

## There are complexities associated with package versions.

SBOM guidance will need to reflect identification and versioning information that is consistent with the public "main" repository for that package. **CENSUS II: LESSON LEARNED**  The most widely used FOSS is developed by only a handful of contributors.

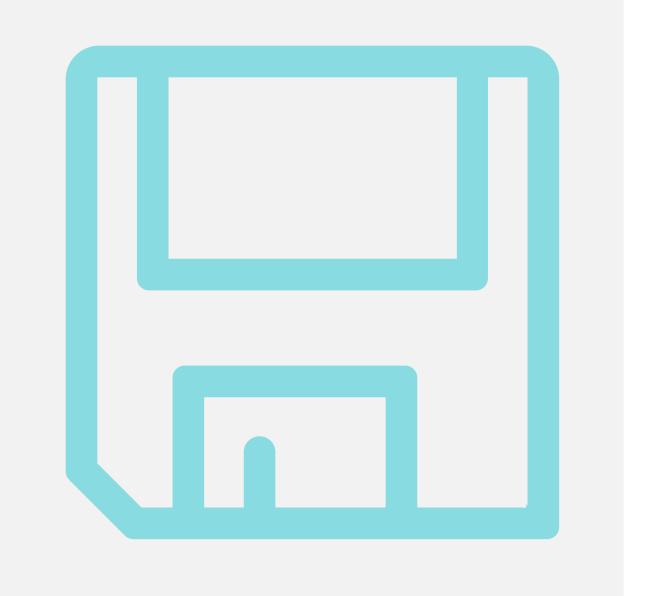
Results in one dataset show that 136 developers were responsible for more than 80% of the lines of code added to the top 50 packages.

CENSUS II: LESSON LEARNED



## The persistence of legacy software

in the open source space suggests that open source has not escaped the problem of legacy technology.



CENSUS II: LESSON LEARNED



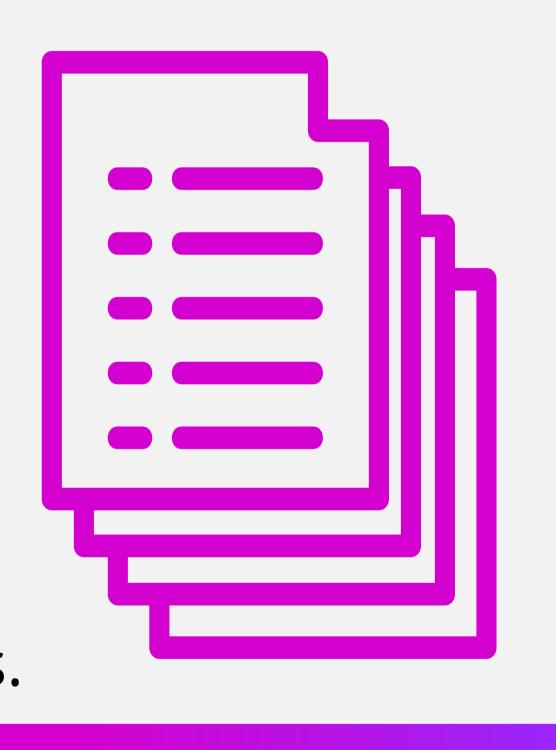
security companies were the basis of the Census II research effort.



**CENSUS II: METHODOLOGY** 

## The research generated eight top 500 lists,

a combination of versioned/ version-agnostic, direct/ indirect dependencies, and npm/non-npm hosted packages.



**CENSUS II: RESULTS** 



When considering npm, indirect & direct, version agnostic packages, the top used

debug.

When considering non-npm, indirect & direct, version agnostic packages, the top used package was the go package github.com/aws/aws-sdk-go.

CENSUS II: RESULTS



When considering npm, direct only, version agnostic packages, the top used package was lodash

**CENSUS II: RESULTS** 



log4j showed up as number 38

in the non-npm, direct, version-agnostic packages list.

**CENSUS II: RESULTS** 





