Legal Issues for FOSS-based Supply Chain Management

Herve Guyomard, Black Duck Software

Agenda

- Legal Case in Supply Chain
- Open Source in Mobile
- Mobile devices
- Supply Chain Management
- Summary

Recent Legal Example: Open Source in the Electronic Industry Supply Chain

BusyBox

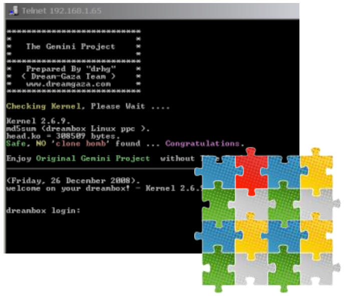
Popular utility **uses the GPLv2 license**

GCI TECHNOLOGIES
GEMINI • CORTEX • iKEY

COMTREND
Leading the Communication Trend

WD Western Digital®

Device OEMs **embedded the code in components**



```
Telnet 192.168.1.65
****************************
*                          *
*   The Gemini Project     *
*                          *
****************************
*   Prepared By "drhg"     *
*  ( Dream-Gaza Team )     *
*   www.dreamgaza.com      *
****************************

Checking Kernel, Please Wait ....

Kernel 2.6.9.
md5sum (dreambox Linux ppc ).
head.ko = 308509 bytes.
Safe, NO 'clone bomb' found ... Congratulations.

Enjoy Original Gemini Project  without

(Friday, 26 December 2008).
welcome on your dreambox! - Kernel 2.6.

dreambox login:
```

Westinghouse

JVC

HDTV manufacturers **used components in their products**

BEST BUY

Sold the HDTVs

SFLC sued 14 OEMs/retailers

Settlement: Westinghouse assessed monetary damages and legal fees, lost revenue due to injunction, and lost inventory (all HDTVs donated to charity).

“BusyBox” Current State

- 100s of companies have settled
- Court cases, dating back to 2009 are still pending
- Free Software Foundation (FSF) is still aggressively pursuing potential violators

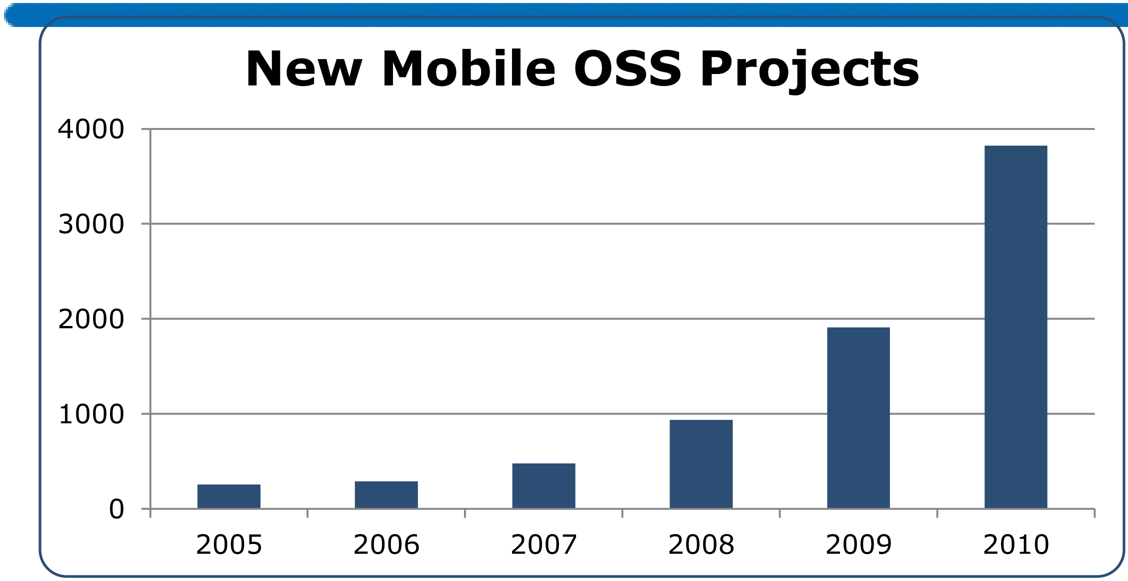
Ongoing Issues

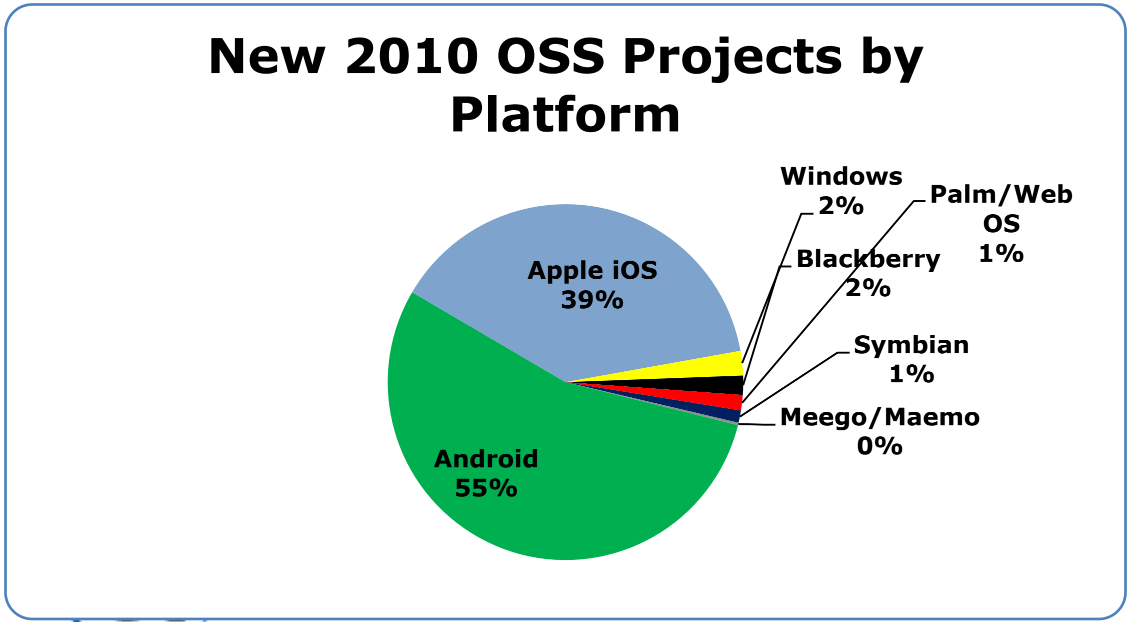
- Litigation as a means to settle open source disputes continues
  - Developers find advocates in influential groups such as the Free Software Foundation (FSF) and the Software Freedom Law Center (SFLC)
- Lawsuits
  - Not about monetary gain, but are about enforcing license obligations
- SFLC strategy
  - The SFLC has taken on a number of open source cases, all pro-bono, with the hope of setting in motion a new paradigm of awareness and compliance

Agenda

- Legal Case in Supply Chain
- Open Source in Mobile
- Mobile devices
- Supply Chain Management
- Summary

Open Source Drives Mobile Innovation



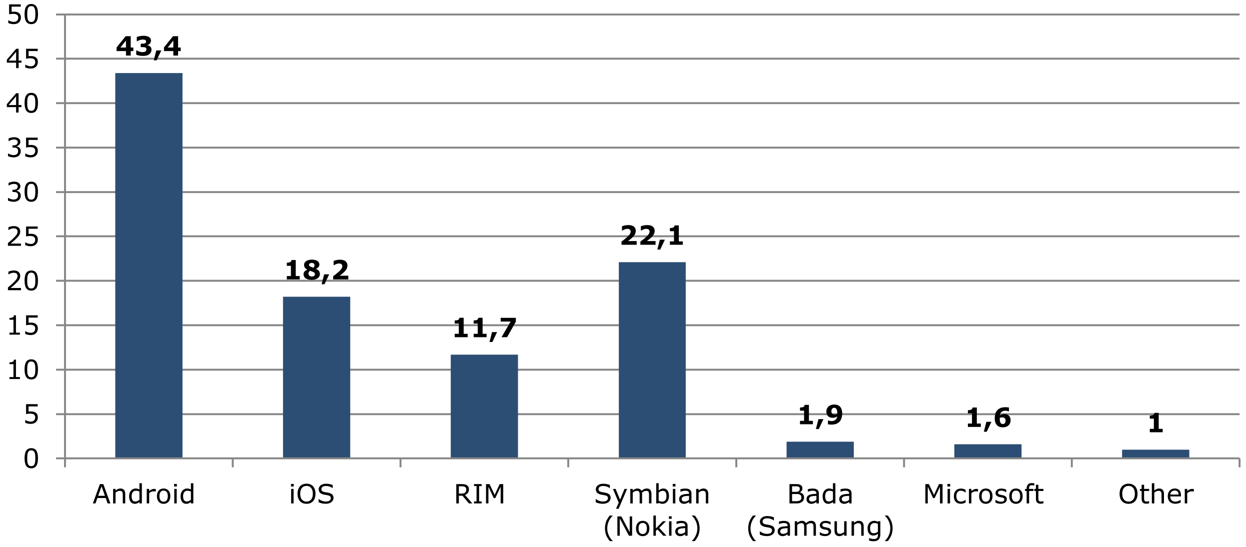


- Over 3,800 new OSS projects in 2010, doubling each of the last 3 years
- 94% of new projects that specify a platform are targeting Android and Apple/iOS
- Open source has redefined the mobile industry and is spreading far beyond

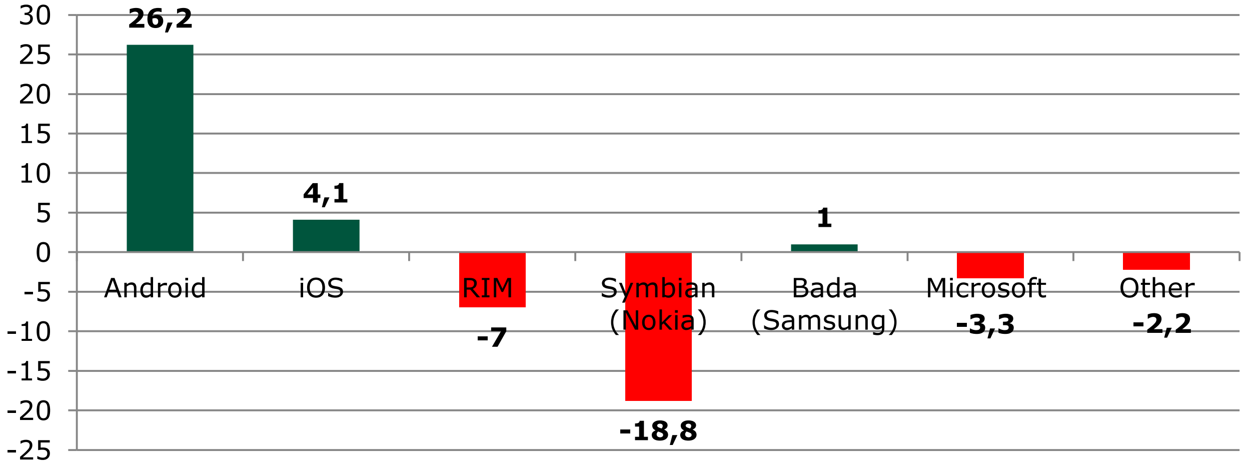
Know Your Code.

Open Source is a Large, Growing Opportunity

O/S Market Share: Q2 2011



Share Gain (Loss) 2010 to 2011



- 428.7 million units
- 16.5% growth form Q2 ’10

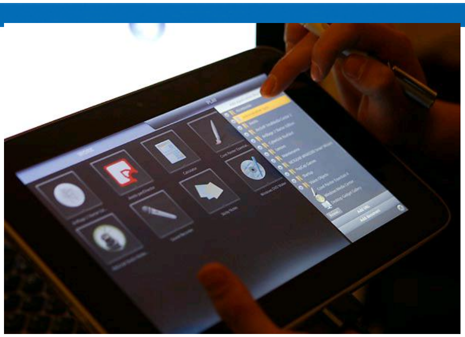
Source: Gartner , August 2011

Know Your Code.

Open Source Devices: Phones, Tablets, eReaders, TVs, Autos, more…..

Automobile: Android powered SaaB

Barnes & Noble Nook



Lenovo LePad

Droid 3 by Motorola

Samsung Galaxy

Dell Streak

Motorola Xoom

HTC Evo Shift

Sony Internet TV

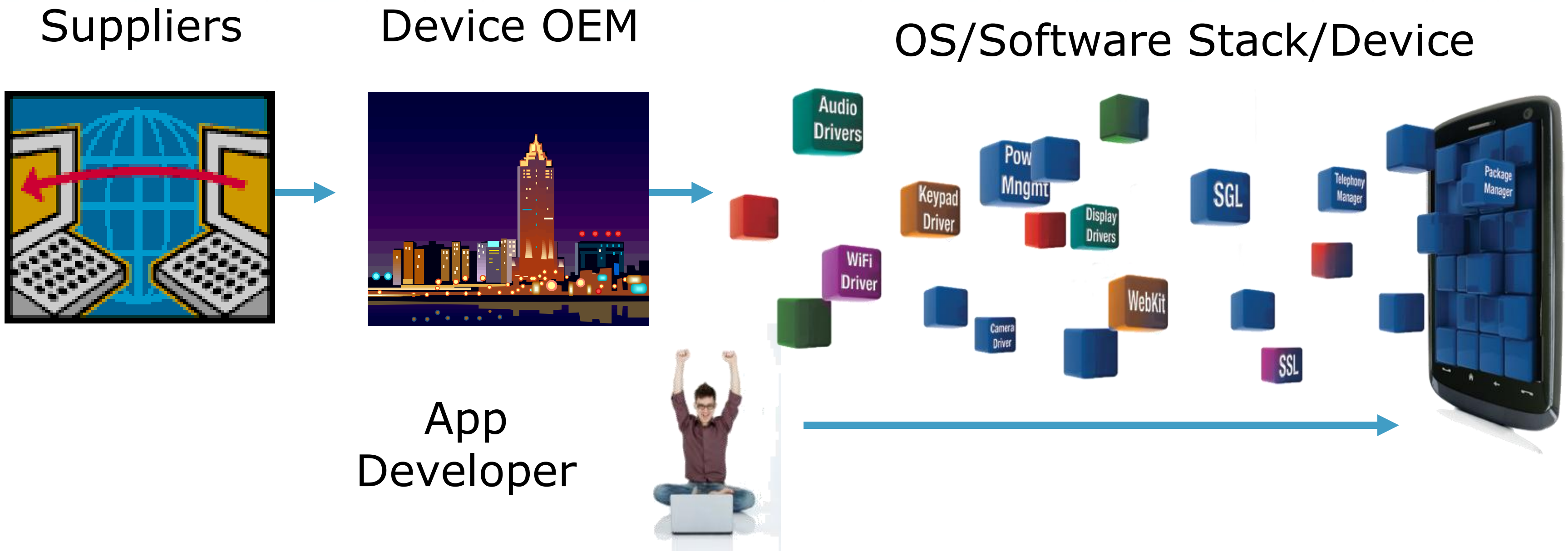
Panasonic Toughbook

HP Touchpad (?)

blackduck

Know Your Code.

Managing OSS in the Mobile Ecosystem and Software Supply Chain



Suppliers

Device OEM

OS/Software Stack/Device

App Developer

Typical Smartphone has over 300 components

- *Corporate-Owned IP*
- *Proprietary/Licensed IP*
- *FOSS*
- *Outsourced development*
- *Multi-level supply chains*

- *Security*
- *Networking*
- *Email*
- *Graphics*
- *Database*
- *Web Services*
- *Many more…*

Agenda

- Legal Case in Supply Chain
- Open Source in Mobile
- Mobile devices
- Supply Chain Management
- Summary

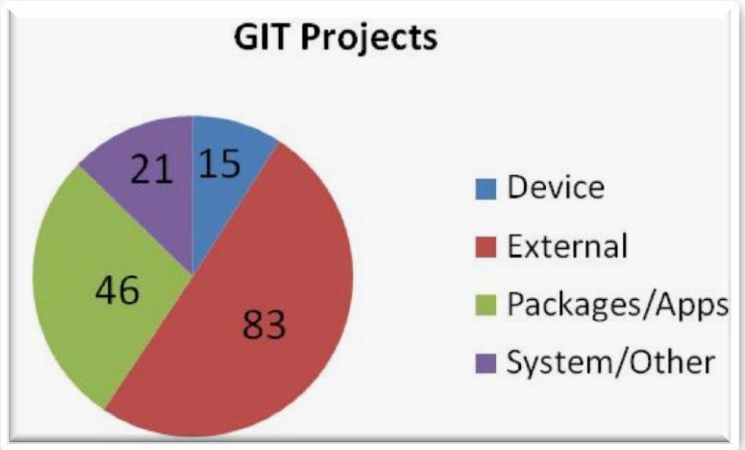
Complexity for Device Manufacturers

- Components and code from many suppliers
- Need to control and manage building software on a rapidly changing O/S
  - Multiple releases per year
- Customize Android for:
  - The type of device (phone, tablet, TV, etc.)
    - Device drivers, power consumption, etc.
  - User experience
- Do it all while ensuring compliance

What’s Inside Android?

Android

- 165 Projects
  - 83 are “External”
  - Does not include Kernel Mirror
- Total Size
  - Over 80,000 Files
  - Over 2GB total size
  - Does not include Kernel Mirror



A Look Inside Two Android Components: Bionic & Webkit

License types in: Bionic

BSD 2.0*
CMU License
Cryptix License
Free clause
FreeBSD
Historical free
INRIA OSL
Intel OSL
Internet Software Consortium
MIT
Public Domain
Python InfoSeek
X.Net License

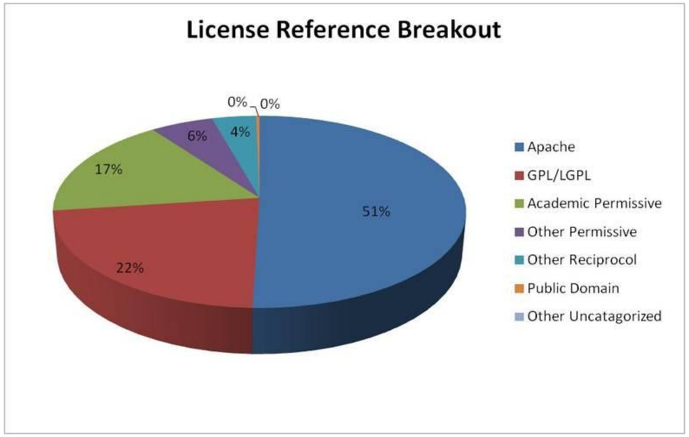
License types in: Webkit

BSD 2.0
David M. Gay License
GPL 2.0
ICU License
LGPL 2.1*
MIT License V2
MIT v2 with Ad Clause License
Mozilla Public License 1.1
PCRE License
Public Domain
SWIG License
The wxWindows Library License
zlib/libpng License

***Declared license**

Android's Composition

- Licenses
  - Declared license: Apache 2.0
  - Components reference 19 different licenses
  - External components
    - Linux, Webkit use reciprocal licenses (GPLv2, LGPL)
  - Other components: more than 30 of them use reciprocal licenses (GPL, LGPL, CPL, etc.)
    - e.g. dbus, grub, emma, e2fsprogs, bluez, Bison
  - Non-OSI approved licenses are used, including OpenSSL and Bzip2



Obligations and Misperceptions

- No “small device” exceptions
- Must provide source for the specific device
- Compliance is required by every vendor that ships the platform
- There is no “downstream defense for upstream” violations

Agenda

- Legal Case in Supply Chain
- Open Source in Mobile
- Mobile devices
- Supply Chain Management
- Summary

Software Supply Chain Management

- Open source is typically outside of normal commercial s/w procurement processes
- The Challenges
  - An increasingly diverse and distributed set of development resources
    - Internal teams
    - Commercial software vendors
    - Outsourcers
    - Open source communities
  - Little/no visibility into the origins of the software

Supply Chain Comparison: Hardware vs Software

- Hardware supply chain techniques
  - ERP systems brought together different users and processes
  - Workflow automates task creation
    - Notifications
    - Process Monitoring
  - Central repositories of data
  - Business Process Integration is the key
- Technology companies have software supply chains
- Software products have bills of materials (BOM’s)

The Golden Rule for Proper Software Supply Chain Management

Treat the management of open source software as an integrated, cross functional **business process**, and not simply as a development process.

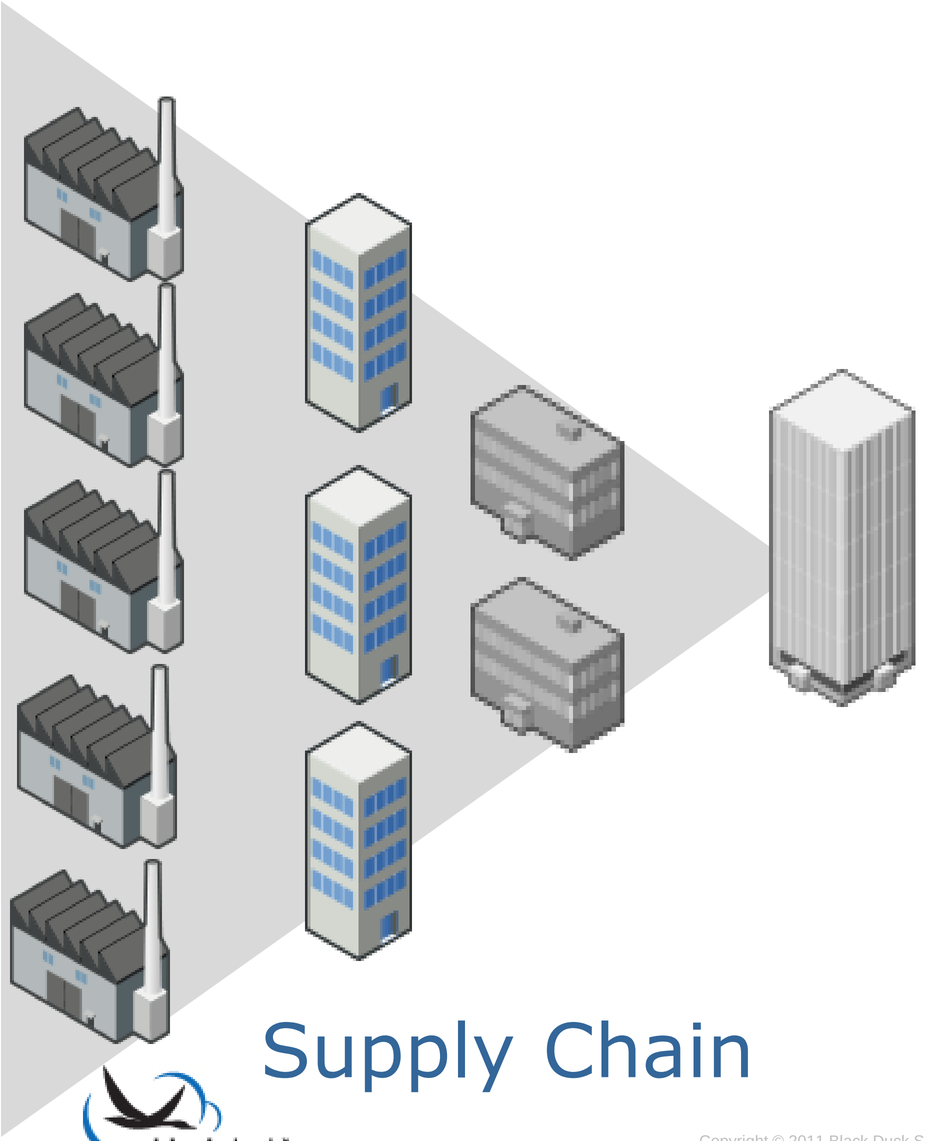
blackduck

Know Your Code.

Supply Chain Program Elements

1. Published Policy
2. Open Source Process Owner
3. Approval Processes
4. Monitoring & Tracking Process
5. Obligation Verification Process

Compliance in a Supply Chain is a Challenge



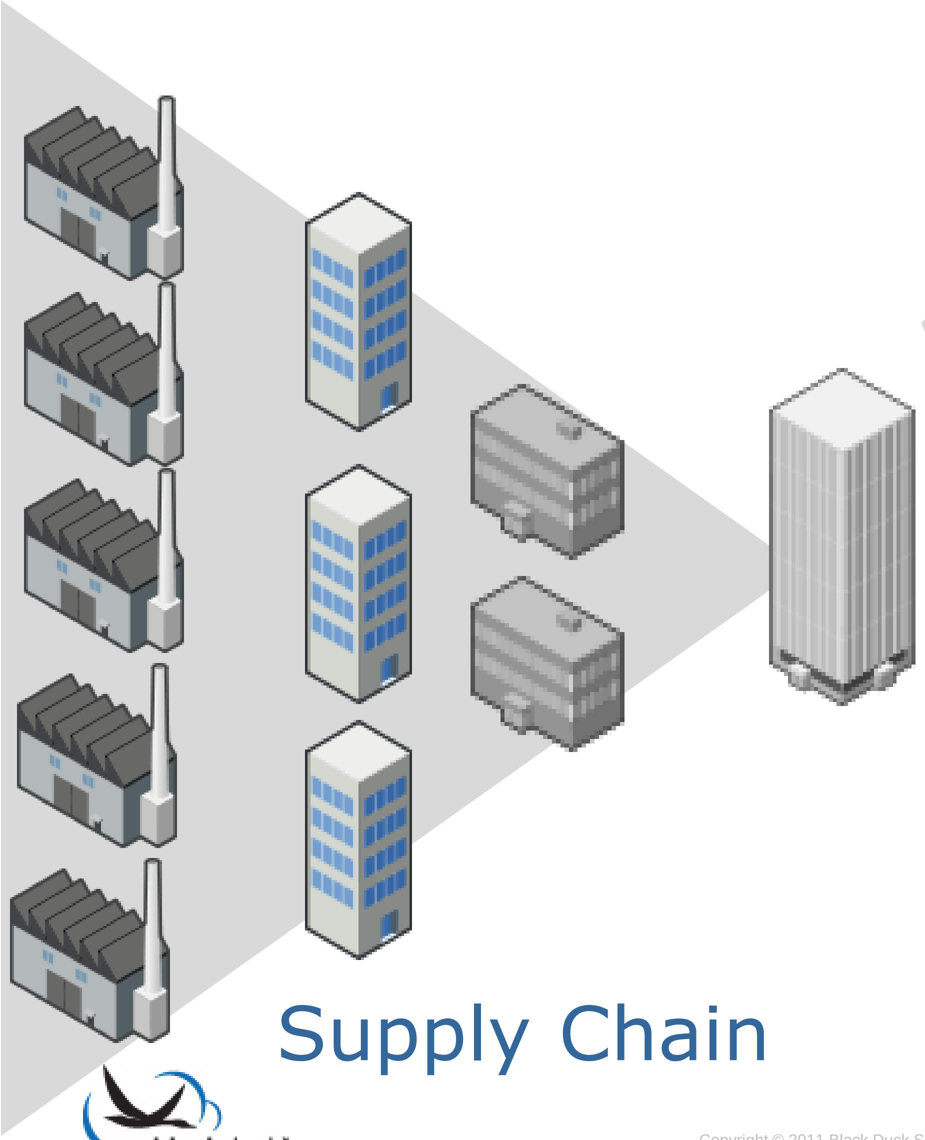
One Product =

Many Suppliers

Many OSS Packages

Many OSS Licenses

In Supply Chains SPDX™ Can Help

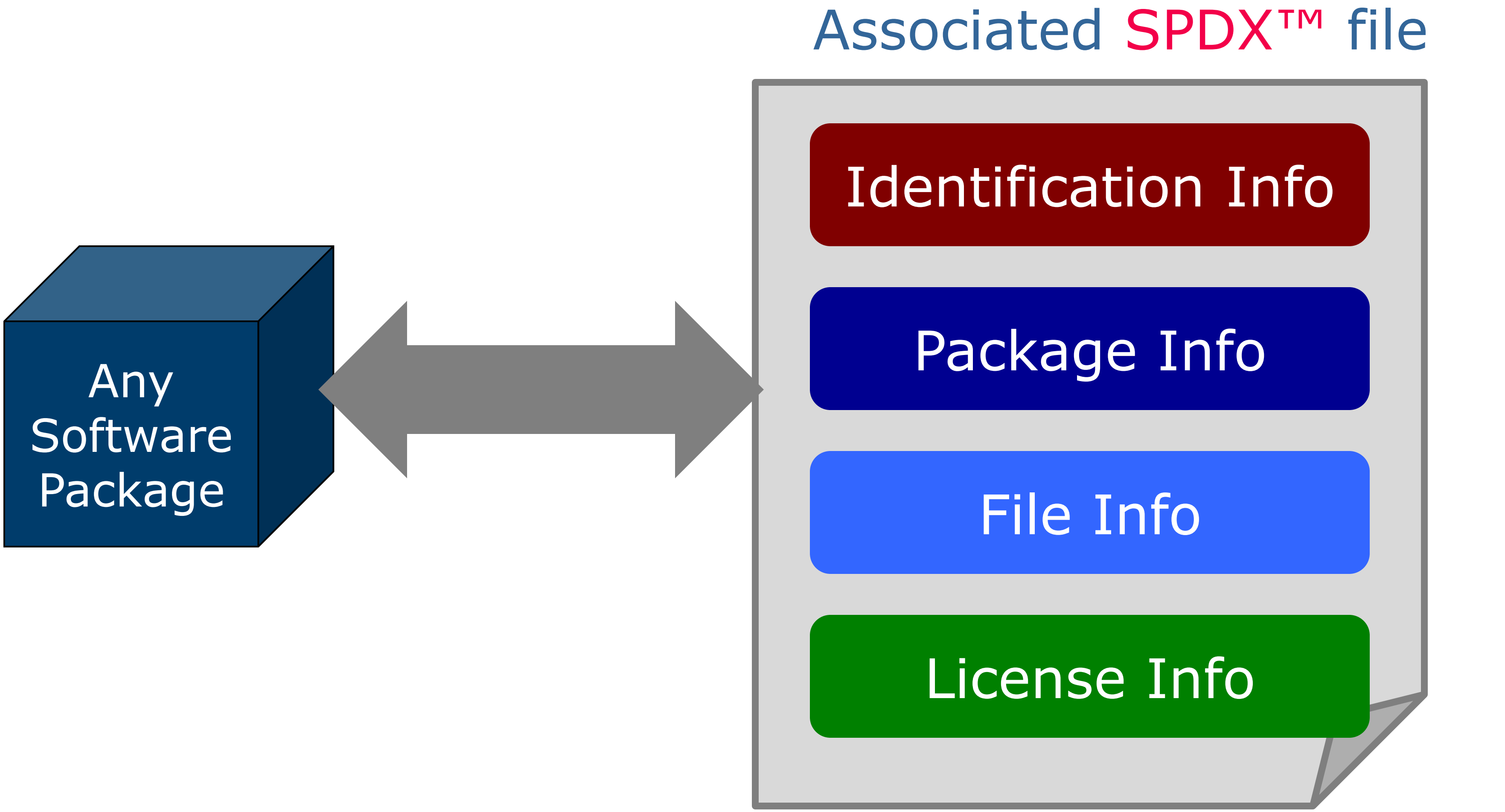


A standard format for communicating a software Bill of Materials across the supply chain.

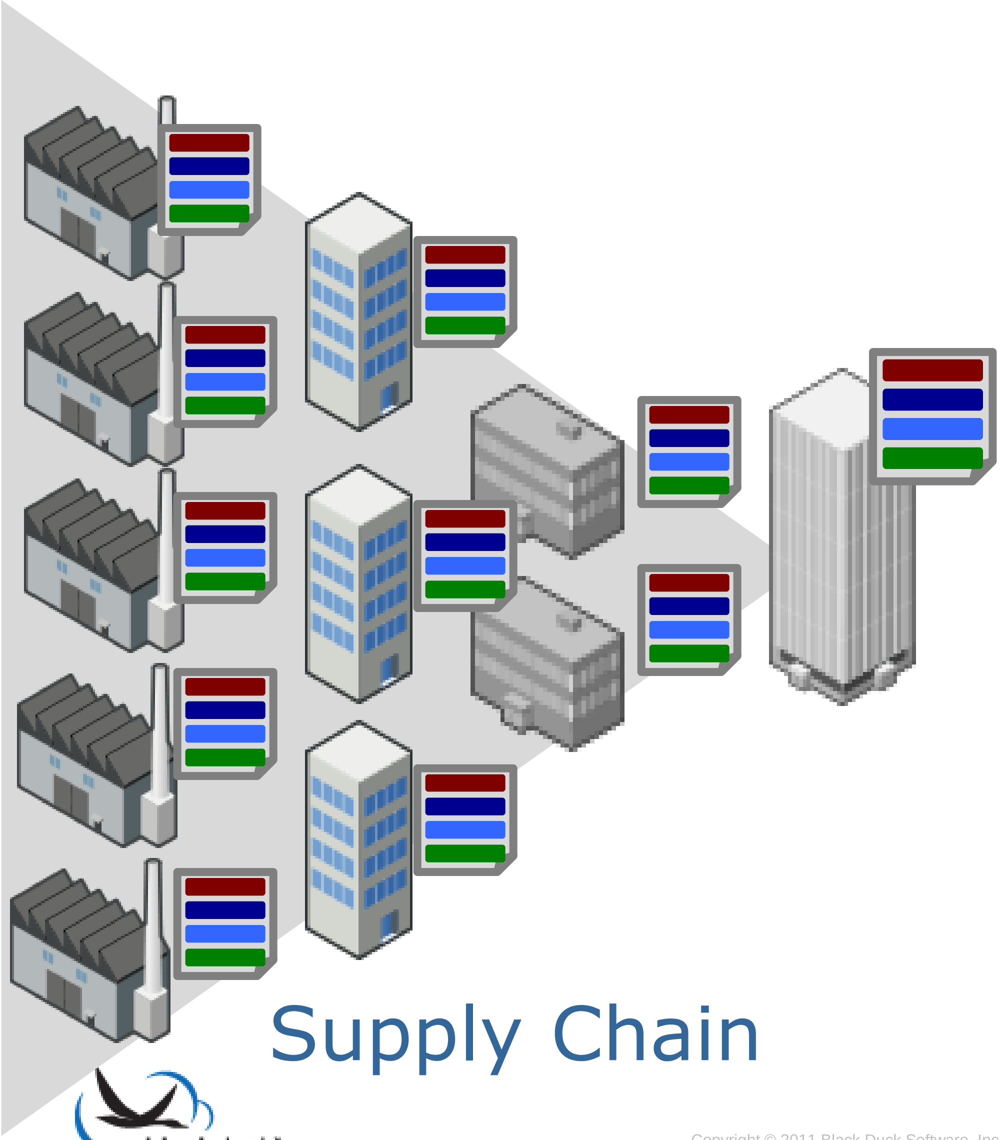
Software Package Data Exchange™ (SPDX™)

- Working group under Linux Foundation
- Charter:
  - Create data exchange standards to enable license and component information sharing (metadata)
- Participation from organizations including software, systems and tool vendors, consultants and foundations

SPDX™ File = Software BOM



SPDX Benefits



Supply Chain

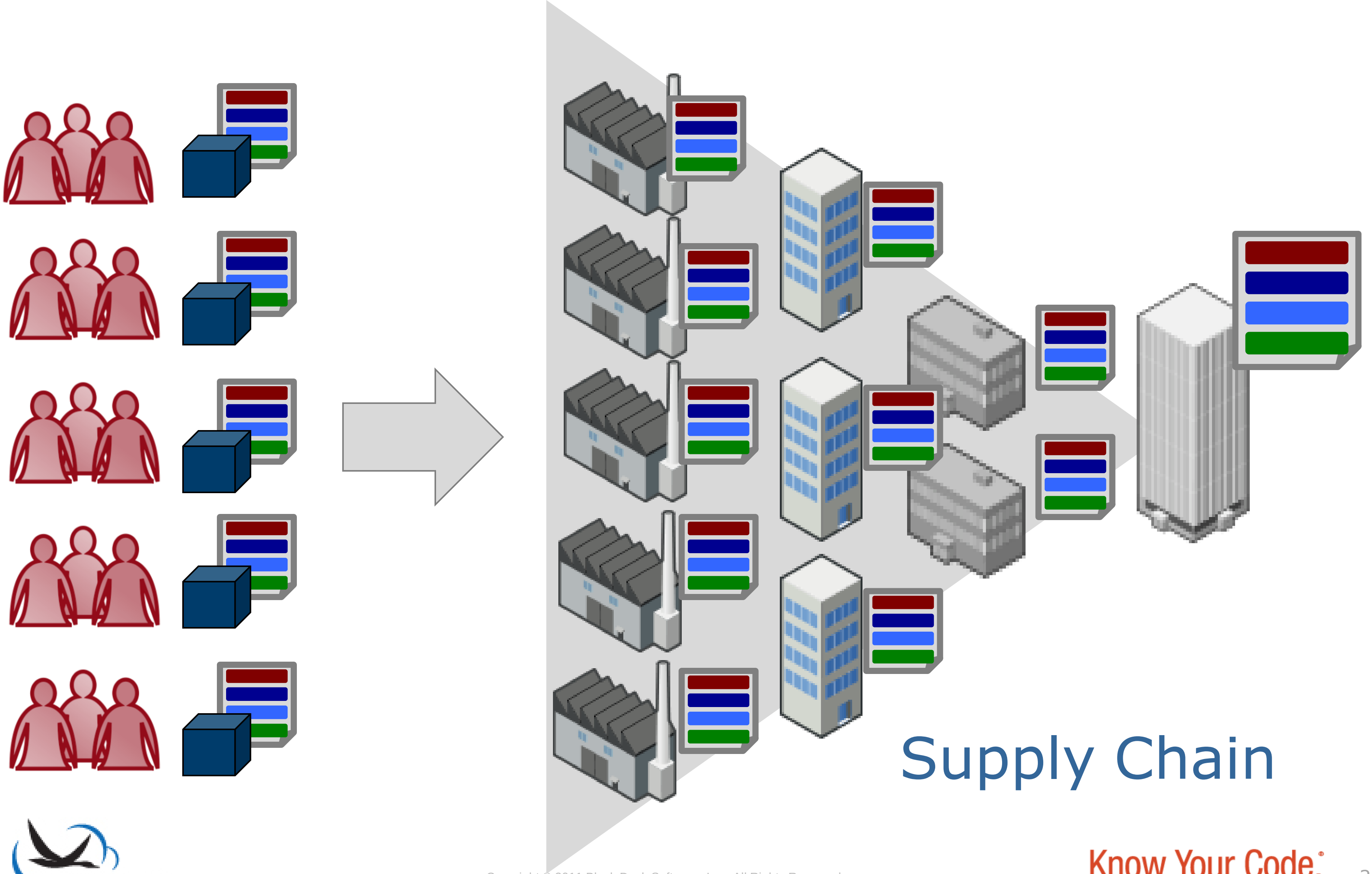
Benefits

Reduce effort

Reuse analysis

Improve compliance

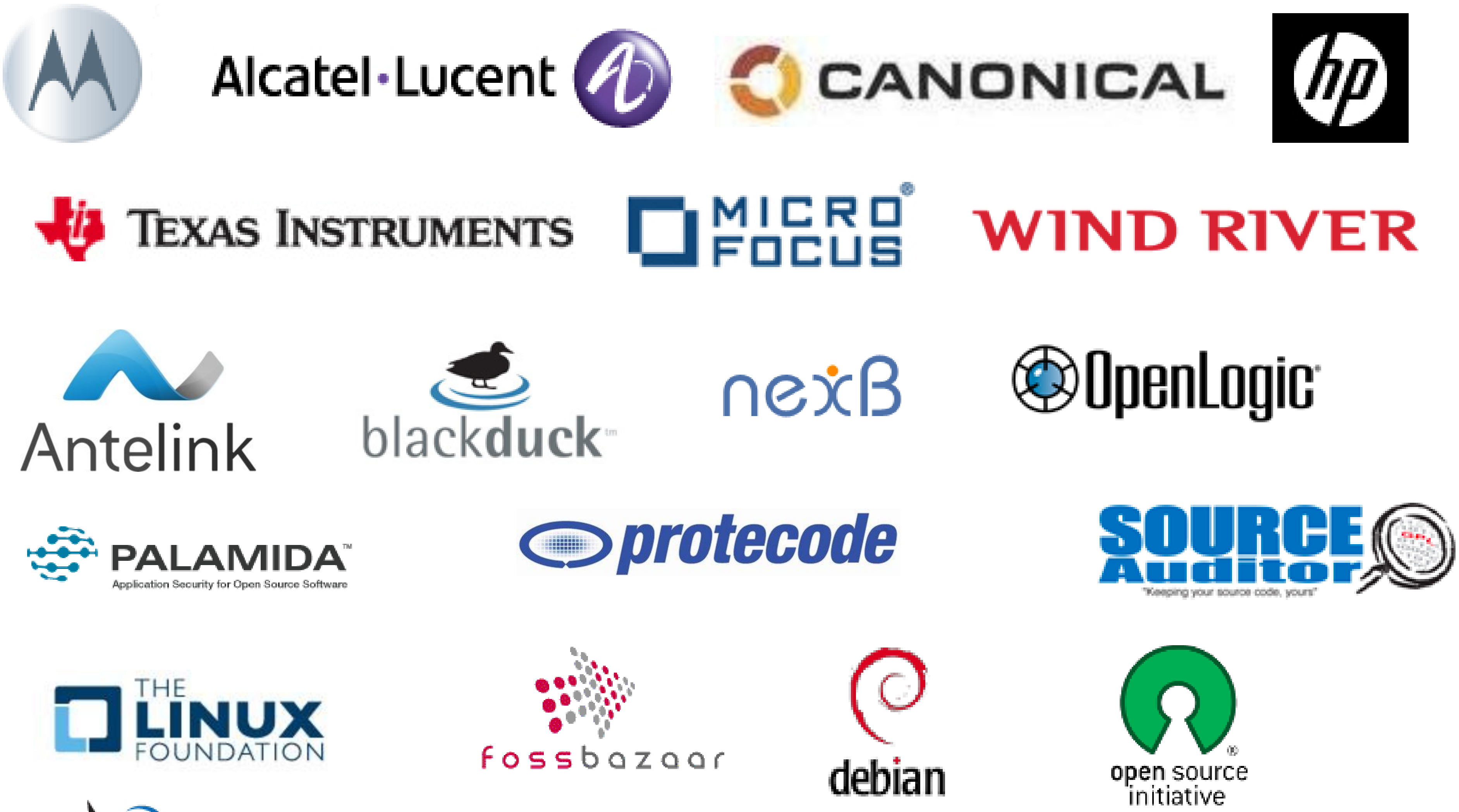
Communities Can Use SPDX™



Summary

- Open source has revolutionized the mobile and device landscape, other industries will follow
- Supply chain management techniques from hardware are useful for managing software
- “SPDX is a crucial building block in an industry-wide system of automated license compliance administration” Eben Moglen
- Effective management and control requires training, tools, processes and standards

Broad Participation



Thanks!

- Questions?

Herve Guyomard

Black Duck Software

hguyomard@blackducksoftware.com