Open Source Governance and Resources

Object Management Group

Standards for FOSS Governance Workshop

December 11, 2013

Virginia Fournier

Senior Counsel, Cloud Computing and Open Source

Hewlett-Packard Company

Agenda

- Open source landscape
- Why open source governance matters
- HP’s approach
- Available resources
- Q&A

Open source landscape

Examples of open source software

It is everywhere

Benefits of using open source software

Participation in the open source community can bring many benefits to an organization's business

- High quality software with zero marginal cost
- Source code can be customized for specific needs
- Direct user input that drives improvements
- Great security record (more eyes)
- Low-cost tools for software development and distribution widely available
- Avoid vendor lock-in and minimize development costs
- Decrease time-to-market for software products and solutions

Industry-wide open source successes

- **Operating systems**: Linux (embedded, mobile, server)
- **Web serving**: Apache - the world's most popular web server
- **Java middleware**: Tomcat, JBoss, Spring, Struts and Hibernate
- **Web development languages**: Perl, Python, PHP, Ruby, Rails, Grails, Go and Javascript
- **Internet security**: SSH/SSL
- **Cloud:** OpenStack and CloudStack
- **Developer environments**: Eclipse
- **Development tools**: GCC and the GNU Tool Chain
- **Databases:** MySQL, MariaDB, Drizzle, PostgreSQL and NoSQL
- **System management**: Nagios, CFEngine, Puppet and Chef
- **Distributed file & print services**: Samba
- **Web content management**: Drupal, WordPress, Plone and MediaWiki
- **Virtualization**: Xen and KVM
- **Big Data analytics**: Hadoop, Cassandra, Hive, Zookeeper, Traffic Server and Memcached
- **Web browsing**: Firefox, Chrome and Opera
- **Office productivity**: OpenOffice / LibreOffice

Challenges of using open source

Tracking & Managing Data

- How is it acquired?
- How is it chosen?
- How is it used? Where?
- How is it supported?
- How is it updated and secured?
- How is the project tracked?
- How is it licensed?
- How mature is it?

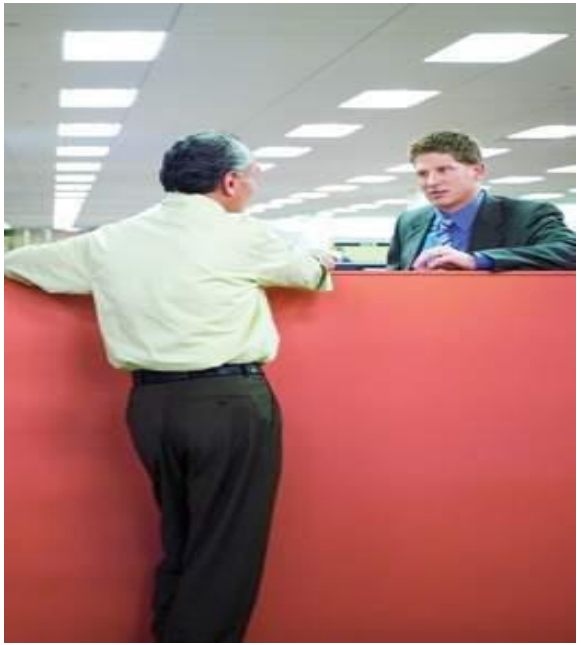
Licensing

- Key misunderstanding of open source licenses: there are obligations
- Open source licenses and licensing can be complex and complicated
- Keeping track of what open source is being used as products are developed
- Keeping track of the various open source licenses that govern different code bits used by an application, and how those code bits governed by different licenses interact

How is open source software different from commercial software?

Commercial Software

- Negotiated agreement
- Warranties
- Indemnification
- Support available
- No copyleft issues
- Costs money



Open Source Software

- No negotiations – take license “as is”
- No warranties
- No indemnification (IP)
- Support may not be available
- May have copyleft issues
- No cost

Why licenses are important

The fact that a piece of software may be readily available for free does not mean that the software is in the public domain (it's not like "free beer").

The copyright owner's permission is required to copy, distribute, or modify binary or source code under copyright law.

The copyright owner's permission is in the form of a license.
Open source software and license selections have legal implications.

Key message: open source software is licensed

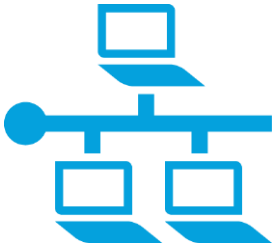
Why open source governance matters

Why open source governance is important

- Open source is everywhere!
- Open source usage & contributions often not visible
- Increasing requirements for compliance
- IT policies & processes may be insufficient
  - Usage must be reviewed in context (internal vs. distribution)
  - Legal exposure from 60+ Open Source Initiative (“OSI”) “approved” licenses (and there are many others) – many free & open source software (“FOSS”) packages could be in one product
  - Streamlined processes help to reap benefits & mitigate risks

HP’s approach

HP’s breadth in open source



Deploy internally

Redistribute

Embed

Contribute IP

Participate

Help customers

HP open source activities

Evaluating open source projects

Is the project healthy? Some things to consider are:

- Determine the **age** of the project ✓
- Identify people. **Who** is involved in the project? ✓
- Know the date of last **release**. ✓
- Find out if questions on mailing list get **answered**. ✓
- Are developers open to **ideas** from others on mailing list? ✓
- What are the **license** terms and can you comply with them? ✓
- Do developers have a **roadmap** (formal or informal) for the project? ✓

Case Study: OpenStack® Project

- Project began in July 2010
- 13,000 individual members from 130 countries, and 850 organizations; platinum sponsors include AT&T, Canonical, HP, IBM, Nebula, Rackspace, Red Hat and SUSE
- Havana is the latest release, October 17, 2013
- Questions on mailing list and on website do get answered
- Developers open to ideas from other members of the community
- Licensed under Apache 2.0
- Developers do have a roadmap for the OpenStack Project, and it's on the OpenStack website

Open source governance lessons learned

- Corporate-wide policies defined and communicated
- Develop open source legal expertise
- Corporate-wide training and awareness
- Inventory and track open source
- Need for open source review process/board
- Leverage tools for analysis and automation
- Special interest groups
- Find the org champions/sponsors

Best practices and available resources

HP shares best practices openly

Promoting open source governance in enterprises

fossology

- Forum to facilitate study of FOSS via free data analysis tools
- Original FOSSology tool-set developed and contributed by HP
- Tools scan files for licenses and copyright notices
- Similar to Black Duck, Palamida

http://www.fossology.org

- Community for FOSS governance; especially in IT environment
- Focus is on developing and sharing information and best practices, education, tools
- Founded by HP and partners; now part of Linux Foundation's Open Compliance Program

http://www.fossbazaar.org

http://www.linuxfoundation.org/programs/legal/compliance

SPDX

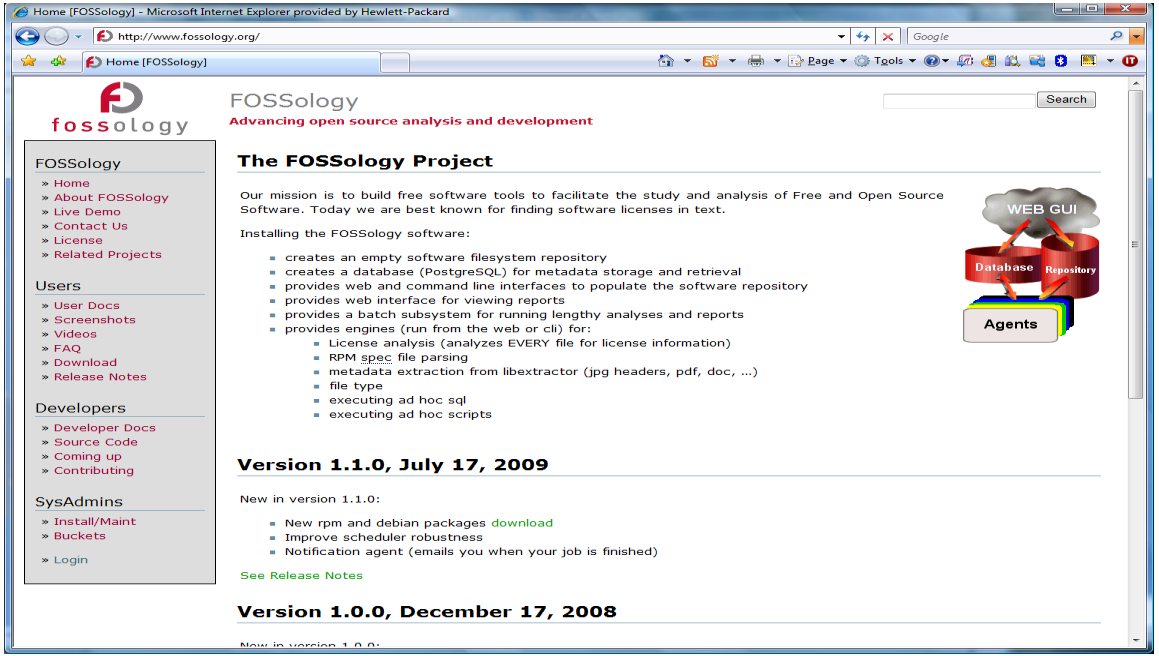
- Forum to standardize the format for communicating the components, licenses and copyrights associated with a software package
- Specification drafting began in a workgroup of FOSSBazaar; now part of the Open Compliance Program

http://www.spdx.org

FOSSology

http://www.fossology.org

Open source project built around an open and modular architecture for analyzing software



Linux Foundation Open Compliance Program

- A workgroup of the Linux Foundation
- Capture benefits and minimize risks of open source
- A community & knowledge-base for the exchange of best practices in:
  - Open source acquisition and deployment
  - Defining policies for governing open usage
  - Instituting processes for execution of those policies
  - Identifying tools and other resources to aid the execution of those processes
  - Discussing current events affecting open source

SPDX

SPDX standard format for communicating licenses and copyrights associated with software package

- Focus is on just the facts – no interpretations or legal analysis
- Provides a unified method for exchanging license information
- Avoids due diligence redundancy

SPDX working group is organized under the Linux Foundation's Open Compliance Program

- Intellectual property contributed by participants
- SPDX data file covered under the Creative Commons CC0 1.0 Universal license
- SPDX specification covered under the Creative Commons Attribution License 3.0

Structure

- General meeting and mailing list
- Teams: Technical, Business and Legal

Very inclusive process

- Self-subscription for interested participants
- Those willing to "do" can influence direction
- Mailing lists, wiki, phone calls, Birds of a Feather (BOF) sessions …
- http://spdx.org

A sample of available resources

Organizations

- Open Source Initiative (OSI)
- Free Software Foundation (FSF)
- FSF Free Software Licensing and Compliance Lab
- FSFE Freedom Task Force (FTF)
- gpl-violations.org
- Software Freedom Law Center

Communities

- Linux Foundation Open Compliance Program
- FSFE Legal Network

News and journals

- International Free and Open Source Software Law Review

Conferences

- FSFE ELN (European Legal Network)
- EOLE - European Open Source Law Event

Tools

- FOSSology
- Binary Analysis Tool
- Open Source License Checker
- Proprietary tools from Black Duck, nexB, Palamida

Open source developer resources

- OpenLogic Exchange (OLEX) – Download certified open source and get support
  http://olex.openlogic.com/
- Google Code Search – Find open source software by various criteria
  http://www.google.com/codesearch
- GitHub – Source code hosting and collaborative development
  https://github.com/
- SourceForge – Popular open source repository
  http://sourceforge.net/
- Ohloh – Open source project info/insight, social networking
  http://www.ohloh.net/

Summary

- Open source software is pervasive and its use is increasing
- Companies should think holistically about their use of open source software
- Companies should make informed decisions about open source software
  - Strategy
  - Selection
  - Integration
  - Governance
  - Contribution
  - Tooling

Q&A