Future Open Source Leaders
OpenChain Training

Sami Atabani
Senior IP Consultant

Copyright © 2020 Sami Atabani - licensed under CC-BY-1.0
Have you seen this?

OSS Developer

Legal

I wonder if I can use this OSS in this latest AI product… hmmm I should talk to legal.

Hi, Lady Justice, I would like to use this OSS in our latest AI product, is that okay?

Hi developer, maybe… what is the license and which product is it going to be redistributed in?

It’s for the neural network, I think the OSS is under….

Apache

Sigh…

Can you check?

I have just checked, I think it is Apache 2.0.

Apache 2.0 is a whitelisted license according to our policy, can you extract the license text and copyright notices to fulfil the obligations?

Sure, I’ll be in touch soon.

Some time later…

Sort of… I have the copyright notices, but the license is GPLv2.0 but it is Apache 2.0 on the project homepage

So… do you have the license text and copyright notices so we can fulfil the license obligations?

Hmmm… We need to do further digging to confirm which license applies.
Why is Open Source licence compliance critical

- Revocation of licence
- Business success
- Engineering efficiency
Why do we need to manage Third Party IP (TPIP)?

• Risk analysis and management
  • Support and maintenance
  • License obligations and interaction with company agreements

• Business Implications
  • Potential impact on negotiations
  • Customers want to know!

• Improve efficiency
  • Repeat requests
  • Inconsistent processes lead to delay and frustrations

Managing TPIP needs to be proactive (not an exercise in putting out fires)!
How most organizations interact with Open Source

- Contribute to external open source project
  - On behalf of Company
  - As an individual
- Join an open source project, standards body or other collaborative group
- Create a company open source project
- Create a new standards body

Use TPIP (incl. open source software & implementing a standard)
  - Internally
  - In a product
What does good open source licence compliance mean?

• Knowing what open source packages are in your distributed software

• Knowing what open source licences apply to the open source packages in your distributed software

• Ability to fulfil open source licence obligations

• Having a clear process to accomplish all of the above
What is OpenChain?

- A collaborative project with a vision to build licence compliance trust across the supply chain
- Providing a licence compliance framework for organisations to follow
- Offering consistency across the supply chain
Road to OpenChain conformance

- Do we have a clear policy governing open source?
- Do we have a documented process adopted across the organisation?
- Do we have the necessary tooling?
- Have all employees who interact with open source including licence compliance been trained?
- Do we audit our process?
Company Third Party IP Policy

*Business success in technology companies is often dependant on monotonising our IP rights. With the same token you must respect the IP rights of other.*
Process for managing Open Source and compliance

- Documented process for managing TPIP
- Online tooling to track TPIP
  - Accessible across company
  - Capture key details
  - Record compliance obligations
  - Clear process for fulfilling source code release
- Automation of compliance
  - Fossology, Tern, Commercial tools
Company wide training

• Educate staff about basics of IP Law
• Enable staff to understand why compliance is essential
• Highlight benefits of managing TPIP
• Provide clarity on responsibilities
• Where to find information
Road to OpenChain Conformance

1.1.1 Documentation of FOSS policy
1.1.2 Internal communication of policy
   1.2.1 Training material
   1.2.2 Documented way of tracking training
   1.2.3 >85% Software staff complete training

Training modules created:
• Introduction to Intellectual Property Law
• Introduction to Patents
• Introduction to Open Source Software and Licenses
• Introduction to Processes for Third Party IP, Open Source, and Standards

Available via Learning Portal, mandatory for some

>85% Software staff complete training (currently 91% - over 5000 employees)
What does success look like?

• Clearly defined policy and process for TPIP management
• Automation of compliance and tracking tools
• Well understood governance and structure
• Education of employees across the organisation
Organisation management of OSS, third party IP, and standards

Use TPIP (incl. open source software & implementing a standard)
- Internally
- In a company product

Contribute to external open source project
- On behalf of company
- As an individual

Join an open source project, standards body or other collaborative group

Create a company open source project
Create a new standards body

Open Source Program Office (OSPO)
Hi, Lady Justice, I want to use this library from this OpenChain conformant project.

Hi developer, can you send me the SPDX file?

Great! Let me look over it.

Yes, these licenses are whitelisted with the company policy. You can go ahead and record this request in the TPIP tracker.

Sure… in fact I have the SPDX file here.

Short time later…

Sure. I will also attach the SPDX file.

Great! I will approve it later today.

Being OpenChain conformant makes my life easier.
Thank you!