Corporate Open Source Compliance: The Hard Parts

Andrew Wilson
Intel Open Source Technology Center
4-December-2014

Introductions – Andrew Wilson

- Director of open source compliance at Intel Corp
- Involved with FOSS in some capacity since the late 1980s.
- Chair of the Carrier Grade Linux steering group 2002-2005.
- Co-author and instructor for Intel’s internal open source training
- Former venture capitalist and dealmaker with Intel Capital
- I have a longtime interest in the interaction of technology, law, economics, and society

Disclaimers!

- I am not a lawyer; this is not legal advice
- One size never fits all. What is right for Intel may be wrong for you.
- Offered in the hope that some of our experience may be helpful for you
- Open source is about sharing

Open source* compliance is usually straightforward

- When you have process, training, and policies
- When there is a set procedure and it is followed
- “Many eyes make all bugs shallow”
- … usually true, but not always
- Still some areas where extra efforts are often needed

**includes Free, Libre, and Open Source*

Andy’s irritant list (not in any particular order)

- Balky corporate infrastructure
- 3rd party SW
- M&A transactions
- understanding tool output
- lack of open source legal specialists
- contributor agreements
- Patent-encumbered standards

Balky corporate infrastructure

- Intel has big download servers – usually a good thing
- Except when they require a click to accept end user license (EULA) for all SW downloads
- And GPL says
  - It is not a contract; no click to accept required
  - And you may not sublicense under more restrictive terms (no EULA)
- One drafting fix is to revise all corporate EULAs to say they do not apply to GPL or to other FOSS; the open source license governs
- One technical fix is change the system to allow no-EULA downloads

3rd party SW

- Everyone uses outsourcing suppliers (even outsourcing suppliers)

- Some 3rd party suppliers do not (or cannot) provide accurate license information

- Free plug: this problem is so pervasive the Linux Foundation Open Chain initiative aims to create an ISO standard for SW information
  - Much work to do
  - Partial fix: use SPDX tagging whenever possible

- Be firm and precise with suppliers. Tell them exactly what you need.
  - “One man’s ceiling is another man’s floor” – Paul Simon
  - To your customers, you are a supplier. Pass along all information you would want from your suppliers.

M&A

- Special (& very important) case of 3rd party problem
  - If you are a customer and there is a compliance issue, it is the vendor's problem.
  - When you buy the vendor, their problem becomes /your/ problem
- Most small companies will have a less rigorous view of open source compliance than multinationals – fact of life
- M&A team must know this. Must engage open source team before the close.

Code scanning tools

- Now routinely used for M&A transactions
- Tools are good ☺
- No tool is ever perfect ☹
- Tool reports /must/ be reviewed by trained humans
- Creates a demand which can be peaky and unpredictable for reviewers

Lack of open source legal specialists

- Same problem as qualified reviewers of code scanning tools, only possibly worse
- Shocking (to me) mismatch between $ volume of world commerce dependent on open source versus number of qualified legal specialists
- Not a recognized legal subspecialty and very few experienced practitioners
- Lack of case law in most jurisdictions does not help and places a premium on personal experience

Contributor license agreements (CLAs)

- Disclaimer! I have written CLAs myself. They are not inherently bad.
- They /are/ corporate licenses and therefore require top-level corporate legal approval
- Worst case scenario: each sub-project requires its own CLA, even if the text is exactly the same as all others (yes, I mean the Apache Foundation)
- Then add a requirement for individual contributors to sign in addition to the corporation which employs them
  - Bother!

Patent-encumbered standards

- Hard problem. Standards world and FOSS world do not (usually) talk to each other.
- RAND standards do not play well with the GPL “liberty or death” provision. RANDZ or RF are much more compatible (if harder to find).
- Creates a need to prescreen FOSS code submissions for standards-related patent issues.
- Free plug! Samsung, Intel (+ many others) are attempting co-development of the OIC standard and the Iotivity reference open source implementation. RANDZ standard, and, a permissive open source license (Apache v2)!

We’re at the tail end!

Questions!