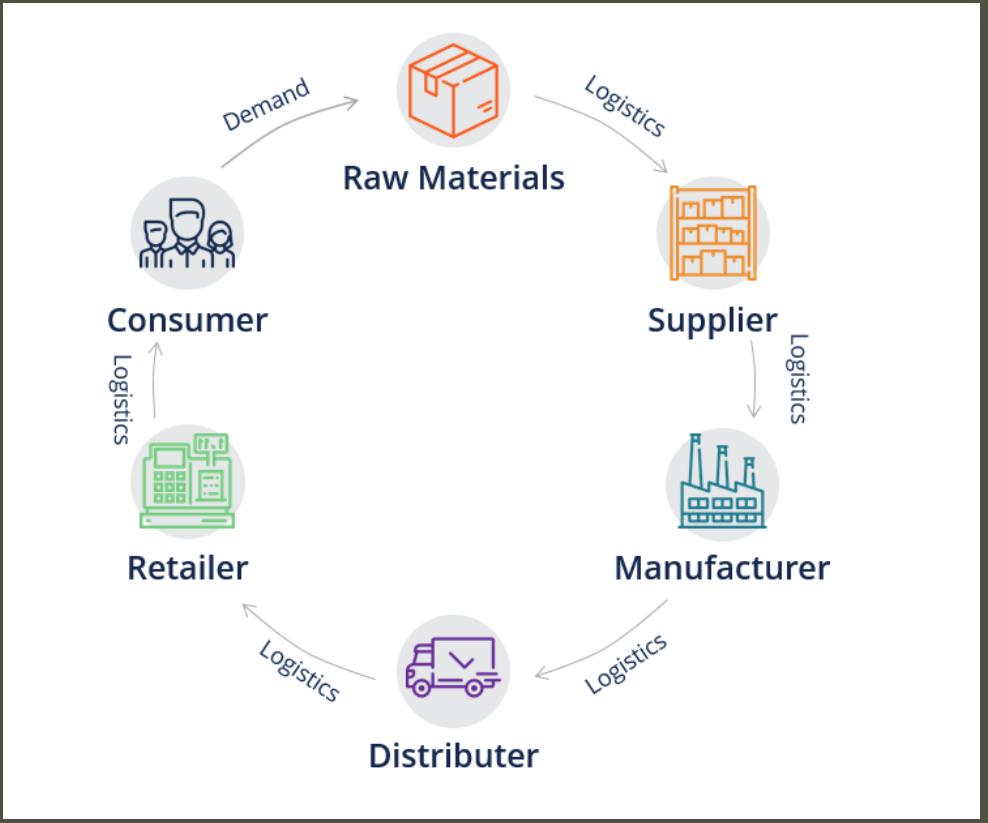
Is There Really an SBOM Mandate?

Bradley M. Kuhn, Policy Fellow & Hacker-in-Residence
at Software Freedom Conservancy

FOSDEM 2025, Saturday 1 February 2025

Slides at: https://ebb.org/bkuhn/talks/FOSDEM-2025/

The Analogy Does Not Fit



Is There Really a Software Supply Chain?

Is There Really a Software Supply Chain?

Not Really!

Is There Really a Software Supply Chain?

Not Really!

- ~~Shipping containers~~
- ~~Giant cranes~~
- ~~Leakage (literal or figurative)~~
- ~~phone, lights, motor car~~
- ~~any single luxury~~

Is There Really a Software Supply Chain?

The analogy does not fit **for the same reasons that FOSS is a moral imperative**!

Physical objects are hard to store, move, copy, modify and reinstall.

FOSS is *trivially* stored, moved, copied, modified and reinstalled.

Who Cares about a Software Supply Chain, Then?

Who Cares about a Software Supply Chain, Then?

Manufacturers and firms who **want to make proprietary software** who seek to punish (for financial gain) any consumers who share their software in the **same way the laws of physics "punish" us by making it hard to move physical items around the world.**

The Bill of Materials Is About Physical Objects

SBOM, like any cute marketing term, favors form over function.

SBOM Has No Formal Definition

As a marketing term, SBOM lacks specificity, which we should use to our advantage as activists.

CRA Does Not Mandate a Format

There are competing SBOM format standards.

The CRA probably says the most about SBOMs of any regulation in the world …

… but it mentions it only a few times and rather vaguely.

& CRA implementation regulations are still in flux.

“Market surveillance authorities should be able to request manufacturers … to submit the … SBOMs that they have generated pursuant to this Regulation. In order to protect the confidentiality of SBOMs, market surveillance authorities should submit relevant information about dependencies to ADCO in an anonymised and aggregated manner. ”

“[M]anufacturers should identify and document components contained in the products with digital elements, including by drawing up an SBOM. … Manufacturers should not be obliged to make the SBOM public.”

“Implementing powers should be conferred on the Commission to … specify the format and elements of the SBOM … ”

The Biden EO is Moot

You may have heard there has been a regime change in my homeland.

The Biden EOs are being rescinded and/or ignored.

There is **no law in the USA that mandates SBOMs**.

At least as long as we remain a Republic, **executive orders do not have the force of law** by themselves.

We Still Shouldn't Ignore SBOMs

Despite there being no actual mandate, we shouldn't ignore SBOMs, because …

A Wise Lawyer Once Said

(heavily paraphrased)

Blessed are the list makers, for they shall inherit …
the …
bureaucracy … ?!?

This Probably Will Happen To You

Hopefully You Can Say

The Only Truly Valuable SBOM is …

The complete, corresponding source code including "scripts used to control compilation and installation of the executable" … and a verifiably reproducible build.

Everything after that is just making lists.

Follow-Up / Talk License

I have a keynote about another interesting topic tomorrow:

15:00 in Janson on SUN 2025-02-02

Please donate to become a Conservancy Sustainer:

https://sfconservancy.org/sustainer/