Survey of Legal Questions in the Software Supply Chain

Survey Flow

Standard: Consent (2 Questions)
Standard: Definition of SBOM (5 Questions)
Block: Legal Stuff (8 Questions)
Standard: AI Questions (3 Questions)
Standard: Demographics (4 Questions)

Page Break

Start of Block: Consent

CF1 Investigating the state of practice in software supply chain management RESEARCH GOAL AND PROCEDURE The purpose of this study is to investigate issues, needs, and opportunities related to software supply chain management. This includes details regarding software licensing, compliance, and other legal concerns.

The (open source) software supply chain is the set of processes, components, and tools used to develop, build, and publish a software product (a system, library, tool, etc.). Software vendors often create software products by assembling open source software components (aka dependencies) developed by third-party developers or organizations. Common tasks involved in supply chain management include maintaining license compliance among components, managing and screening dependencies, and mitigating security threats introduced in software dependencies. If you decide to participate, you will take a brief survey/questionnaire. The survey will last about 20-30 minutes during which time you will be asked questions regarding your thoughts and experience regarding several topics related to the open source supply chain, **including Software Bills of Materials (SBOMs) and associated legal concerns.** We may contact you by email to invite you to participate in a follow-up interview. RISKS AND BENEFITS There are no foreseeable risks for participating in this research. There are no benefits to you as a participant other than to further research in software engineering and the open source software supply chain. PARTICIPATION You must be at least 18 years old to participate. Your participation is voluntary, and you may withdraw from the study at any time and for any reason. If you decide not to participate or if you withdraw from the study, there is no penalty or loss of benefits to which you are otherwise entitled. There are no costs to you or any other party. Your decision whether or not to participate will not prejudice your future relations with [Organization]. If you decide to participate, you will be entered into a drawing for a $50 USD Amazon gift card upon completion of this survey. We will randomly choose respondents and give out 10 gift cards. CONFIDENTIALITY The data collected by this study will be confidential, including your responses. Any information obtained in connection with this study that can be identified with you will remain confidential and disclosed only with your permission. You will be assigned a code number to protect your identity and all data will be kept secure. If you give us your permission by signing this document, we plan to disclose the results of the questionnaire in any publication resulting from this study. The disclosed results will not be personally identifiable (if needed, they will be anonymized). The de-identified data could be used for future research without additional consent from participants. The Institutional Review Board (IRB) and [committee] that monitor research on human subjects may inspect study records during internal auditing procedures and are required to keep all information confidential. CONTACT This research is being conducted by [Anonymous Author(s)] from [Organization]. Questions regarding the rights of research subjects may be directed to [redacted]. Such committee has reviewed and approved the present research ([protocol]) CONSENT You are welcome to print this page to keep a copy of this form.

Do you consent to participate in this survey?

JS

CF2 **YOU ARE MAKING A DECISION WHETHER OR NOT TO PARTICIPATE.**

IF YOU WANT TO PARTICIPATE, PLEASE ENTER YOUR NAME IN THE TEXT FIELD BELOW, AND START THE SURVEY.

Please enter your name.

_____

End of Block: Consent

Start of Block: Definition of SBOM

D1 Are you familiar with the concept of Software Bills of Materials (SBOMs)?

- Yes (1)
- No (2)

Display This Question:

If Are you familiar with the concept of Software Bills of Materials (SBOMs)? = No

SBOM Technical Def The National Telecommunications and Information Administration defines a **Software Bill of Materials** (SBOM) as follows:

An SBOM is a formal, machine-readable **inventory of software components and dependencies**, information about those components, and their hierarchical relationships. These inventories should be comprehensive – or should explicitly state where they could not be.

SBOMs may include **open source or proprietary software** and can be widely available or access-restricted. SBOMs should also include baseline attributes with the ability to uniquely identify individual components in a standard data format. The most efficient generation of SBOMs is as a byproduct of a modern development process. For older software, less-automated methods exist.

Display This Question:

If Are you familiar with the concept of Software Bills of Materials (SBOMs)? = Yes

D2 What do you consider to be the minimum adequate baseline component/dependency information for an SBOM?

_____

_____

_____

_____

_____

Display This Question:

If Are you familiar with the concept of Software Bills of Materials (SBOMs)? = Yes

D3 In your estimation, how many SBOMs meet this minimum standard in practice?

_____

_____

_____

_____

_____

D4 Are you aware of any specific requirements that organizations must meet when creating SBOMs for software products that will be used in highly regulated industries, such as healthcare, finance, or defense? If so, please describe those requirements.

_____

_____

_____

_____

_____

End of Block: Definition of SBOM

Start of Block: Legal Stuff

L1 Updating equipment in critical facilities, like hospitals, can be difficult since all equipment needs to be first approved by government regulators.

How do you think that an SBOM that includes information about the software and hardware components of such equipment could facilitate faster and more accurate approvals, if at all?

_____

_____

_____

_____

_____

L2 Are you aware of any disputes relating to an organization's creation or use of SBOMs?

- ○ Yes (please explain) (1) _____
- ○ No (2)

L3 If an SBOM is inaccurate or incomplete, what legal liability do you see for the entity that produced it?

_____

_____

_____

_____

_____

L4 What liability do you see for the creators of tools used to automatically generate SBOMs that are incomplete or inaccurate?

L5 In your opinion, to what extent will the provision of an accurate and complete SBOM become a standard provision in software licenses and related contracts?

L6 Should the creator of an SBOM be required to provide a certification that the SBOM is correct and complete? Please elaborate on your response.

L7 What steps can organizations take to protect their proprietary information and trade secrets when creating and distributing SBOMs?

L8 An SBOM could reveal a vulnerability or security issue in a software component.

To what extent are organizations legally obligated to disclose any vulnerabilities or security issues they discover as a result of creating an SBOM to their customers, partners, or the public?

End of Block: Legal Stuff

Start of Block: AI Questions

AI1 We refer to a **"DataBOM"** as a document which serves as a Bill of Materials for a dataset used to train a AI or machine learning model. A DataBOM would include information regarding the nature and provenance of any information or values (images, text, etc.) included in the dataset.

AI2 GitHub Copilot is a service described as an "AI pair programmer." Copilot can quickly generate code based on prompts from human programmers. To accomplish this, the AI system learned to generate code through training on open-source code from the Internet, including material hosted in public GitHub code repositories. In late 2022, a class action lawsuit was filed against GitHub, Microsoft (GitHub's owner), and OpenAI (the company behind the AI model

which powers GitHub Copilot).

The plaintiffs in the GitHub Copilot litigation claim, among other things, that by training their systems on public GitHub repositories, the defendants have violated the attribution requirements of certain open-source licenses which apply to the code on which the AI model was trained.

In your opinion, would the use of complete and detailed DataBOMs be sufficient to cover the attribution requirements of open source software licenses?

_____

_____

_____

_____

_____

AI3 Do you anticipate DataBOMs being used with other large AI projects, like ChatGPT, that are trained on large corpora from the Internet?

- ○ Yes (4)
- ○ No (5)
- ○ I don't know (7)

End of Block: AI Questions

Start of Block: Demographics

*

Q1 How many years of legal experience do you have?

_____

Q2 Which country / countries are you and / or your organization based in?

_____

Q3 Please enter your email address. This will be used to contact you if you are identified as the recipient of the Amazon gift card.

_____

Q4 Would you be willing to participate in a follow-up interview based on your responses?

- Yes (1)
- No (2)

End of Block: Demographics