



DOI:10.1145/2879643

Pamela Samuelson

# Legally Speaking

## New Exemptions to Anti-Circumvention Rules

*Allowing some reverse engineering of technical measures for non-infringing purposes.*

**E**VERY THREE YEARS, the U.S. Copyright Office opens a new inquiry into whether the law that bars circumvention of technical protection measures (TPMs) used by copyright owners to protect access to their works are impeding lawful uses of the works. Those who propose exemptions to the anti-circumvention rules must offer substantial evidence that TPMs are thwarting lawful uses.

After examining this evidence, the Copyright Office recommends to the Librarian of Congress that he should grant certain specific exemptions for the ensuing three years. A new application will be necessary in the next rule-making cycle to extend the exemption beyond the three-year term.

My July 2015 *Communications Legally Speaking* column offered an overview of the exemptions being sought during the current triennial review. It also explained why I thought some would be granted, some would be narrowed, and some would be denied.

In late October 2015, the Librarian issued a motley set of exemptions

that largely bore out my predictions, although the exemptions granted were more numerous and generous to circumventors (that is, reverse engineers) than in previous triennial reviews.

After offering some general observations about the rule-making process, this column focuses on the anti-circumvention exemptions of greatest interest to computing professionals: those that enable unlocking of all-purpose mobile devices, those that allow jailbreaking that will enable owners of devices to run software that would otherwise not be available on their devices, and those that affect computer security testing.

### Three General Observations

First, the Office has now accepted two propositions that years ago might have been almost unthinkable: that, as critics of the anti-circumvention rules have been saying since 1998, TPMs impede many lawful activities and many circumventions of TPMs enable legitimate non-infringing acts.

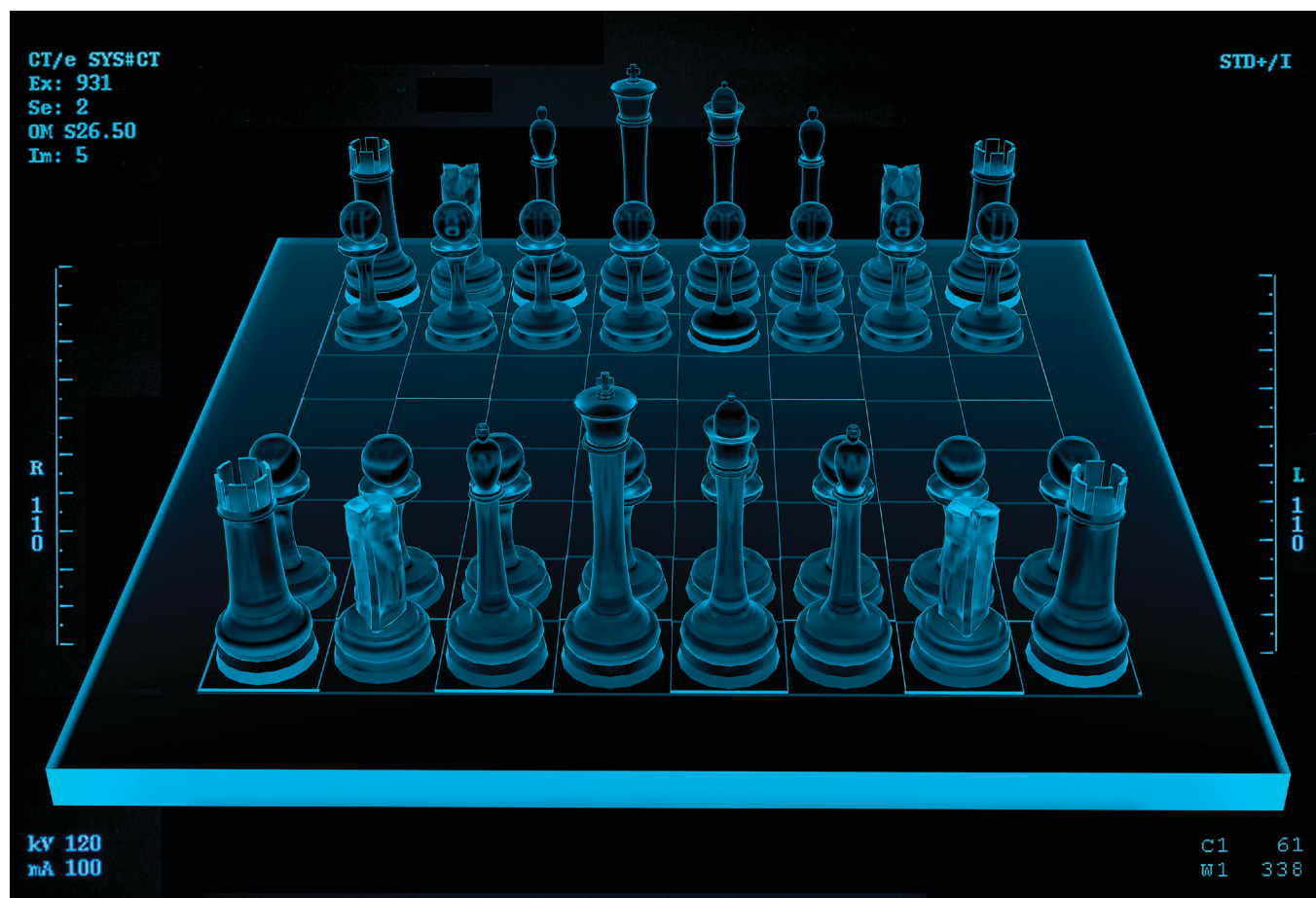
For each exemption granted, the Office had to admit the specific use to

be enabled was either fair use or otherwise privileged under U.S. copyright law. So the Office has developed an official record of lawful uses enabled by reverse engineering of TPMs. This is a step in the right direction.

Second, the Office has recognized the ubiquity of software embedded in a wide range of consumer products, such as automobiles and medical devices, means the anti-circumvention rules now arguably have implications far beyond the anti-piracy purposes that drove adoption of the rules back in 1998.

Yet, rather than saying, as perhaps it should have, the anti-circumvention rules have no application to, say, farmers who want to reverse engineer the software in their tractors to repair or modify them, the Office has implicitly accepted the anti-circumvention rules do apply to these acts. It has, however, provided an exemption that enables some reverse engineering of these vehicles.

Under the new exemption, farmers and other owners of motor vehicles can reverse engineer software to repair



or modify the vehicles themselves, but they cannot hire someone to do it for them. The Office insists new legislation would be required to enable third-party help to fix vehicle software. This substantially limits the utility of the granted exemption.

Third, the Office has suspended some granted exemptions—for reverse engineering of motor vehicles, medical devices, and some security testing—for 12 months to allow the U.S. Department of Transportation (DOT), the Environmental Protection Agency (EPA), and the Food and Drug Administration (FDA) to consider whether such reverse engineering should be permissible given health, safety, or environmental concerns raised by exemption opponents.

This suspension effectively deprives successful applicants of the benefits of the granted exemptions for a full third of their durations. It also subjects them to the risk that if they engage in the acts described in their applications during the first 12 months, they will open themselves to anti-circumvention liability, even though the Office accepted

the lawfulness of the uses in granting the exemption.

In addition, these reverse engineers will now be subject to new rounds of scrutiny by the DOT, EPA, and FDA. And if these agencies object, the anti-circumvention exemptions granted in 2015 may never go into effect.

### Unlocking and Jailbreaking Exemptions

Five sets of exemption requests focused on unlocking various types of information technology devices: cellphones, tablet computers, portable mobile connectivity devices, wearable wireless devices, and smart devices. These exemptions were sought to enable users to connect to their preferred wireless providers, to improve the resale value of the devices, and to avoid harm to the environment by encouraging disposal of devices rather than reuse of them.

In past rulemakings, exemptions permitted unlocking only with regard to cellphones. Congress instructed the Librarian to consider in this latest review process whether to include other devices as well.

The Office supported the first four requested exemptions because they enabled non-infringing uses of the devices TPMs were impeding. But the Office limited the scope of the exemptions to “used devices.” This means bypassing the TPMs to connect to a preferred wireless carrier is only exempt if the device had been lawfully acquired and activated to a network. This exemption did not extend to devices embedded in motor vehicles. The Office denied the smart devices exemption request on the ground it was too vague in its definition and scope.

Other exemption requests focused on “jailbreaking,” that is, bypassing TPMs to access operating system software for the purpose of enabling the owner of the device to install and execute software that could otherwise not be run on that OS. (Think of this as allowing users to get apps for their iPhones or iPads from a source other than the Apple App Store.) The exemption also allows removal of unwanted preinstalled software from the device.

The granted exemption was, however, not so broad as to enable jail-

breaking of dedicated devices, such as e-book readers or laptops. Yet, it did extend to all-purpose mobile devices, such as phones and tablets. Also granted was a similar exemption allowing the jailbreaking of smart TVs.

### Security Research

The Copyright Office is now on record that the anti-circumvention rules have had a chilling effect on good faith computer security testing. The existing statutory exemption for such testing is, the Office has recognized, unduly narrow. Especially in this day and age when cybersecurity risks are so evident, further breathing space for good faith security testing is much needed.

The Office was not, however, willing to support as broad an exemption for such testing as some computing professionals had sought. The Office pointed out that submissions in support of security testing exemptions focused on testing of consumer-facing products, such as motor vehicles, e-voting technologies, and software-enabled medical devices, not large-scale industrial or governmental systems. The exemption granted was tailored to allow testing of consumer-facing products.

As noted earlier in this column, this exemption was suspended for 12 months so other agencies concerned with these devices could consider what if any further limits should be imposed on security testing.

Yet, the suspension did not apply to e-voting technologies. The Office was persuaded there were no public safety issues posed by this exemption to justify a delay in its implementation. Given the upcoming U.S. presidential election, we should be glad that good faith security researchers will be free to investigate whether some malefactors are tampering with software that might throw that election.

The Office expressed concern that the security testing should be conducted in controlled environments designed to ensure individuals and the public will not be harmed. The FDA insisted on a limitation to the medical device exemption to exclude systems that were being used or could be used by patients. The Office also limited the exemption for circumventing TPMs to get access to patient data being collected by the software.

## Most applicants for exemptions got something for their troubles, even if not as extensive an exemption as requested.

### Other Exemptions

Very few of the proposed anti-circumvention exemptions were rejected outright, although some were. As predicted in my July 2015 *Communications* column, the proposed exemption to allow backup copying and format shifting of DVD movies fell flat. But most applicants for exemptions got something for their troubles, even if not as extensive an exemption as requested.

As for bypassing TPMs for noncommercial, documentary, or nonprofit educational purposes, for instance, the Office is now willing to say that certain bypassing of TPMs protecting Blu-ray discs and online streaming services, as well as DVDs, should be exempt.

But the Authors Alliance plea for a broad multimedia e-book exemption was denied. Film studies professors are the main beneficiaries of the new exemption. So I, as a law professor, run the risk of anti-circumvention liability if, for example, I make an e-book with clips from movies portraying different versions of James Bond so my students can consider whether Bond should be a copyright-protectable character.

Other granted exemptions included one to allow bypassing TPMs to develop assistive technologies for print-disabled persons to provide access to contents of literary works distributed electronically and another to provide a narrow privilege to provide alternative feedstock for 3D printing.

Also exempt is bypassing TPMs by libraries, museums, and archives to preserve video games when the games'


developers have ceased to provide necessary remote server support. The Office even recognized the legitimacy of a user's interest in being able to continue playing videogames for which outside support had been discontinued.

### Conclusion

This synopsis of the 2015 anti-circumvention rule is no substitute for reading the original. The final rule, along with submissions in support of and opposition to exemptions during the triennial review and other relevant materials, can be found at <http://copyright.gov/1201>.

Be forewarned, though, that the final rule is a dense 21 pages long, and like the Copyright Act of 1976, it is not exactly an easy read. For those computing professionals who engage in reverse engineering that involves some bypassing of TPMs for non-infringing purposes, the rule contains mostly good news. Yet, a close read (and possibly some legal advice) may be needed before computing professionals can feel completely safe relying on a granted exemption.

Yet to be addressed in the case law or the policy arena is how strict the courts will or should be in reading the exemptions recently granted. Under a strict reading, only those who have applied for and been granted explicit exemptions are relieved from circumvention liability. Any straying beyond the prescribed borders of the exemptions, even to engage in similar non-infringing activities, may seem dangerous.

However, there is some case law to suggest bypassing TPMs for non-infringing purposes does not violate the anti-circumvention rules, even if there is no applicable exemption. Moreover, lawsuits against non-infringing reverse engineers seem unlikely because courts will be unsympathetic to claims that merely bypassing a TPM to engage in legitimate activities is illegal. Still, the risk averse may understandably be unwilling to offer themselves up to be the test case for this proposition. 

Pamela Samuelson ([pam@law.berkeley.edu](mailto: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.