SPDX IN SOFTWARE EXCHANGES

Matt Germonprez
Georg Link
Robin Gandhi

University of Nebraska Omaha

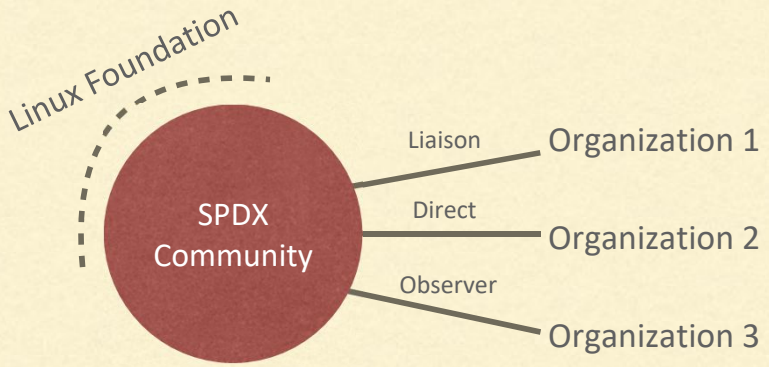
Omaha! The Rumors are True

ATTRIBUTION 4.0 INTERNATIONAL (CC BY 4.0)

- Share — copy and redistribute the material in any medium or format
- Adapt — remix, transform, and build upon the material
- for any purpose, even commercially.
- The licensor cannot revoke these freedoms as long as you follow the license terms.
- https://creativecommons.org/licenses/by/4.0/

Interview Sample

- 16 Interviews
- 16 Questions
- 30-45 Minutes
- Approximately 10 hours



Types of Organizations:

- Software Oriented
- Hardware Oriented
- Compliance Tooling
- Open Source Built

SPDX Relationships:

- Liaison
- Direct Participant
- Observer

Organizational Roles:

- Developer
- Founder
- Lawyer
- Compliance Manager
- Project Manager

Interview Questionnaire Development

- Research team experience
  - With Community - Since 2012
  - With Tooling - Yocto // DoSOCS
  - With Companies - Community Members and Non-members
- Vetted with Linux Foundation Members
- Available upon Request

FINDINGS

https://c1.staticflickr.com/1/165/367040618_7c938238f7_b.jpg

SUCCESSES (1/2)

License List

- *"Once SPDX created a vetted list, we no longer sent volumes of agreements."*
- *"We always standardize on the license list in every discussion, whether it be with an attorney, a product manager or an engineer."*

Short Identifiers

- *"I love the short identifiers. It's the greatest, handiest thing. It's very efficient."*
- *"It's really simple to adopt."*

SUCCESSES (2/2)

SPDX Community Collaboration

Exchange of ideas with like minded folks

Solving shared issues around compliance

- *"It's the process of discussion that generates most of the viable input."*
- *"It does help with reaching out with other people with similar interests and understanding what's going on and what the problems are."*

Internal Processes are Being Informed by SPDX

- *"SPDX has been talking about this license expression syntax and so we said let's use that."*

MIXED OPINIONS (1/2)

Spec is Representative of Compliance Issues – But it is Too Complicated

- *"Excessive complexity is getting in the way of adoption."*

Declared and Concluded Licenses

Different levels of rigor in reaching conclusion

Software does not give the best results - always requires manual intervention

- *"This is where, at some point still, I think humans have to make some decisions."*
- *"It's useful for someone to communicate the level of verification that they've done."*
- *"We do this [sign-off] manually currently."*

MIXED OPINIONS (2/2)

Automated Tooling

Helps with declared - concluded relationship

Inaccuracies results and variable strategies in dealing with those inaccuracies

- *“They’re not necessarily relying on the outputs, the report, or anything.“*
- *"I know that the SPDX report is not 100% representative of all IP that’s in a product. It’s our best approximation so far.”*

POINTS OF CONCERN (1/4)

The ‘X’ in Exchange

Supply chain drivers are largely nonexistent upstream or downstream

- *No one has asked us for an SPDX report for our product yet. They’ve asked for open source disclosure. They don’t care what the format is.*

Lack of Full Coverage of Licenses with Standard List

Organizations may manage a combination of internal and standard list

Lack of motivation to contribute new licenses to license list

- *“That's actually probably one of the barriers to adoption of the SPDX license identifier system is that it's so incomplete from our perspective for purposes of anything like a Linux distribution.”*
- *“I don't [submit all licenses to the SPDX list] because sometimes I think this is a really obscure license, it's just not worth the effort.”*

POINTS OF CONCERN (2/4)

The Ability to Consume

Difficult to use SPDX without a tool

Tools could be better tailored to lawyers and release managers

Right now the tools appear to be tool-vendor focused

- *"We have to at least produce a PDF or an HTML report."*
- *"If you have an SPDX file, it can't be reviewed by a human being without having some tools available."*
- *"Mostly, it's not for our developers, it will be for our release managers."*
- *"The SPDX specification is meant for tool people, not for developers or anyone else."*

POINTS OF CONCERN (3/4)

SPDX Fields are Unused for Internal Management

The information is there and it could be mapped but this is rarely done

Unsure of the precise coverage of the spec and internal needs

- *"All the other data backup software in our data warehouse, we wouldn't pull out the open source data especially put into SPDX to interpret it."*
- *"We're still trying to figure things out."*

POINTS OF CONCERN (4/4)

Vulnerabilities not a Big Concern for SPDX

These risks are handled by a separate group in the company

Vulnerabilities are typically dealt with prior to exchanges in a supply chain

- *"I'm not really all that concerned about providing vulnerability tracking, so we're not going to do that."*
- *"That's something that's handled separate from legal risk. We have [a different] department."*
- *"Ideally you wouldn't ship a product with known vulnerabilities that exist in that package."*

At Best, SPDX is Mentioned in Developer Training Programs

- *"We just talk about using the license identifiers because it's a standard. That's really about it."*

http://www.freeiconspng.com

FOOD FOR THOUGHT

http://free-extras.com/images/goofy_cartoon-4929.htm

FOOD FOR THOUGHT (1/2)

- Large organizations perceive value in automated gates
  - But use in continuous integration is limited
- OSS risk knowledge may become common and distributed
  - Formalizing it through a central spec runs counter
  - OSS mature institutions may already handle compliance issues well

FOOD FOR THOUGHT (2/2)

- What is the business driver? Not all organizations have complex supply chains in a classic software supply chain sense.
- Different use cases based on different supply chains
- The supply chain end point practices are highly variable
- Organizations that are not engaged in the SPDX community may not perceive value in adoption, even with community liaisons!

http://www.freeiconspng.com

THANKS

University of Nebraska Omaha

- We are very willing to chat with your organization more.
- If you would be willing to do an interview with me or Georg, please let us know.

UPDATE

- The results of this project are published and available:

- Gandhi, R., Germonprez, M., & Link, G. J.P. (2018). Open data standards for open source software risk management routines: An examination of SPDX. In ACM GROUP '18 Proceedings. https://doi.org/10.1145/3148330.3148333