Opinion on Digital Restrictions Management

Technological measures to defeat users' rights, and the response to those measures embodied in Draft 1, have been a particularly active subject of discussion and debate in the first round of public deliberation.

These measures — often described by such Orwellian phrases as "digital rights management," which actually means limitation or outright destruction of users' legal rights, or "trusted computing," which actually means selling people computers they cannot trust — are alike in one basic respect. They all employ technical means to turn the system of copyright law, where the powers of the copyright holder are limited exceptions to general freedom, into a prison, where everything not specifically permitted is utterly forbidden, and indeed, if the full extent of their ambition is realized, would be technically impossible. This system of "para-copyright" has been created since the adoption of GPLv2, through legislation in the United States, the European Union, and elsewhere that makes it a serious civil or even criminal offense to escape from these restrictions, even where the purpose in doing so is to restore the users' legal rights that the technology wrongfully prevents them from exercising.

As a digital rights organization, we would not be following our mission if we did not oppose these injustices. But the reason our license must respond to these practices at all is the result of a remarkable irony. Those who wish to impose DRM on the public would like to do so by using software covered by the GPL, a license that is intended to preserve the very freedom that they seek to crush. They are not satisfied merely with publishing programs having limited capability, which free software permits. They seek to go further, to prevent the user from removing those limits, turning Freedom 1, the freedom to modify, into a sham.

GPLv2 did not address the use of technical measures to take back the rights that the GPL granted, because such measures did not exist in 1991, and would have been irrelevant to the forms in which software was then delivered to users. But GPLv3 must address these issues: free software is ever more widely embedded in devices that impose technical limitations on the user's freedom to change it.

These unjust measures must not be confused with legitimate applications that give users control, as by enabling them to choose higher levels of system or data security within their networks, or by allowing them to protect the security of their communications using keys they can generate or copy to other devices for sending or receiving messages. These technologies present no obstacles to the freedom of free software. The user is presented with choices, and figuratively as well as literally retains all the keys to the digital home.

By contrast, technical restrictions that allow other parties to control the user have no legitimate social purpose. In existing applications where the user is not afforded the same degree of real power to modify the free software in his system that vendors or distributors have retained, or have conveyed to third parties, the software has been delivered in a fashion that violates the spirit of the GPL, regardless of whether it complies with the letter of the license. The freedoms the GPL grants have actually been withdrawn by technical means. It may even be a crime for the user to modify that free software to escape from those restrictions and regain control over what is still, at least nominally, his own system.

To highlight the essential issue of preserving Freedom 1 as a real, practical freedom, we have rewritten the relevant sections of the license. In section 1, we have tried to limit as precisely as possible the situation in which an encryption or signing key is part of the Corresponding Source Code of a GPL'd work. Where someone is provided a GPL'd work, he must receive the whole of the power to use and modify the work that was available to preceding licensors whose permissions he automatically receives. If a key would be necessary to install a fully functional version of the GPL'd work from source code, the user who receives the binary must receive the key along with the source. The requirement of full functionality, which we have illustrated with examples, is no more optional than it would be if GPL'd software were redistributed with an additional license condition, rather than a technical limitation, on the uses to which modified versions could be put.[1]

In section 3, which has been retitled as well as redrafted, we have specifically stated the rule, previously implicit, that modes of distribution that establish limitations on use or modification that are inconsistent with the terms of the license are not permitted by the license. In addition, we have added disclaimers, based on advice of counsel from nations that have enacted para-copyright provisions akin to the Digital Millennium Copyright Act in the US or pursuant to the European Union Copyright Directive. We believe these disclaimers by each licensor of any intention to use GPL'd software

[1] There is a clear distinction between this situation and the situation of authenticated modules or plug-ins distributed as part of a multi-component software system, so that instances of the software can verify for the user the integrity of the collection. So long as the decision about whether to run a modified version is the user's decision, not controlled by a preceding licensor or a third party, the vendor's authentication key would also not qualify as part of the Corresponding Source under the language we have adopted for Draft 2.

to stringently control access to other copyrighted works should practically prevent any private or public parties from invoking DMCA-like laws against users who escape technical restriction measures implemented by GPL'd software.

We believe that these provisions, taken together, are a minimalist set of terms sufficient to protect the free software community against the threat of invasive para-copyright.