FINOS 14 November, 2018

Amanda Brock, Open Invention Network,
Consultant, abrock@openinventionnetwork.com

Open Source – the inevitability?

Step One:
What is an Open Source Audit?

Step Two:
Why conduct an Open Source Audit?

Why audit – good hygiene

Why audit – financial arrangements

Why audit – litigation or regulatory review

Step Three:
How to do an Open Source Audit?

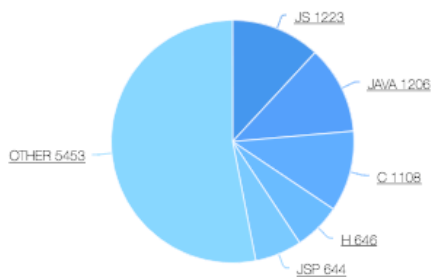# Kick Off
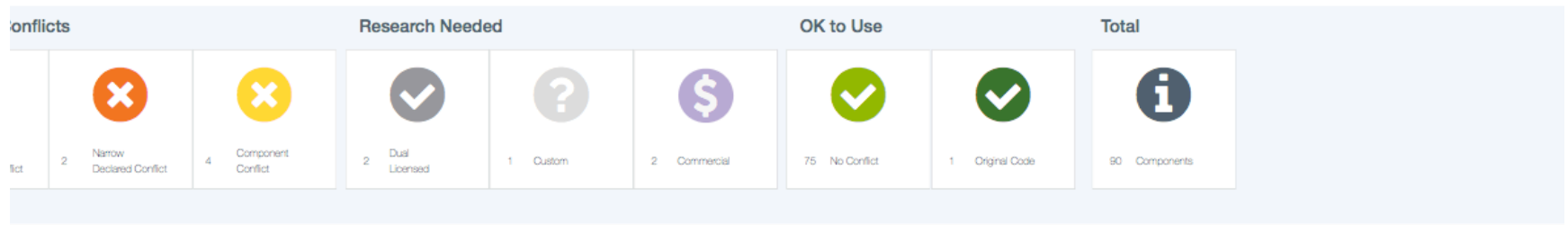
Who should be involved in the audit – decision makers
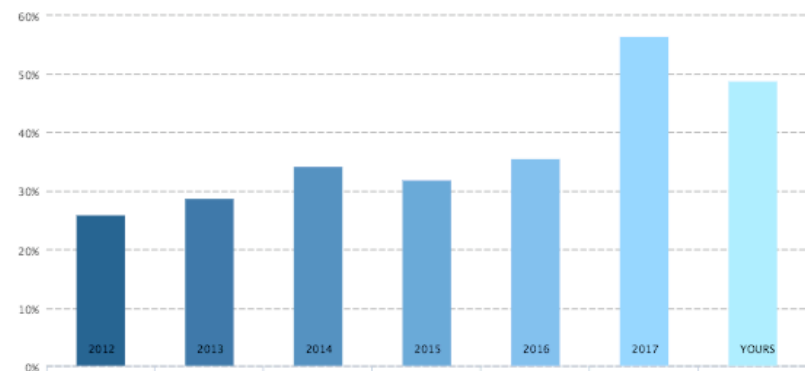
What tools should we use to conduct an audit?

BlackDuck Audit report

BlackDuck Dashboard

Audit output – Flexera priority

| Licence Priority	Typical Licence for level	Description
1	Copyleft/Viral Style licenses such as: GPL, AGPL, LGPL, CDDL, MPL, EPL.	Contains viral (copyleft) licenses. Dual/Tri licenses with viral license as an option.
2	Commercial Licences, Less common OS licenses, Vanity / Strange licenses, Code Project Open License Items with no known or unknown licence.	Contains items with lesser known open source license, Commercial license, or unknown licenses.
3	Permissive/Attribution style licenses such as: Apache 1.1or 2.0, MIT, BSD, Public Domain	Typically require a simple attribution in the product or documentation.
4	Dual/tri licenses with permissive option such as: GPL or MIT	Associated dual/tri licenses where one of the option is permissive.

Open Source Initiative approval

Copyleft and the GPL

"I make my code available for use in free software, and not for use in proprietary software, in order to encourage other people who write software to make it free as well."

"I figure that since proprietary software developers use copyright to stop us from sharing, we co-operators can use copyright to give other co-operators an advantage of their own: they can use our code."
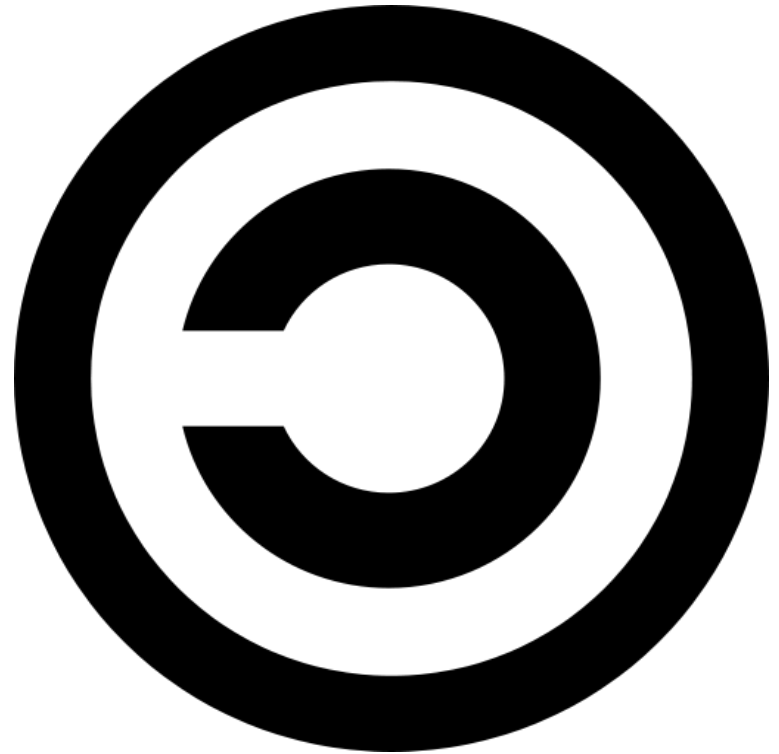
Viral Effect of Copyleft
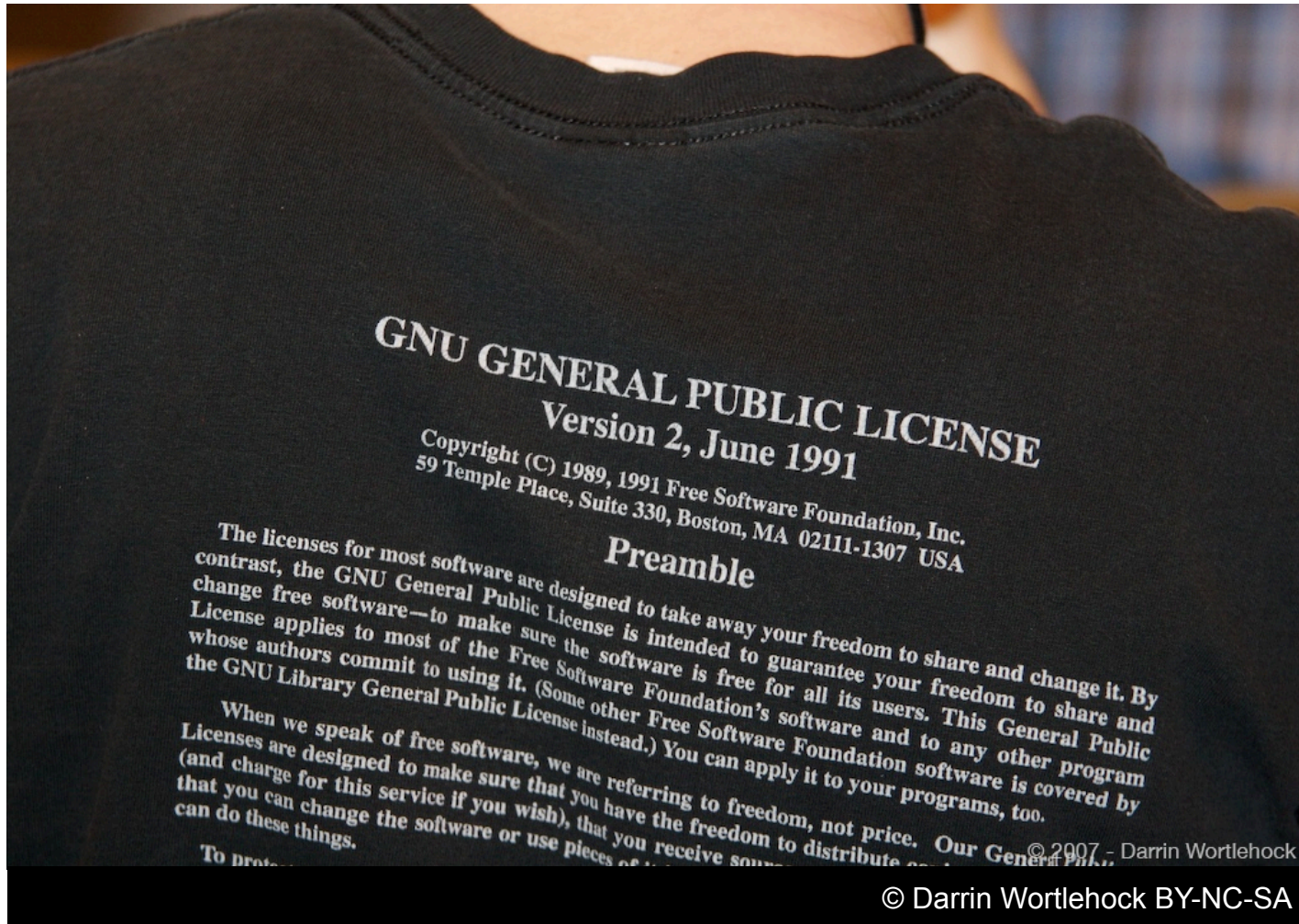
Permissive BSD

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Fixes

- Technical – engineering
- Legal – licensing decisions
- Licensing Hocus pocus – interactions etc.
- Decisions will impact later procedures and policies

BOM – licence status and components

❌	Declared Conflict (Broader Reach)	Conflicts	886	8.62
❌	Declared Conflict (Narrower Reach)	Conflicts	332	3.23
❌	Component Conflict	Conflicts	220	2.14
✅	Dual Licensed (Commercial vs. Conflict)	Research	410	3.99
❓	Custom	Research	114	1.11
$	Third Party Commercial	Research	440	4.28
✅	No Conflict	OK to Use	3,442	33.48
✅	Original Code	OK to Use	4,436	43.15

Declared Conflict Broad 8,62 %
Declared Conflict Narrow 3,23 %
Component Conflict 2,14 %
Dual Licensed 3,99 %
Custom 1,11 %
Commercial 4,28 %
Original Code 43,15 %
No Conflict 33,48 %
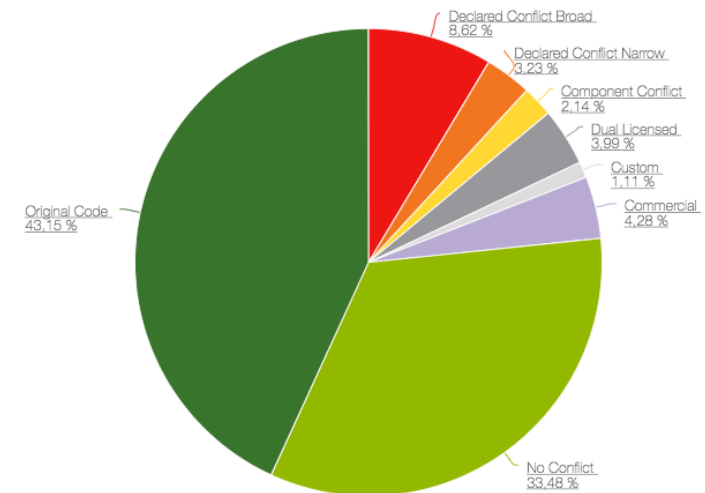
	COMPONENT	VERSION	LICENSE	STATUS	GROUP	USAGE	FILE COUNT	NOTIFICATIONS
1	Sample Audit - Jan 2018 (DO NOT DELETE)	Unspecified	[template] Basic Proprietary Commercial Lice…	Original Code	OK to Use	Original Code	4,436	💬 🚚 🔗
2	3D Tools for the Windows Presentation Foun…	Unspecified	Microsoft Limited Permissive License (Ms-LPL)	Component Conflict	Conflicts	Snippet + File	218	💬 🚚 🔗
3	angular.js	1.1.2	MIT License	No Conflict	OK to Use	Snippet + File	1,459	💬 🚚 🔗
4	Apache ActiveMQ	5.1.0	Apache License 2.0	No Conflict	OK to Use	Dynamic Library	1	💬 🚚 🔗
5	Apache Commons CLI	1.4	Apache License 2.0	No Conflict	OK to Use	Dynamic Library	1	💬 🚚 🔗

Deeper Dive?

Step Four:
What follows an Open Source Audit?

OS Procedures and Policy

'What do you mean don't open source it?
I've already laid off Engineering and QA."

Open Source – warranty

- Limited warranty – best of knowledge

- State of the industry/ art and tools - audited

- Cannot ever warranty IP in open source

- Indemnities?

Some final thoughts

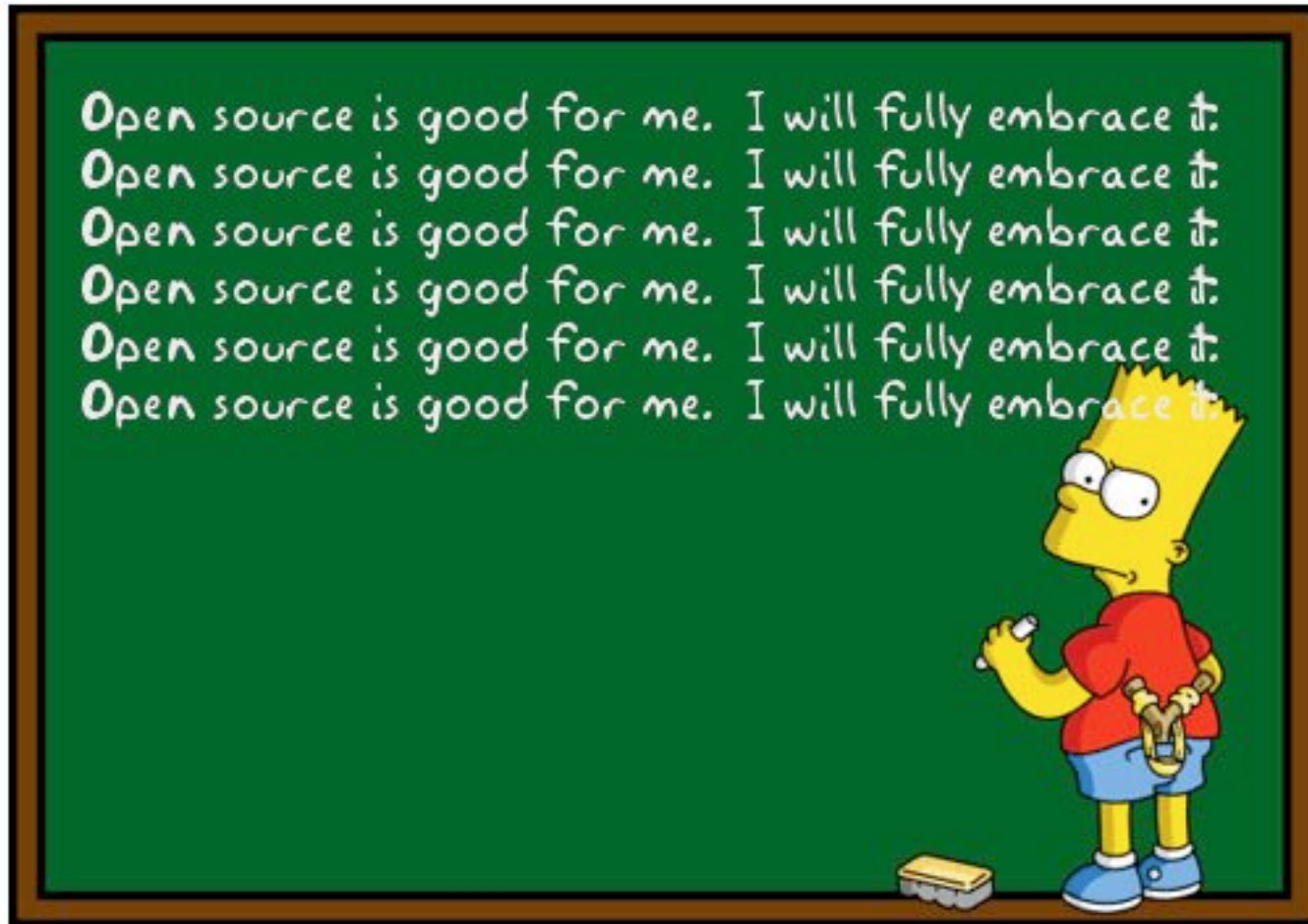# Software Patents

© K. Murali Kumar

Patent War Responses - OIN

Collaboration and Co-opetition

Discussion

© The VAR Guy