Nine Ways to Protect Your State From the Legal Risks Posed by the Use of Open Source Software

Linda M. Hamel, General Counsel,
Information Technology Division,
Commonwealth of Massachusetts
(617)-626-4404
September 17, 2004
The opinions expressed in this article are those of the author alone and do not represent the position of the Romney Administration or constitute an endorsement of any of the products or services referred to herein.

EXECUTIVE SUMMARY

The legal risks posed to states by the use of open source software must be considered in light of the risks posed by the use of proprietary software. States that use open source software face fewer legal risks than their private sector counterparts. The legal risks posed to states by the use of open source software can be managed.

The specific legal risks posed by open source software to states include:

1. Uncertainty surrounding the new terms in such licenses
2. No warranties regarding title, or indemnification against third party intellectual property infringement claims
3. No warranty regarding performance, media or malicious code
4. Automatic revocation and lack of user familiarity with terms
5. Indemnification of prior contributors

States can minimize the legal risks of using open source software by:

1. Adopting and enforcing an open source risk management policy
2. Identifying and tracking all open source code that is used by the State
3. Having legal counsel review all licenses for new and existing open source software and explain them to their agency clients
4. When developing a large system, have legal counsel review all licenses for open source software that agencies propose to use and counsel the agency as to the impact of the lack of warranty and indemnification provisions
5. Requiring legal review prior to distributing code outside of the state enterprise
6. Keeping track of modifications
7. Balancing the Need for Access to the Code with the Need to Limit Source Code Access to Those Who Need It to Perform Their Jobs
8. Considering market based models for shifting risk and
9. Documenting all software projects

1. **Introduction**

Open source software licenses, unlike most proprietary licenses, transfer the software's source code to the licensee and enable the licensee, subject to certain restrictions, to modify and distribute it [1] . The increased use of open source software by state governments offers many advantages. For some of state government's software needs, open source software provides a more cost effective and higher performing alternative to the use of proprietary software.

The widespread use of open source software poses some legal risks for state government. It is important not to overemphasize those risks, because the alternative, use of proprietary software, is hardly risk-free. Worldwide, private and public sector entities that have increased their use of open source software have determined that the benefits of using it exceed its legal risks. Moreover, some of the legal risks posed by the use of open source licenses impact states, compared to private entities, only minimally. At the same time, states should not ignore these risks, which can expose them to financial loss. The purpose of this paper is to outline the legal risks faced by states in connection with their increased use of open source software, and identify best practices associated with the management of those risks. This paper does not address the other technology and business risks, such as reliability and security, that may be faced by state governments using open source or proprietary software.

[1] A wide range of open source licenses is currently in use. For a practical breakdown of the rules embedded in over thirty such licenses, see the Commonwealth of Massachusetts "Open Source Legal Toolkit". Click on "Open Source Licenses Quick Reference" for a chart outlining and comparing such licenses, and "Guide to Quick Reference Chart" for an explanation of the headings

2. Proprietary Software Legal Risks

The use of any software under a license, whether proprietary or open source, poses legal risks to the licensee. The legal risks of open source software must be considered in light of the legal risks incurred by the users of proprietary software.

Users of any software, whether it is licensed under a proprietary or open source license, are at risk of violating the intellectual property rights of a third party. Proprietary software licenses reduce, but do not eliminate, the financial risk posed to licensees by potential third party intellectual property infringement claims, through the use of warranties of title and indemnification clauses. Such provisions can provide significant protection against third party liability claims when their terms are sufficiently broad and they are issued by established, financially solid licensors.

However, warranties of title and promises of indemnification are not guarantees that the licensee will suffer no loss as a result of third party claims. Some indemnification clauses are so narrowly worded that the protection they afford licensees is minimal. In addition, due to fluctuations in the market for software, some software licensors will be out of business by the time indemnification is sought by a licensee . Furthermore, mere financial indemnification from the licensor cannot eliminate the cost to the licensee of personnel time and system downtime that may occur during the pendency of litigation associated with the third party claim. Beyond indemnification for damages and attorneys fees related to third party intellectual property infringement claims, most proprietary software licenses strictly limit the licensee's remedy, should third party infringement be determined, so that the licensee cannot recover from the software vendor other costs that it incurs in connection with such claims.

Preexisting software (software not developed for the licensee) is a "good" under Article 2 of the UCC. **See USM Corp. v. Arthur D. Little Systems. Inc.**, 28 Mass. App. Court 108, 119 (1989)(turnkey system involving both hardware and software a "good" under UCC Article 2); **Olcott International Co., Inc. v. Microdatabase**, 793 N.E. 2d 1093 (Ind. 2003) (generally available standard software is a good under Article II of the UCC). But the warranties of merchantability and fitness provided to "buyers" of goods under the UCC are almost always explicitly and effectively disclaimed in proprietary software licenses. While some proprietary software licenses provide warranties regarding the software's performance, the media on which the software is provided, and the absence of malicious code, such warranties are almost always extremely limited in scope and duration.

Finally, a software license is a contract between licensor and licensee, and licensees who fail to comply with proprietary license terms are always exposed to breach of contract claims.

3. Open Source Software Legal Risks

At a minimum, the following legal risks are presented by the use of open source software:

a. **Uncertainty surrounding the new terms of open source software licenses**

While the legal significance of standard proprietary software license terms has been extensively litigated and interpreted by the courts on many occasions, there has been insufficient litigation surrounding the meaning of the new legal terms included in open source licenses to develop a "common law" of open source licensing, a judicial gloss on commonly used open source license terms. Novel terms that appear in open source licenses create risks for licensees because they have no settled legal interpretation. Among the new terms that have not been interpreted by the courts are the allegedly "viral" provisions of the GPL, under which the GPL asserts that it applies, in some circumstances, to certain software programs that incorporate GPL code.

Significantly, the uncertainty surrounding this particular provision in the GPL is an example of a legal risk that poses

far less of a problem for states than it does for private sector licensees. States, unlike their private sector counterparts, are far less likely to be in the business of commercializing code based on the GPL. While a private sector software company may be concerned about whether an entire software program that it develops around a kernel of GPL code is in its entirety subject to the GPL, which would limit its commercial potential, state agencies, which are not typically commercial sellers of code, will have no such concerns [1] .

[1] State institutions of higher education that commercialize software that they have developed might, however, have the same concerns as a commercial firm.

b. **No Warranties Regarding Title, or Indemnification Against Third Party Intellectual Property Infringement Claims**

Unlike proprietary software licenses, most open source software licenses offer the licensee neither warranties regarding the licensor's title nor indemnification for third party intellectual property violations [1]. A user of open source code is therefore exposed to a higher risk of paying costs, attorney's fees and damages as a result of claims that the software infringes third party intellectual property rights.

In **SCO Group v. International Business Machines Group**, 2:03CV00294 DAK, (D. Utah 2003), SCO sued IBM for billions in damages, claiming that IBM, through its support and development of Linux, had breached contracts IBM entered into with SCO's predecessors in Unix ownership regarding non-disclosure of Unix code. Specifically, SCO claimed that IBM has introduced Unix code into Linux. SCO has brought related claims against two users of IBM's version of Linux in **SCO v. AutoZone**, and **SCO v. DaimlerChrysler**. These pending cases have received worldwide attention because they raise the specter of other putative code owners suing distributors and users of open source software for third party intellectual property infringement.

The risks faced by a state in connection with third party intellectual property infringement claims are substantially less than the risks faced by a private party. The U.S. Supreme Court has ruled that states cannot be held liable for damages under U.S. intellectual property law.[2] See **Florida Prepaid Postsecondary Education Expense Board v. College Savings Ban**, 119 S. Ct. 2199 (1999). After Florida Prepaid, states are still subject, at least in theory, to being enjoined under Federal law from using infringing code, and for money damages for patent violation based on claims brought in state court for torts like conversion of personal property, as well as claims based on "taking", reverse condemnation, or trade secret violations. However, it appears highly unlikely that a court would exercise its equitable powers, given the balance of the harms, to halt a states' use of infringing software embedded in a mission critical system in the context of an infringement action. Any harm suffered by the putative owner of the code would appear to be dwarfed by the harm suffered by citizens temporarily unable to register for food stamps online or receive emergency information through the state's website because these systems were shut down on the grounds that they relied on infringing software. Similarly it will be difficult for intellectual property owners to prevail against states by bringing state law claims. A state court sitting on such a claim would be hampered by its unfamiliarity with the complex intellectual property issues that have traditionally been handled in Federal court and reluctant to stretch state law to encompass third party infringement claims.

In theory, a state could waive its sovereign immunity against being sued for intellectual property infringement claims, and thus subject itself to money damages under U.S. patent, copyright and trademark law [3]. State CIOs should consult their legal counsel to determine whether their state has waived its right to be sued for intellectual property infringement, and assess their risk of being subject to claims for monetary damage for infringement of third party intellectual property rights accordingly.

*[1] Some open source licenses may include warranty and indemnification terms. For instance, the Mozilla Public License 1.1 permits licensees to offer downstream licensees warranties, indemnification, support and liability provisions, but only if they indemnify upstream contributors against any fallout from such commitments. **See**, Mozilla Public License 1.1 The GPL, the most commonly used open source license, does not permit licensees to redistribute the code with such terms. See the General Public License.*

*[2] More accurately, **Florida Prepaid** makes it practically impossible for states to be held liable for damages under U.S. intellectual property law. In Florida Prepaid, the court stuck down the Patent and Plant Variety Remedy Clarification Act, through which Congress had attempted to abrogate the sovereign immunity of states with respect to patent infringement claims. The Court held that Congress did not have the authority to abrogate states' Eleventh Amendment immunity under the powers given the legislative branch under Article I of the Constitution. While acknowledging that Congress did have the authority to abrogate the states' sovereign immunity under the due process clause of the 14th amendment, it found that it could not do so in the case of the Act at issue because Congress had failed to find that the states had either engaged in a pattern of infringement or failed to provide victims of infringement with suitable state law remedies. Although Florida Prepaid dealt only with patent claims, the court's decision in a related case **College Savings Bank v. Florida Prepaid Postsecondary Board of Education Expense Board**, 527 U.S. 666 (1999), and an earlier lower court case regarding copyright infringement, **University of Houston v. Chavez**, 517 U.S. 1184 (1996), indicate that Florida Prepaid applies to all Federally protected intellectual property law.*

[3] The Massachusetts Tort Claims Act waives the Commonwealth's immunity against suit only with respect to torts. See Mass. Gen. L. ch. 258 s. 1 et seq. Thus Massachusetts has not waived its sovereign immunity with respect to liability for money damages under U.S. patent, copyright and trademark law.

c. **No Warranties Regarding Performance, Media or Malicious Code**
Most open source software licenses also offer no warranties regarding the software's performance, the media on which the code is provided, or the presence of malicious code. Most such licenses, like their proprietary counterparts, also disclaim the UCC warranties of merchantability and fitness. Thus even the minimal warranties that appear in proprietary licenses, and the financial backing of the firms that stand behind them, are not available to licensees using open source software.

d. **Automatic Revocation and Lack of User Familiarity with Terms**
Proprietary software license terms have become so standardized that information technologists are familiar with the most important rules surrounding proprietary software use---no reverse engineering, no modification or enhancement, no distribution to non-licensees, etc. By comparison, open source licenses present new legal terms with which even experienced software licensing lawyers, let alone their technologist clients, may not be familiar. There are a wide variety of open source licenses, each of which has its own terms. Unlike the typical proprietary End User License Agreement (EULA) in which terms are likely to be similar from one software product to the next, there is significant variation between the terms of open source licenses; a user who is familiar with the terms of the GPL should not assume that they are identical to those of the Apache or BSD licenses.

Failure to comply with the terms of open source licenses can result, at least in theory, in automatic revocation of the license. For instance, the GPL, like most open source licenses requires that, if the licensee distributes modifications or enhancements to the code, the GPL must be applied to those modifications and enhancements. The licensee's failure, when distributing such modifications and enhancements, to license the new code under the GPL may automatically revoke the original GPL license to use the original code. Failure to carefully read and comply with the specific open source license that accompanies open source code can expose organizations to the legal risk that their use of open source code is "off license" and therefore in violation of US intellectual property law or state trade secret law. More importantly, license violation can result in a breach of contract claim, against which no state is immune.

e. **Indemnification of Prior Contributors**
Some open source licenses require that, under certain circumstances, the licensee indemnify upstream contributors to the code. **See** n. 3, herein. States that, like the Commonwealth of Massachusetts, are constitutionally or statutorily prohibited from indemnifying parties with whom they contract must carefully monitor the circumstances under which open source code is distributed so that such indemnification provisions are not triggered.

4. Managing the Legal Risks Posed by Open Source Software

Although the legal risks of using open source software cannot be eliminated, they can be reduced through the adoption of the risk management policies and procedures outlined below. Measures taken to mitigate legal risk are also part of good software asset management and serve to mitigate business risks as well. Many organizations have instituted an open source review board, an interdisciplinary group composed of business, technical and legal staff. The function of these boards is to review and approve the acquisition of open source software by the organization as well as the dissemination of open source developed or modified by the organization. The risk management procedures listed below can be incorporated into the review process utilized by such a board.

a. **Adopt an Open Source Risk Management Policy**
The state's central IT organization should adopt an open source risk management policy, addressing the topics discussed in the items below. The policy should apply to all agency employees, contractors and agents. Like any other policy, the open source policy will be not as effective unless audited and enforced.

b. **As part of your IT asset management program, identify and track in an accessible electronic inventory all open source code that is used by the State**
Identify and track all open source code used by your state, and the licenses under which it is used, including open source code that is embedded in proprietary products. Use of an accessible online electronic application will enhance agency compliance with this requirement and can also serve as a repository for the code and licenses, facilitating re-use and enhancement by other state entities.

An additional benefit of inventorying open source code, aside from risk management, is that agencies will have a source of information about the experience of other agencies in using particular open source programs. More importantly, possession of a complete inventory simplifies the task of updating software to include recent bug fixes, including security patches, and new software releases.

The inventory should also identify the source from which the agency obtained the code. The risks of obtaining code from an open source community website are, in some cases, different than the risks of obtaining code from a vendor. Finally, the inventory should document software versions and modifications.

c. **Have Legal Counsel Review All Licenses for New and Existing Open Source Software and Explain Them to their Agency Clients**

Legal counsel should review all open source licenses for open source software currently being used by your state, and for new open source software that agencies are considering acquiring, and explain their meaning to their agency clients. Technologists are so familiar with boilerplate proprietary license terms that they rightly tend to focus on the variable provisions of such licenses, such as the number of licenses, rather than on the familiar legal terms. They and other software users need to be educated about the unfamiliar terms that appear in open source licenses, preferably before the software is downloaded and utilized.

d. **When Developing A Large System, Have Legal Counsel Review all Licenses for Open Source Software that the Agency Proposes to Use, and Counsel the Agency as to the Impact of the Lack of Warranty and Indemnification Provisions**
When agencies are developing large, mission critical systems, and plan to incorporate open source software, in addition to assessing business and technical risks, they need to consider the risks posed by the lack of warranty and indemnification provisions in open source licenses. The more critical the application to the mission of the agency, the greater the importance of having a deep pocket to turn to if the software is defective.

The mechanism by which the software is selected should also be reviewed by counsel. If the agency itself chose the open source software without consultation with the vendor performing the development, the vendor may have little or no liability if the system fails. If the vendor performing the development played a major role in selecting the open source software, the selection process should be well documented and the vendor is a potential source of backup if system failure can be tracked to a careless choice of open source software.

Counsel should review all open source licenses for software that will be involved in the project, ask whether the vendor recommended the use of such software, and consult with their agency clients regarding the impact of the open source license's terms on the project's vendor-state risk-shifting profile.

e. **Legal Review Prior to Distribution Outside the State Enterprise**
Prior to distributing open source code outside the state government, agencies should consult with legal counsel to ensure that the proper license is affixed to the code, that the conditions imposed on distribution have been met, and that the distribution will not expose the state to indemnification risk.

f. **Keep Track of Modifications and Enhancements**
Agencies should keep a record of modifications and enhancements to the open source code that they use. Modifications and enhancements should be documented in the state's open source inventory in a timely manner.

g. **Balance the Need for Access to the Code with the Need to Limit Source Code Access to Those Who Need It to Perform Their Jobs**
Agencies could minimize their legal risks by limiting source code access to those who need it to perform their jobs, and keeping a record of such access. It is true that, the more individuals who have access to the source code, and therefore the opportunity to violate the license by failing to comply with its terms regarding software development and distribution, the greater the risk of using open source software. Yet states need to minimize these legal risks against the need for each state to cultivate a community of talented individuals who take ownership of the modification and improvement of the code. Each state must strike a balance between minimizing the legal risks associated with access to code within their own organization and maximizing the utility of creating their own open code community.

h. **Consider Market Based Models for Shifting Legal Risks.**
The marketplace has responded to the new legal risks posed by the use of open source software by the emergence of vendors who provide, for a fee, insurance, indemnification, and/or code replacement agreements as a means of managing the risk of intellectual property infringement and other legal risks posed by the use of open source software. Often, these entities also provide for a fee professional services and support. These entities include Red Hat, Novell, HP, Sun, and Open Source Risk Management. Many such services are offered only in connection with Linux. In some cases, states should consider whether, for a particular system, shifting the legal risks inherent in open source use to this type of entity makes sense for them. States should keep in mind, however, that because their risk of suffering financial loss as a result of third party intellectual property infringement litigation is significantly less than that of private sector licensees, their return on investment for using market-based services solely for the purpose of reducing exposure to third party intellectual property claims is minimal.

i. **Document All Software Development Projects**
States should ensure that all software development projects funded by them are documented to capture information about the use of open source and proprietary code and the licenses under which such code is used; the names of all individuals who contributed to the project; and their signed work for hire agreements. Otherwise, it will be difficult to acquire the information necessary to maintain an up to date enterprise wide inventory of open source software.

5. Conclusion

Use of either open source or proprietary software poses some legal risk to states. States face fewer risks in connection with the use of open source software compared to their private sector counterparts, and the risks that they do face can be managed.

Did you find the information you were looking for on this page? *

- Yes
- No

Send Feedback