Best Practices for Open Source Compliance and Governance in Automotive

Kim Weins
SVP, OpenLogic
November 2011
Agenda

- Open source in Automotive
- Why Comply?
- Challenges of Compliance
- Best practices
End-to-End Open Source Management

Enabling Successful and Safe Open Source Adoption At Hundreds of Enterprises
Open Source in the Car
And Outside the Car

Mobile Apps

Cloud-Based Services
But Compliance is an Issue

Developers List

- ____________
- ____________
- ____________

OSS licenses you think you are using

Scan Results

- ____________
- ____________
- ____________
- ____________
- ____________
- ____________
- ____________
- ____________
- ____________
- ____________

OSS licenses you REALLY are using
71% of Apps using Open Source under GPL, LGPL and Apache do not comply

Source: OpenLogic Mobile Research 3/2011
Why comply?
Supply Chain Customers Demand It

Contract Terms

*Licensor shall disclose to Customer any Open Source included in the Work Product provided pursuant to this Agreement and shall warrant that Work Product complies with all of the relevant Open Source licenses.*
Cisco settles FSF GPL lawsuit, appoints compliance officer

Source: Ars Technica

Best Buy, Samsung, others named in GPL lawsuit

Source: cnet

Free software lawyers win GPL lawsuit

Injunction and $90,000 fine granted

Source: The Inquirer
Consumers Notice

**dtaubert**

Owners - please look through your manuals, other paperwork, and any digital media that accompanied the car. If the Volt uses GPL software, the various licenses would have been provided in one of these.

---

**dtaubert**

In the 711_03.08.03.02.zip archive:

<table>
<thead>
<tr>
<th>Length</th>
<th>Date</th>
<th>Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>22614</td>
<td>2010-12-13</td>
<td>13:18</td>
<td>field_upgrade_20101210-D1.1.2.tar.bz2</td>
</tr>
<tr>
<td>10147461</td>
<td>2010-12-13</td>
<td>13:12</td>
<td>linux-2.6.24-pro5024_eflex_fb_20101210-D1.1.2.tar.bz2</td>
</tr>
<tr>
<td>1078895</td>
<td>2010-12-13</td>
<td>13:14</td>
<td>u-boot_20101210-D1.1.2.tar.bz2</td>
</tr>
</tbody>
</table>

11248970 3 files

Under field_upgrade/target, there are many files named after "eflex", which would appear to be an early project name for the Volt:


The rest is not very exciting - a Montavista ppc kernel and boot loader. Curiously absent is the user side of things. Namely, GNU libc...
Loss of Your IP

Derivative work?

Depends on the license and how you combine the code

Open Source under “Copyleft” license

Your code

Linking
What are the challenges?
Three Challenges

1. Bundled licenses
2. SW development practices
3. Supply chain complexity
What most people think

Open Source Package

License

Reality

Main Open Source Package

Bundled Open Source Packages

Main License
Bundled License
Bundled License
Bundled License
Bundled License
Software Development Practices

SourceForge

Google Code

GitHub

and more….

FREE!

Your Source Code
Supply Chain Complexity

Software from vendors

Your Source Code
Compliance
Best Practices

(Be aware, not afraid)
Compliance Best Practices

1. Understand open source licensing
2. Create an open source policy
3. Track all open source usage – including from vendors
4. Conduct a scan or audit of your code
5. Develop a compliance checklist
1. Understand OSS Licensing

- Official definition of OSS license
  - Approved by the Open Source Initiative (OSI)
    - [http://www.opensource.org/](http://www.opensource.org/)
  - Currently over 70 approved licenses
  - Key Criteria
    - Free distribution
    - Source code is available
    - Derived works are allowed
    - Non-discrimination

- Many other “non-OSI” open source licenses
## Categorizing Open Source Licenses

### Liberal
- **No Strings**
  - MIT/X
  - W3C
- **Strings Attached**
  - Original BSD
  - Apache Software License
  - Eclipse Public License

### Copyleft
- **“Traditional” Open Source**
  - GNU GPL
  - GNU LGPL
- **Additional Clauses**
  - GNU GPL v3
  - GNU AGPL
  - Common Public License
  - Mozilla Public License
  - SISSL
  - IBM Public License
2. Create an Open Source Policy

- Things to include
  - Licenses allowed
  - Approval processes
  - Audit and compliance processes

- Considerations
  - Keep it lightweight
  - Don’t let fear guide you
3. Track all Open Source Usage: Why?

- Know what you are using
- Identify opportunities for sharing or savings
- Legal & compliance
- Maintenance
- Support
Vendor Best Practices

- Contract Requirements
  - Disclosure
  - Approval
  - Warranties
  - Indemnification
  - Scanning/Audit requirements

- Best Practices
  - Discuss open source with them early in the project
  - Get list of open source early in development cycle
  - Get a final list of open source when they provide final code
  - Get source code from vendor if at all possible (not just binaries)
  - Either scan all incoming code that you plan to distribute or consider spot audits
Getting Binaries vs Source Code

- Why you want to get source code from vendors
  - Source code scanning is more accurate than binary scanning
  - You can scan it and verify what open source is there
  - Your company must comply with open source licenses coming from vendors
  - Many vendors don’t have strong open source compliance programs
  - Relying on “manual, self-reporting” is extremely inaccurate

- If you accept binaries from vendors, consider the following
  - Does the vendor have an open source governance policy/process?
  - Does the vendor scan their own code?
  - Will the vendor supply you with results of scan?
  - Will the vendor warrant and indemnify around use of open source?
  - Is the vendor of sufficient size to make good on indemnification?
  - What is cost to you if the vendor gets it wrong?
    - Stop shipment?
    - Legal costs?
    - Reputation risks?
Create “Risk Tiers” for Software You Provide

- Risk Tier 1 – Fundamental
  - Product doesn’t work without it
  - Examples: Car dashboard, Anything that runs the car
- Risk Tier 2 – Critical to “experience”
  - Product works without it, but not a great experience
  - Examples: Entertainment system
- Risk Tier 3 – Nice to haves
  - Examples: Optional “apps” or add-ons
<table>
<thead>
<tr>
<th>Risk Tier</th>
<th>Acceptable Formats</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Tier 1</td>
<td>Source code</td>
<td>You scan</td>
</tr>
<tr>
<td>Fundamental</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Tier 2</td>
<td>Source code or binaries</td>
<td>You scan or vendor scans and provides</td>
</tr>
<tr>
<td>Critical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Tier 3</td>
<td>Binaries</td>
<td>Vendor scans and provides Bill of Materials</td>
</tr>
<tr>
<td>Nice to Have</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Conduct a scan or audit of your code

- **Outcome of an OSS audit:**
  - List of open source packages
  - List of open source licenses
  - List of license obligations (compliance checklist)
  - List of licenses that may have conflicting terms

- **Options**
  - Scanning tools
  - Audit services
  - Manual review
5. Develop a compliance checklist

- Create a compliance checklist:
  - Notices in code and/or documentation
  - Source code provided in proper way
  - Is there an EULA for your product?

- If there are conflicts or compliance is not possible:
  - Can you live without this code?
  - Is there an alternative to the code?
  - Can you contact the author and ask for an exception/different license?

- Risk management:
  - What is likely to get litigated?
  - What are your sticking points that prevent perfect compliance?
Complying with Licenses

Open Source Downloads  

**Click to see:**

Licenses available for download

**LEGAL NOTICE:** This software is distributed without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose. For additional information, see the [Licenses available for download](#) and information provided in the source code files.

**WARNING:** Making modifications to the vehicle may adversely affect performance and/or safety. Additionally, software modifications not issued through the company will void the warranty coverage for those vehicle components that are damaged or otherwise affected by the software modification.

Click to download software and additional materials

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Part</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>------------</td>
<td>------</td>
<td>----------</td>
</tr>
</tbody>
</table>
Thanks!

- **Learn more**
  - [www.openlogic.com](http://www.openlogic.com)
  - Free resources at [www.openlogic.com/downloads](http://www.openlogic.com/downloads)
    * Policy Builder
    * Whitepaper: Open Source Compliance in the Supply Chain
  - [SPDX](http://www.spdx.org)
    * [www.spdx.org](http://www.spdx.org)
- **My contact information**
  - Kim.weins@openlogic.com
- **Follow**
  - @openlogic
  - @KimAtOpenLogic