Implementation of a FOSS License Compliance Program

_Coscup/GNOME Asia 2010_

Soeren Rabenstein (石書任)
ASUSTeK Computer Inc.
Legal Compliance Department
August 14, 2010
Syllabus

◆ Top 6 Misjudgements
◆ Compliance Program
◆ Tools
◆ Mistakes to Avoid
Top 6 Misjudgments

1. “We don’t use FOSS”
   In fact, most products involve FOSS, e.g.
   - Linux used in the majority of embedded devices
   - ~ 70% of the Internet runs on FOSS
   - Mobile platforms: Symbian, Android, WebOS, MeeGo
   - MacOSX/NEXTSTEP based on BSD
   - even Windows 7 contains FOSS
2. “Open source licenses are not enforceable or at least not enforced, so we don’t need to worry about license compliance”

Many court decisions, e.g.
– Welte./. Skype (Munich)
– Jacobsen ./. Katzer (Northern California)
– SFC ./. Samsung, WD, Best Buy, JVC, Bosch, Zyxel, Westinghouse, Phoebe, and others (last December, New York)
3. “Customers don’t care about our use of open source”
   – The copyright holders are amongst the consumers
   – Organizations like gpl-violations.org act based on specific complaints… there are many
   – Products are exposed to the market, you cannot hide
   – End-user-brand companies face big risks, will push it up the supply chain
Top 6 Misjudgments (Cont.)

4. Somebody else takes care of it
   - “The legal department will take care of it”
   - “The engineering department will take care of it”
   - “The supplier will take care of it”
5. “We use so little open source software that we can handle it informally”
   - If you do not manage it, you cannot know how big or little it is

6. “We are using FOSS for ‘Software as a Service’ (SaaS) applications only, so open source licenses obligations won’t apply”
   Not true for:
   - AGPL
   - M&A
Compliance Program

Open Source is ubiquitous

1. Needs to be managed
2. Process implementation is critical
Compliance Program (Cont.)

- Appoint central person for overall compliance
- Get management’s support
- Analyze current FOSS use
- Review licenses
- Define approved uses
- Delegate tasks/responsibilities
- Set-up SOPs that integrate with the existing workflows (verify, get feedback and revise)
- Publish policies/SOPs
- Educate employees
- Improve and control
Compliance Program (Cont.)

Required Processes

- Code management
- License management
- Inbound compliance
- Release management
- Outbound compliance
- Violations
Compliance Program (Cont.)

- Product Manager
- Engineers
- Legal

- Production
- IT
- Sales/Customer Support
- Community
- Supply chain
- Customer
Avoid external miscommunication

• Publish a dedicated contact window

• Enlist your compliance program with the Linux Foundation’s Compliance Directory

http://www.linuxfoundation.org/services/compliance/directory.
“Software BOM” or “Bill of Code”

• ‘List of ingredients’
• … and their respective licenses
• Code management essential
• Control document for compliance
  – Checklist for inbound compliance
  – Checklist for source code release
  – Checklist for license texts
• Product documentation for B2B customer
# Tools

## “Software BOM” or “Bill of Code”

### List of open source packages

<table>
<thead>
<tr>
<th>MachineName</th>
<th>DeclaredName</th>
<th>DeclaredLicense</th>
<th>DeclaredCopyright</th>
<th>URL</th>
<th>SourceInfo</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>KERNEL</td>
<td>GNU/Linux kernel 2.6.25.4</td>
<td>GPL-2.0</td>
<td>Linux Kernel Organizat</td>
<td>unknown</td>
<td><a href="http://www.kernel.org">http://www.kernel.org</a></td>
<td>YES</td>
</tr>
<tr>
<td>XFREE86_470</td>
<td>Xfree86 4.7.0</td>
<td>Xfree86 License</td>
<td>The XFree86 Project,</td>
<td>unknown</td>
<td><a href="http://www.xfree86.org">http://www.xfree86.org</a></td>
<td>YES</td>
</tr>
<tr>
<td>FIREFOX_3.0.4</td>
<td>firefox webbrowser 3.0.4</td>
<td>MPL-1.1</td>
<td>Mozilla</td>
<td>unknown</td>
<td><a href="http://www.mozilla.com">http://www.mozilla.com</a>,</td>
<td>NO</td>
</tr>
<tr>
<td>asus_acpi.patch_2.6.25.4</td>
<td>ACPI4Asus 0.3</td>
<td>GPL-2.0</td>
<td>Julien Lerouge, Karol</td>
<td>unknown</td>
<td><a href="http://acpi4asus.sourceforge.net">http://acpi4asus.sourceforge.net</a></td>
<td>YES</td>
</tr>
</tbody>
</table>

### List of closed source / proprietary packages

<table>
<thead>
<tr>
<th>MachineName</th>
<th>DeclaredName</th>
<th>DeclaredLicense</th>
<th>DeclaredCopyright</th>
<th>URL</th>
<th>SourceInfo</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADOBE-FLASH-PLAYER_10.0.0-d569</td>
<td>Adobe Flash Player 10.0.0-d569</td>
<td>Adobe Software License</td>
<td>Adobe</td>
<td>unknown</td>
<td><a href="http://www.adobe.com/">http://www.adobe.com/</a></td>
<td>NO</td>
</tr>
<tr>
<td>SKYPE_2.0</td>
<td>Skype 2.0.0.72</td>
<td><a href="http://www.skype.com/legal/e">http://www.skype.com/legal/e</a></td>
<td>Skype Limited</td>
<td>unknown</td>
<td><a href="http://www.skype.com">http://www.skype.com</a></td>
<td>NO</td>
</tr>
<tr>
<td>my_program1</td>
<td>My proprietary 1.0</td>
<td>my license agreement</td>
<td>Me :)</td>
<td>unknown</td>
<td>developed inhouse</td>
<td>YES</td>
</tr>
</tbody>
</table>
Tools (cont.)

Software Package Data Exchange™ (SPDX™)

- standard for communicating the components, licenses and copyrights associated with a software package
- Use in documents like SW-BOM/BOC
- SPDX™ to become industry standard
  ➔ Target Q4/2010
  ➔ monitor www.spdx.org
Source Code Scanning Tools and Services

• Fossology
• Blackduck™ Protex
• nexB™ Software Audit
• OpenLogic™
• Palamida™
• Source Auditor™
Further analysis tools

- Binary Analysis Tool
- Dependency Checker Tool
- Bill of Material Difference Tool
- ...

First port of call:

⇒ fossbazaar.org
Mistakes to avoid

• Policy/SOP need to suit workflows
• Policy/SOP must not be
  – too strict
  – too technical
  – too legal
  – unrealistic
• Ensure compliance till EOL+3years (Avoid the ‘Build Guru’)
• Be flexible, don’t just add another bureaucracy layer
Question and Answer

Thank You!