes illegal. Some submissions argue for exceptions to allow bypassing TPMs for purposes of repair and modification of software in vehicles. A few ask for broader exceptions for computer security research purposes.
Several proposed exceptions aim to overcome impediments the anti-circumvention rules pose for creating multimedia e-books, other educational materials, documentary films, and remixes of technically protected works. Two submissions request exceptions for bypassing TPMs to provide assistive technologies for print-disabled persons so they can, for example, have access to digital books in alternative formats.

One submission asks for an exception to enable consumers to be able to continue to use videogames they have purchased after the games' makers have stopped providing support for the games. Two other submissions seek to enable space-shifting of DVD movies. Two others want to make broader personal uses of technically protected works. All submissions for this year's triennial review can be found at http://copyright.gov/1201.

Missing from the triennial review in 2014–2015 is a proposed exception to allow bypassing of TPMs to “unlock” cellphones so their owners can access alternative wireless networks. Even though the Copyright Office denied a requested exception to enable this activity in the last triennial review, Congress passed a special law in 2014 that granted an exception for this legitimate activity, a sensible result given that cellphone unlocking poses no threat of copyright infringement.

**Interoperability**

Because the DMCA rules have an interoperability exception, it may seem puzzling that so many of the proposed exceptions to the anti-circumvention rules address interoperability issues. The existing exception permits reverse engineering of technically protected software “for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs.” The information obtained thereby can only be used or disseminated to others for interoperability purposes.

Does that exception permit circumvention for purposes of enabling consumers to use computer tablets or wearable computing devices to access alternative wireless networks or to access mobile hotspots? The Rural Wireless Association fears it does not, so it is seeking exemptions for these kinds of activities. Unfortunately, the cellphone unlocking exception passed by Congress does not extend to these devices. Yet, these uses would seem to pose no threat of copyright infringement to justify outlawing this type of circumvention of TPMs.

Another interoperability exception being sought is Public Knowledge’s effort to enable bypassing of TPMs that makers of 3D-printing devices have embedded in their software to stop unauthorized firms from competing in the supply of feedstock to owners of their 3D printers. Competition policy
would seem to support the grant of this exception, which also poses no threat of copyright infringement.

Two other interoperability exceptions focus on bypassing TPMs to enable consumers to have more choices on the applications that can run on their devices. One submission asks for an exception so owners of Linux operating system computers can watch lawfully purchased DVD movies. Another submission requests an exception so owners of videogame consoles can bypass TPMs that limit the applications that can run on those consoles.

**Computer Security**

Computer researchers Steve Bellovin, Matt Blaze, Ed Felten, Alex Halderman, and Nadia Heninger submitted a request for a computer security testing exception that would permit bypassing TPMs to access computer software and databases embodied in various technologies to test for vulnerabilities, malfunctions, and flaws.

Among the types of software systems in devices these researchers envision testing are: insulin pumps, pacemakers, car components (including braking and acceleration systems), controls for nuclear power plants, smart grids, and transit systems, as well as smart technologies for the home. These researchers argue that such systems are very important for the health and safety of their users and of the public at large. Malfunctions, flaws, and vulnerabilities may cause considerable harms to individuals and to the public, so good faith testing is a public good. It too poses no threat of infringement, which was the principal justification for adoption of the anti-circumvention rules in the first place.

There is an existing computer security exception in the DMCA, but it requires advance permission of the owner of the computing system being tested and seems to limit the dissemination of results of security testing to the owner of that computing system.

The Bellovin submission wants computer security researchers to be able to test vulnerabilities without getting advance permission. The researchers also want to be able to disseminate their research results in responsible ways, such as by presentation of research results at conferences and in journal publications. The DMCA rules now contemplate that a copyright owner in technically protected software could enjoin dissemination of research results. This has had a chilling effect on the research that can be done to test the security of a wide variety of computing systems.

**What Will the Office Do?**

If the past is any predictor of the future, chances are quite high the Copyright Office will eventually deny the overwhelming majority of the requested anti-circumvention exceptions, no matter how harmless they might seem.

Some proposals will likely be rejected because the Office believes proponents failed to prove that TPMs are actually an impediment to lawful uses of copyrighted works; it is not enough to assert that TPMs might impede legitimate activities.

Some proposals may be denied because the Office perceives the requested exception will enable infringing uses. Eldridge Alexander, for instance, is unlikely to get an exception so he can bypass CSS to create a software library of his DVD movies because bypassing CSS would also enable infringing uses of the movies.

The Office may dismiss some requested exceptions as unnecessary because it perceives there are other ways to achieve the stated objective (for example, video capture of images from movies for educational or critical uses rather than bypassing the TPMs).

Even those exceptions the Office grants may be more restrictive as granted than as requested. During the last triennial review, for example, the Office was willing to grant an exception for film studies professors to bypass CSS to show clips from movies to illustrate filmmaking techniques. However, the Office did not recognize that many other types of instructors could benefit from an exception that enabled them to make fair use clips of movies to illustrate other types of lessons.

During the current triennial review, the Authors Alliance (of which I am a co-founder) has proposed exception for multimedia e-books that would, for instance, enable me to show clips from various James Bond movies so that my students could consider whether James Bond is an “idea” or an “expression” under copyright law, an issue that has been litigated in some U.S. cases.

Will the Office recognize the validity of the interoperability and computer security testing exceptions being sought? One can certainly hope so. However, without a team of technologists to analyze the submissions and advise the Office about the exception proposals, there is reason to worry the Office will regard these exceptions skeptically, especially if entertainment industry groups oppose them as they have in the past.

**Conclusion**

Congress should have adopted narrower anti-circumvention rules in the first place. Only circumventions that facilitate copyright infringement should be illegal. This would obviate the need for a triennial review process, and make reverse engineering of digital works far less risky than it is today.

Over time, the anti-circumvention rules may perhaps be amended so that computer security and interoperability interests are better protected than they are now. Yet until that day comes, we should be grateful the triennial review process exists to provide a mechanism by which computing professionals, among others, can make the case for reverse engineering as a legitimate activity that serves the public interests in competition, ongoing innovation, and public health and safety.

---

Pamela Samuelson (pam@law.berkeley.edu) is the Richard M. Sherman Distinguished Professor of Law and Information at the University of California, Berkeley.

Copyright held by author.
Copyright of Communications of the ACM is the property of Association for Computing Machinery and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.