FOLEY

FOLEY & LARDNER LLP

Understanding Open Source Software: Risks and Rewards

Presented By:

Michael R. Overly, Esq., CISSP, CIPP, CISA, ISSMP, COP, CRISC



Agenda

- Two perspectives
- Nomenclature
- Where did “Open Source” come from
- Types of licenses
- Impossible to avoid
- Benefits
- Challenges/Risks
- Documenting Risk
- Vendor engagements

© 2023 Foley & Lardner LLP

Two Perspectives

- Customer/consumer of open source
  - Every business is a customer/consumer
  - Received either as a standalone open source or included as part of a commercial product/service
- Distributor/vendor of open source
  - Original developer and distributor/vendor
  - As recipient of open source from others and then redistributed either alone or as part of recipient products/services

© 2023 Foley & Lardner LLP

Nomenclature

- Source code
- Object code
- Library or function calls (LGPL v. GPL)
- Linking
  - Static – Essentially one, combined executable
  - Dynamic – Proprietary and open source separately compiled at execution/run time
- Derivative Work
- Viral v. Non-viral licenses

© 2023 Foley & Lardner LLP

A Printer Jam Changes the World

By most accounts, the birth of the open source/free software movement can be traced to a printer jam in 1983. Richard Stallman wanted to patch his printer software to fix the problem. To do that, he needed access to the source code, but Xerox considered the source code proprietary and declined to disclose it. Stallman quit his job and set about developing software and licensing scheme to ensure his software was always “free.” The rest is history . . . .

© 2023 Foley & Lardner LLP

Open Source Software

- What is “Open Source”
  - Software that is distributed with the source code under a license that promotes continued development
- Types of licenses: GNU General Public License, Apache License, Mozilla, BSD, and many others
- Where does open source come from
  - Online projects like SourceForge.net, Bitbucket, GitHub, etc.

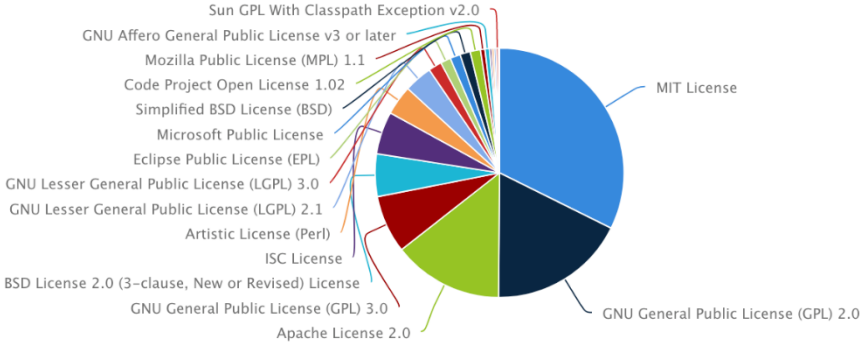
© 2023 Foley & Lardner LLP

Open Source Software

- It takes a village . . . .
- One or more developers creates a new application, a “project” and posts online
- Others contribute, provide bug-fixes, etc.
- Contributors can be anywhere in the world
  - Many laws can apply
- Contributors may, and likely do, work for others
  - Employment agreements

© 2023 Foley & Lardner LLP

The World of Open Source



Source: Black Duck KnowledgeBase

© 2023 Foley & Lardner LLP

A Few Notes of Interest

- GPL v2 versus v3
  - Distribution clarified
  - Hosted/cloud environments
- GNU Affero General Public License V3
  - Cloud Kills
- Civil disobedience - Protest licenses (Higher risk of infringement?)

© 2023 Foley & Lardner LLP

Impossible to Avoid Open Source

- Found in almost every commercial application
- Interoperability may require it
- OMB: Federal Source Code Policy requires agencies to release at least 20% of new custom-developed software as Open Source each year.

© 2023 Foley & Lardner LLP

Benefits of Open Source

- Free (or not?) – Pricing models
- Access to source code
- No need to rely on a single vendor
- Many-eyes theory
- Organic growth

© 2023 Foley & Lardner LLP

Overview of Challenges

- Two Major Considerations
  - Viral v. Non-Viral Licenses
    - Many grey areas
  - No standard contractual protections
    - You are on your own
    - No warranties, no indemnities, etc.

© 2023 Foley & Lardner LLP

Challenges of Open Source Licenses

- Open source licenses not yet fully tested by courts.
  - Small handful of cases refer to “open source” and the interpretation of open source licenses.
  - Germany is the hotbed
- Many licenses written years ago, many without legal input.
- Some open source licenses have “holes” in them (e.g., GPL v2 liability disclaimer)

© 2023 Foley & Lardner LLP

Challenges of Open Source Licenses

- **No clear legal standard for derivative works**: Current law offers no clear definition of what constitutes a "derivative work" for software. Various circuits employ several different, conflicting rules. The determination of whether something constitutes a derivative work can depend in large part on which rule is applied.

© 2023 Foley & Lardner LLP

Challenges of Open Source Licenses

- Conflicting interpretations within the Open Source community
- Software Freedom Law Center
- Even within the FSF there is disagreement and confusion about what constitutes a derivative work.

© 2023 Foley & Lardner LLP

[I]t is telling how widely their responses diverge – there appear to be *no definitive answers* to the question of what constitutes a derivative work under the FPL, not even from the holders of the licenses in question.

Asay, Matt, "A Funny Thing Happened on the Way to the Market: Linux, the General Public License, and a New Model for Software Innovation" (April 2002) (emphasis added); www.linuxdevices.com/files/misc/asay-paper.pdf.

© 2023 Foley & Lardner LLP

Unknown Pedigree

- While not perfect, commercial developers generally have processes and procedures in place to ensure “clean” development
- The challenge of the community development process
  - No process or procedures for “clean” development
  - In many instances, no contract with individual developers

© 2023 Foley & Lardner LLP

Unknown Pedigree (cont'd.)

- Can individual developers legally make contributions?
  - What about existing obligations to their employers?
  - Where did they get their ideas, programming, and tools from?
  - What about foreign developers?
- Software foundries – The Wild West. Most common method for Open Source development

© 2023 Foley & Lardner LLP

Security Considerations

- Security implications are frequently overlooked
- False sense of security from possession of source code
- Possibility of viruses, back-doors, and other security flaws

© 2023 Foley & Lardner LLP

Security Considerations

- Orphaned Code presents substantial risk (Commonwealth of Massachusetts v. Equifax, failure to patch)
- Many “eyes” theory; successfully used for years in evaluating and testing encryption algorithms

© 2023 Foley & Lardner LLP

Intellectual Property Ownership

- Open Source Threats to Intellectual Property – **Three key areas**:
  - The Open Source Virus:
    - Directly modifying the open source and redistributing
    - Combining the open source with proprietary code
  - Making controlled (frequently uncontrolled) contributions to open source projects – regardless of whether a viral license is present.

© 2023 Foley & Lardner LLP

Considerations for Distributors/Vendors of Open Source

© 2023 Foley & Lardner LLP

Redistributors/Vendors of Products Containing Open Source

- Keep the development environment clean
- Conduct periodic audits
- Hold development personnel accountable
- Fulfill open source license obligations
  - Notice to end customer
  - Availability of source
- Address accountability for open source

© 2023 Foley & Lardner LLP

Documenting Risk

- Each use of open source software requires individual review
  - What is being licensed?
  - How will the software be used?
  - Will the software be combined with other software?
  - Will the software be modified?
  - Will we distribute the software to others?
  - Will the use change over time?

© 2023 Foley & Lardner LLP

Documenting Risk, cont'd

- Use of developer questionnaire or checklists
- Importance of developer responsibility: putting corporate IP at risk, creating potential liability
- Use of these forms has become standard in the industry
- Ensures proper documentation of all uses and accountability

© 2023 Foley & Lardner LLP

Documenting Risk, cont'd

- Getting control over open source use
- Use a questionnaire or other means of documenting each introduction of open source into your environment
- What are Black Duck, Synopsys, and other services?
- Acquisitions – Due Diligence

© 2023 Foley & Lardner LLP

Bright Line Rules for Risk Assessment

- A “yes” to any of these questions requires escalation:
  - Are we modifying the open source and distributing it?
  - Are we statically linking any viral open source with proprietary code?
  - Is the open source no longer actively supported (i.e., no orphan code)?
  - Is the open source governed by a non-standard license?
  - Will you be making any contributions to the open source project from which the software was obtained?

© 2023 Foley & Lardner LLP

Use of Approved License Lists

- What are approved license or green light lists?
- Generally, only identify viral v. non-viral licenses
- Actually, three categories
  - Viral
  - Non-Viral
  - Non-standard
- Viral license identification is not the only risk

© 2023 Foley & Lardner LLP

Use of Approved License Lists, cont'd

- Even if a license is non-viral, there are still risks that must be assessed, mitigated, or accepted
  - Software bugs
  - Support obligations
  - Infringement claims
  - Orphaned code and other security vulnerabilities
  - Risk of having to pull the open source from production

© 2023 Foley & Lardner LLP

Identifying the License

- Frequently confusing
- Developers must be certain they have identified the relevant license
- When in doubt . . . .
- What about dual licenses? Generally one viral and one non-viral
  - How to document.
- Developer may change the license – Beware software updates.

© 2023 Foley & Lardner LLP

Possible to Avoid a Viral License?

- First stop: Dual licensing
- Second stop: Contact the developer
- Third stop: Explore commercial alternatives
- Last stop: Mitigate, but no silver bullet
  - Isolate open source
  - Dynamic linking
  - Leasing hardware

© 2023 Foley & Lardner LLP

How to Give Notice

- Easiest way to a demand letter or lawsuit
- FSF resource – A Practical Guide to GPL Compliance
- Provide reasonable notice to the end customer
  - License.txt
  - URL
  - Attachment to license or other terms

© 2023 Foley & Lardner LLP

Example Disclaimer for EULA

Third Party Software. To the extent any software licensed from third parties, including open source software, (collectively, "Third Party Software") is provided with the Licensed Software, you agree to comply with the terms and conditions of the applicable third party licenses associated with the Third Party Software, in addition to the terms and restrictions contained in this Agreement. All relevant licenses for the Third Party Software are provided at www._____.com. Your use of the Licensed Software shall be deemed your acceptance of the third party licenses.

© 2023 Foley & Lardner LLP

Example Disclaimer for EULA

[** Optional sentence: “Licensor shall support the Third Party Software to the same extent as the Licensed Software.” **]LICENSOR MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS OR IMPLIED, WITH REGARD TO ANY THIRD PARTY SOFTWARE. ALL THIRD PARTY SOFTWARE IS PROVIDED "AS-IS," WITHOUT WARRANTIES OF ANY KIND BY LICENSOR. IN NO EVENT WILL LICENSOR BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DIRECT, INDIRECT, PUNITIVE, EXEMPLARY, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE THIRD PARTY SOFTWARE, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES.

© 2023 Foley & Lardner LLP

Customer/consumer of open source

© 2023 Foley & Lardner LLP

Vendor Contractual Protections for Open Source Software

- Types of contracts creating concern:
  - Development agreements
  - OEM agreements
  - Commercial software license agreements/Cloud/SaaS
- Two categories of risk:
  - Liability/performance
  - Threat to company IP
- IP Threat frequently **irrelevant**

© 2023 Foley & Lardner LLP

Vendor Contractual Protections for Open Source Software

- Initial approach is to require a warranty of no open source software
  - This approach frequently results in the vendor identifying one or more open source components
- If open source is present, will the vendor be responsible for the performance of the open source components? If not, are the components a substantial portion of what is being licensed?

© 2023 Foley & Lardner LLP

Identifying Issues - Vendors

- If Open Source is present, require the following:
  - Specific identification of all components
  - Copies of all licenses
  - Warranty that licensor has right to distribute
  - Open Source will be treated as “Licensed Software” for all purposes: IP indemnity, warranties, and support
  - Contractual “out” for changes in licenses

© 2023 Foley & Lardner LLP

Example Vendor Warranty #1

Third Party Software. In the event Licensor provides any third party software, including open source software, (the "Third Party Software") to Customer in connection with this Agreement, the following shall apply: (i) all such Third Party Software shall be included in the definition of "Software" and subject to all warranties, indemnities, and other requirements of the Agreement relating to the Software; and (ii) except for third party terms and conditions expressly identified (i.e., references to terms that may be viewed through a web site or provided as part of the installation files are not sufficient) in the applicable order document for the Software or in the Agreement, Customer shall not be bound by any such terms and conditions.

© 2023 Foley & Lardner LLP

Example Vendor Warranty #2

Third Party Intellectual Property Rights. In the event Company provides any third party intellectual property (the "Third Party Intellectual Property"), including Open Source Software, to Customer in connection with this Agreement for which Customer would be obligated to accept and be bound by any third party terms and conditions, the following shall apply: (1) Company shall specifically identify in writing all Third Party Intellectual Property in the applicable Order; (2) Company shall attach to the applicable Order written copies of all third party license agreements applicable to Customer; and (3) Company warrants that (i) it has the right to license any Third Party Intellectual Property licensed to Customer under this Agreement; (ii) to the best of Company's knowledge, the Third Party Intellectual Property does not, and the use of the Third Party Intellectual Property by Customer as contemplated by this Agreement will not, infringe any intellectual property rights of any third party; and (iii) unless specifically provided otherwise herein, Customer shall have no obligation to pay any third party any fees, royalties, or other payments for Customer's use of any Third Party Intellectual Property in accordance with the terms of this Agreement.

© 2023 Foley & Lardner LLP

Example Vendor Warranty

With regard to (i) Open Source Software, (ii) any Third Party Intellectual Property that Company fails to identify in the applicable Order, and (iii) any Third Party Intellectual Property embedded in Background Intellectual Property for which Customer is not required to accept any third party terms and conditions, all such intellectual property shall be considered, as appropriate, part of and included in the definition of “Background Intellectual Property” and subject to all warranties, indemnities, and other requirements of this Agreement, including scope of license, relating to the Background Intellectual Property. To the extent permitted by law or contract, Company shall pass through to Customer the warranties for the Third Party Intellectual Property.

© 2023 Foley & Lardner LLP

Example Vendor Warranty

For purposes of this provision, "Open Source Software" means any software, programming, or other intellectual property that is subject to (i) the GNU General Public License, GNU Library General Public License, Artistic License, BSD license, Mozilla Public License, or any similar license, including, but not limited to, those licenses listed at www.opensource.org/licenses or (ii) any agreement with terms requiring any intellectual property owned or licensed by Customer to be (a) disclosed or distributed in source code or object code form; (b) licensed for the purpose of making derivative works; or (c) redistributable.

© 2023 Foley & Lardner LLP

Pulling it All Together

- Understand the “real” risks
- Which perspective are you?
  - Consumer
  - Distributor
- Document uses
- Control/mitigate risk of use
- Hold vendor’s accountable

© 2023 Foley & Lardner LLP

Questions?

© 2023 Foley & Lardner LLP

Contact Information



Michael R. Overly, Esq., Partner

CISA, CISSP, ISSMP, COP, CIPP, CRISC
Technology Transactions & Outsourcing Group

- Foley & Lardner LLP
  555 South Flower Street
  Suite 3300
  Los Angeles, California 90071
  (213) 972-4533
  moverly@foley.com

© 2023 Foley & Lardner LLP