

Overview of Open Source Software Risks and Best Practices for Compliance

David Greenberg | greenbergdm@gtlaw.com | 212.801.6545
Sandy Chiu | chiu@gtlaw.com | 305.579.0558

JULY 28, 2020

www.gtlaw.com

Speakers



David Greenberg
Shareholder, New York



Sandy Chiu
Associate, Miami & New York

Agenda

- Overview
- History and Philosophy: Free and Open Source Software
- Open Source Licenses
- Enforcement
- Best Practices

A low-angle, upward-looking perspective of several modern skyscrapers. The buildings are characterized by repetitive horizontal window patterns and are arranged in a way that creates a sense of height and scale. The sky is a clear, vibrant blue, punctuated by soft, white cumulus clouds. The overall composition is symmetrical and dynamic, emphasizing architectural grandeur.

Overview

What is Open Source?

- No legal definition
- Made widely available in source code form for no charge under a license that allows for use, modification, and distribution by the public under certain terms and conditions.
 - Often developed in collaboration with many parties, i.e., community-based development
 - Developers make improvements, bug-fixes and may provide back to the community
 - Licenses are enforceable!
- Open source is NOT:
 - Public domain
 - “Freeware” (e.g., Adobe PDF reader)
 - Free of costs or conditions
- Free

Open Source-Based Companies and Products



Advantages to Open Source

Why use Open Source?

Quality of Solutions

Competitive Features
and Technical Capabilities

Ability to Customize & Fix

Top 3 OS Technology Areas?

Operating Systems

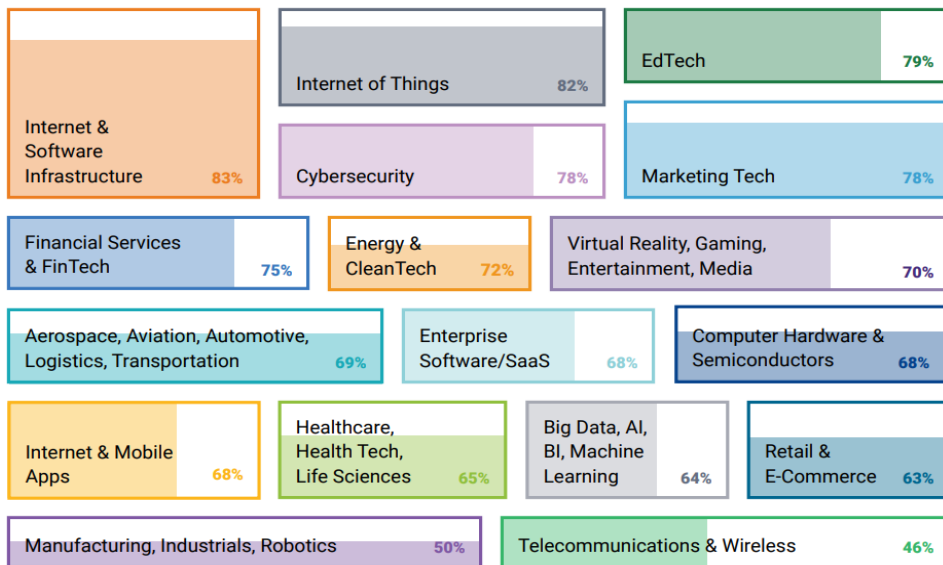
Database

Development Tools

Utilization Rates - 2020

Industries represented in the 2020 OSSRA report

Percentage reflects amount of open source in codebases by industry



Source – Black Duck (Synopsis) 2020 Open Source Security and Risk Analysis (OSSRA) Report. Percentage reflects amount of open source in codebases by industry.



History and Philosophy: Free and Open Source Software

Types of Code – Source Code vs. Object Code

```
#include  
<stdio.h>  
int main()  
{  
    printf("Hello")  
;  
    return 0;  
}
```

Source Code
("human readable")



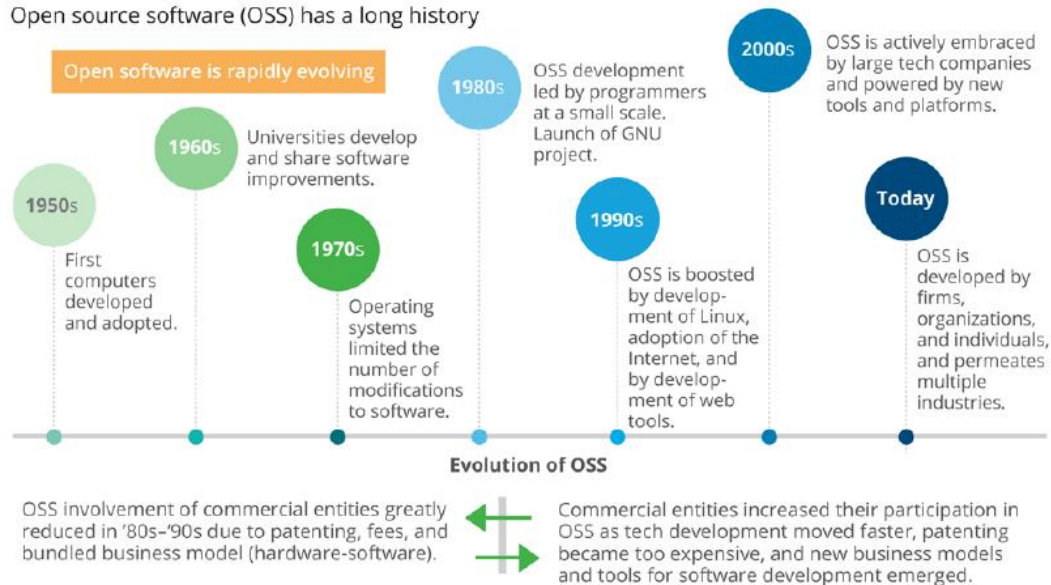
```
100010101010101  
000100101010111  
011111100110000  
001011001101010  
010111011100011  
011111001111000  
000110011110101  
010010010101000
```

Object Code
(binary)

Open Source Timeline

Figure 2. History of open source

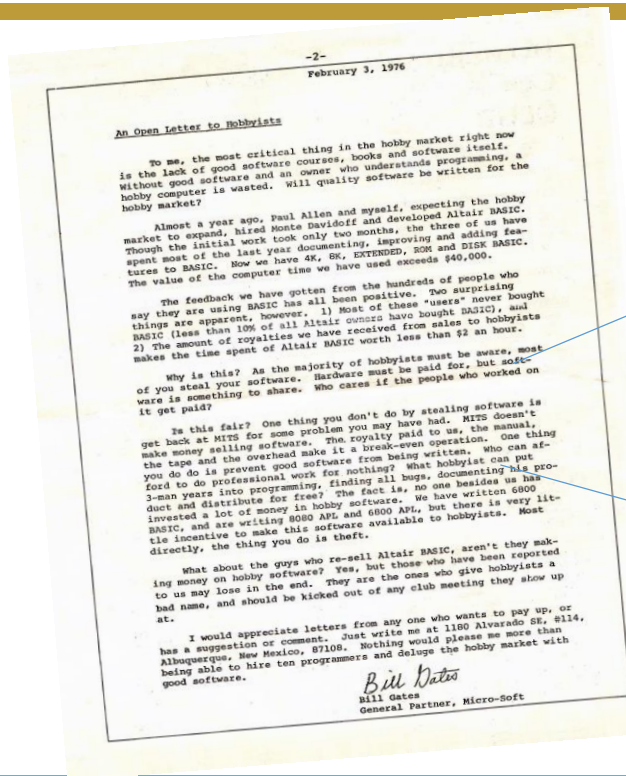
Open source software (OSS) has a long history



Source: Longsight, available at <https://www.longsight.com/learning-center/history-open-source>, accessed September 12, 2017.

Deloitte Insights | deloitte.com/insights

February 1976 – Letter to Hobbyists



"As a majority of hobbyists must be aware, most of you steal your software."

"One thing that you do is prevent good software from being written. Who can afford to do professional work for nothing?"

Traditional Software – Closed Source

- “Traditional” Software Development and Licensing =
Closed Source
 - Private development and methodology
 - Restrictive license terms
 - Fee for license to software
 - Software provider can address any issues



OSS: Two Schools of Thought

1. Free Software Foundation (FSF) [1985]



Richard Stallman, Founder

Author of GNU Operating System

“GNU” = GNU, not UNIX



OSS: Two Schools of Thought

1. Free Software Foundation (FSF) [1985]



- 4 Essential Freedoms:

1. Freedom 0 – Freedom to run the program, for any purpose
2. Freedom 1 – Freedom to study how the program works and to change it (access to source code)
3. Freedom 2 – Freedom to redistribute copies to help others
4. Freedom 3 – Freedom to distribute copies of your modified versions to others

OSS: Two Schools of Thought

1. Free Software Foundation (FSF) [1985]



- 4 Essential Freedoms:

1. Freedom 0 – Freedom to run the program, for any purpose
2. Freedom 1 – Freedom to study how the program works and to change it (access to source code)
3. Freedom 2 – Freedom to redistribute copies to help others
4. Freedom 3 – Freedom to distribute copies of your modified versions to others



2. Open Source Initiative (OSI) [1998]



- Encourages sharing and collaborative improvement of software source code
- Belief – better result from using open-source development methodologies than closed

Open Source Initiative Licenses

- OSI Definition of Open Source Licenses: <https://opensource.org/osd>
- OSI Definition
 - Must allow free redistribution
 - No royalties
 - Must make source code available
 - Must allow derivative works
 - Allow all – no discrimination against people, groups, fields
 - Must be non-product specific and technology neutral
- Note: Open source projects are not bound to this, or any, definition. FSF's definition is different.

A low-angle, upward-looking perspective of several modern skyscrapers. The buildings are characterized by repetitive horizontal window patterns and are arranged in a way that creates a sense of height and scale. The sky is a clear, vibrant blue, punctuated by soft, white cumulus clouds. The overall composition is symmetrical and geometric, emphasizing the architectural lines of the buildings.

Open Source Licenses

2 Categories of OSS Licenses – General Attributes

- **Permissive / Attribution Licenses:**

- May add restrictions
- If modifications are made, these can be made available as open source software or proprietary software
- Attribution is often required

- **Copyleft Licenses:**

- If you distribute object code, you must provide source code
- If you distribute, you must use the same license as the underlying open source component license
- If you engage in development and distribute modifications, source code for modifications must be made available [“viral” impact]
- You must be free to use and modify without restrictions



Copyleft Sub-Categories: Strong vs. Weak

- **Strong Copyleft** – copyleft license provisions are imposed on all derived works. E.g.,
 - GPL v2
 - GPL v3
 - AGPLv3
- **Weak Copyleft** – In certain instances, derivative works inherit the copyleft license. E.g.,
 - LGPL
 - Mozilla Public License (MPL)
 - Eclipse Public License (EPL)

OSS License Usage

- As of 2019, the most commonly used licensees are NOT copyleft licenses
 - Permissive/Attribution licenses (~52%)
 - MIT (~32%)
 - Apache (~14%)
 - BSD (~6%)
 - GPL family of licenses [GPL, LGPL, AGPL] (~32%)
 - GPL v2 (~18%)
 - GPL v3 (~7%)
 - LGPL v2 (~4%)
 - LGPL v3 (~2%)
 - AGPL (~1%)

Source: Black Duck KnowledgeBase

Permissive License Example – BSD-3

Note: This license has also been called the "New BSD License" or "Modified BSD License". See also the [2-clause BSD License](#).

Copyright <YEAR> <COPYRIGHT HOLDER>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



Distribution (also “Conveyance”)

- GPL v2 - Paragraph 2(b) – You must cause any work that you **distribute or publish**, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to third parties under the terms of this license”
- GPLv3 – GPL v3 Paragraph 6 imposes obligations to provide “Corresponding Source” if you “**convey**” a work in object form format. [Terminology switches from “distribute” to “convey” but same principles apply.]

What is Distribution?

- Providing copies to customers?
- Incorporating open source into client-side code downloaded to user's browser?
- Employees?
- SaaS offering?
- Affiliates?
- JV with minority interest?

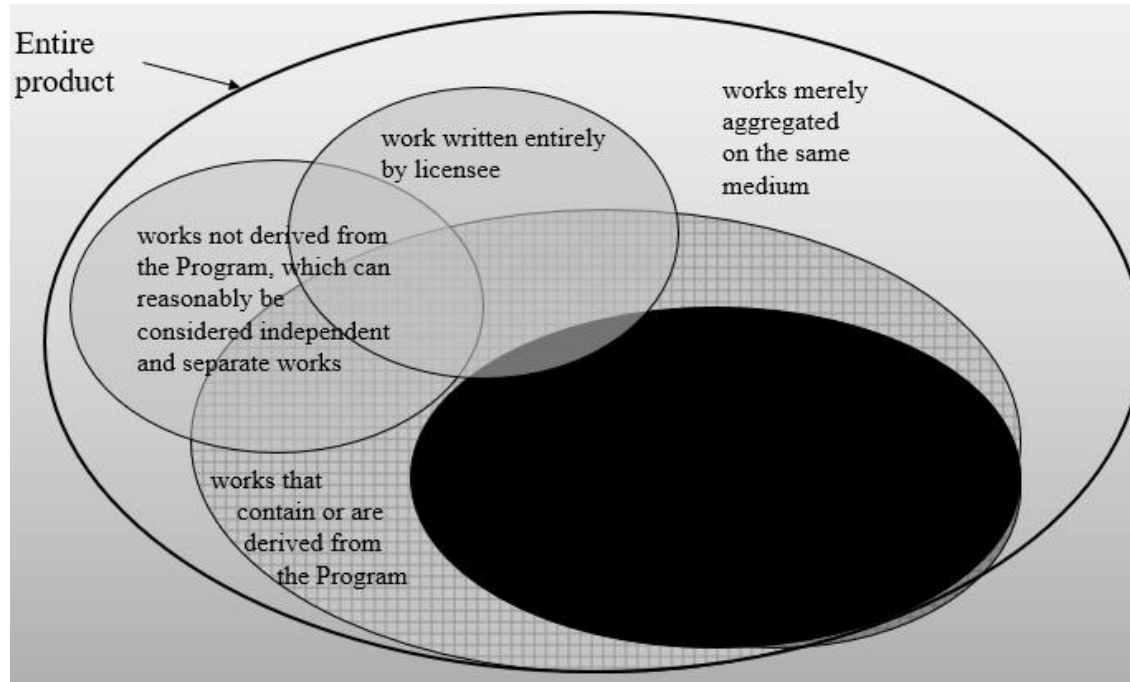
What is Distribution?

- Providing tangible copies to customers? **YES**
- Incorporating open source into client-side code downloaded to user's browser? **YES**
- Employees? **NO**
- SaaS offering? **NO**
- Affiliates? **Probably Not**
- JV with minority interest? **Probably Yes**

“Modifications” vs. Mere Aggregation

- Many obligations are triggered by a “modification” but this can mean more than simply making code changes to licensed OSS component
- GPL v2: Paragraph 0 – (“Program” and “Works Based on the Program” are in-scope)
 - “This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “**Program**”, below, refers to any such program or work, and a “**work based on the Program**” means *either*
 1. *the Program or*
 2. *any derivative work under copyright law*: that is to say,
 3. a work *containing the Program or a portion of it*, either verbatim or
 4. *with modifications and/or translated into another language.*”
- GPL v2: Paragraph 2 – (Works not derived or independent and separate are out-of-scope)
 - If identifiable sections of that work are *not derived from the Program*, and can be reasonably considered *independent and separate works* in themselves, then this License, and its terms, *do not apply* to those sections when you distribute them as separate works.
 - It is not the intent of this section to claim rights or contest your rights to *work written entirely by you*; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program
- GPL v3 – Same issue but terminology changes to “modified versions” versus “mere aggregation”

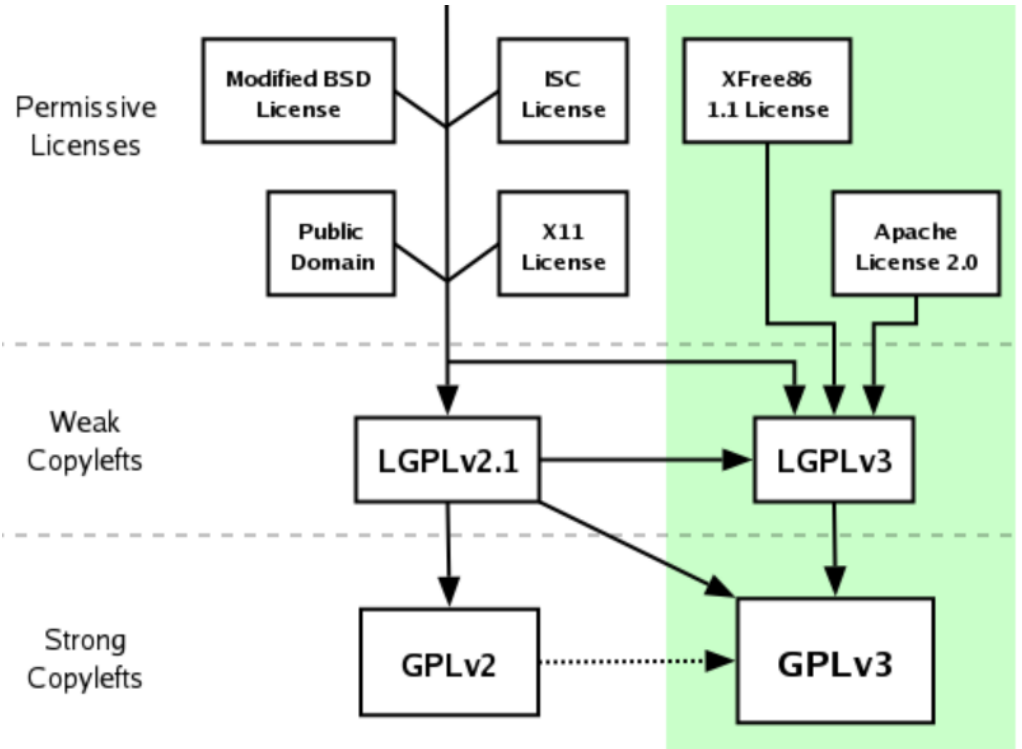
Boundary Issues: Modifications vs. Aggregation?



Source Code Delivery and Notices

- Generally, under GPL, if there is **modification + distribution** of “covered work” (not mere aggregation), must **provide complete corresponding source** or **provide offer**
- Open Source License Notice + Offer
 - How/where to provide license information
 - Embedded licenses
 - Hyperlinks within standard license agreement or license file (mobile app)
 - Package vs. individual component level information

Incompatibility



Patent Grant Provisions

- Certain OSS license require that as a condition of use, you grant others a patent license:
 - Newer OSS licenses (GPLv3, Apache 2.0, EPL, and MPL) contain explicit patent license
 - Older licenses (GPLv2, LGPLv2, BSD, and MIT) contain implied licenses
- If Company has a patent that reads on OSS software that it distributes, it may be **granting a royalty-free license** under its patents:
 - License may limited to modifications that **you** make
 - Or, may extend to any software that includes the OSS component or **is a modification or derivative work by a recipient or downstream user**
 - Some cover existing patents but at times license grant goes to **future patents**.
 - Defensive termination provisions

A low-angle, upward-looking perspective of several modern skyscrapers. The buildings are characterized by repetitive horizontal window patterns and are arranged in a way that creates a sense of height and scale. The sky is a clear, vibrant blue, punctuated by soft, white cumulus clouds. The overall composition is symmetrical and geometric, emphasizing the architectural lines of the buildings.

Enforcement

Risks

- Major Risks Include:
 - Copyright infringement
 - Injunction (orders halting production distribution)
 - Bad PR
 - Adverse impact to patent portfolios
 - Engineer relations issues
- Unlikely to include court orders to disclose source code



Enforcement Landscape



- Enforcers: open source communities, specific individuals, gpl-violations.org, copyright trolls
- Litigation:
 - **VMware.** Christoph Hellwig filed suit against VMware in March 2015 in Germany for not making modified GPL code (alleged combined work) available in source code. FSF supported Hellwig.
 - **BusyBox cases.** 12 distributors of GPL BusyBox software suite were sued (2007-2010) for distributing BusyBox binaries without providing its source code. Distributors included Verizon, Best Buy, JVC, Samsung, Westinghouse. Most parties settled and agreed to comply with LGPL/GPL.

A low-angle, upward-looking perspective of several modern skyscrapers. The buildings are characterized by repetitive horizontal window patterns and are arranged in a way that creates a sense of height and scale. The sky is a clear, vibrant blue, punctuated by soft, white cumulus clouds. The overall composition is symmetrical and dynamic, emphasizing architectural grandeur.

Best Practices

Open Source Policies

- Benefits:
 - Guidelines ensure the company is in agreement about how to use OSS
 - Increase efficiency
 - Maximize the benefit of OSS
 - Minimize the technical, legal, and business risks

Developing an Open Source Policy

1. Program administration and management
2. Discovery, acquisition and evaluation
3. Review and approval
4. Software procurement
5. Code and documentation management
6. Vulnerability remediation
7. License compliance
8. Community participation

Open Source – Quick Guide

	Low Risk	Medium Risk	High Risk
Distributed Modified in Products	BSD, MIT, Apache	Artistic, Eclipse	GPL, LGPL, MPL, CDDL
Distributed Unmodified	BSD, MIT, Apache, Artistic	GPL, LGPL, Mozilla (MPL), Eclipse	
Used in Hosted Software	Most others		AGPLv3, AFL – 3.0, OSL 3.0
Internal Use Only	Almost all		
Contributed Only	BSD, MIT		GPL, LGPL, MPL, Apache

Vendor Management

- OSS License Due Diligence
 - License compliance and security vulnerabilities
 - Important for 3rd party components that will be integrated into a distributed product
 - Request list of OSS components (Bill of Materials)
- Representations and Warranties
 - Require disclosure of all OSS used
 - Assurance that no copyleft obligations apply
 - No privacy or security risks
 - Compliance with laws
 - Ongoing compliance with OSS licenses

Open Source – Diligence Questionnaire

OSS Component	License and Version	Used with which Company Products?	Functionality of OSS Component?	Interaction w/ Product	Used “As is” or modified	Distributed?	Alternate/ Replacement Component Available?
[OSS Component 1]	[e.g., GPL v. 2.0]						
[OSS Component 2]							
[OSS Component 3]							
[OSS Component 4]							
[OSS Component 5, etc.]							

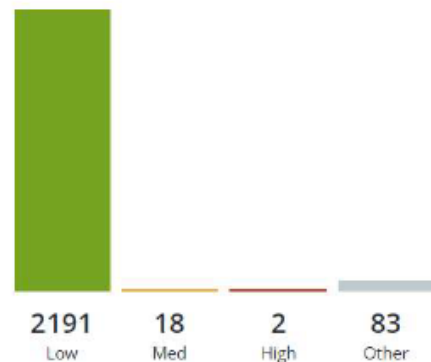
Code Scans



Open Source Report

Analysis Dashboard:

The following charts describe the overall risk disposition of the entire codebase:



License risk distribution chart



Vulnerability Severity distribution chart

Overview of Risk by Products:

The following table describes the risk distribution per project.

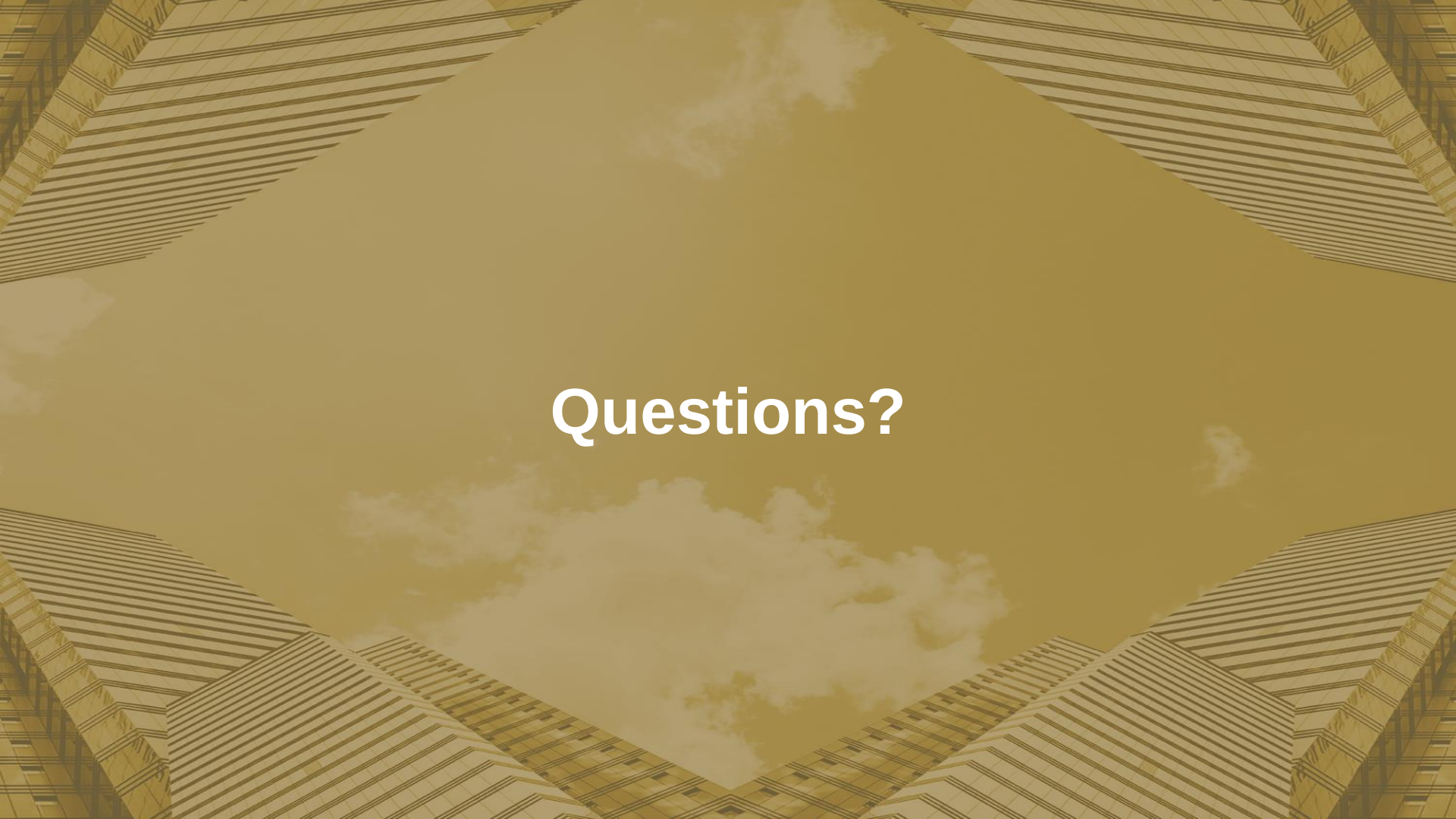
Product/Project	Libraries	Licenses	Security & Quality
Product 1	Total: 3, Direct: 1, Dependencies: 2	Total 1	No Security Vulnerabilities
		No Risky Licenses	1 Outdated Libraries
Product 2	Total: 186, Direct: 186, Dependencies: 0	Total 24	21 Security Vulnerabilities
		Higher Risks: LGPL 3.0 (2), LGPL 2.1 (1), Eclipse 1.0 (1), GPL 2.0 Classpath (1)	125 Outdated Libraries
Product 3	Total: 44, Direct: 18, Dependencies: 26	Total 10	3 Security Vulnerabilities
		Higher Risks: LGPL 3.0 (2)	12 Outdated Libraries
Productt 4	Total: 116, Direct: 116, Dependencies: 0	Total 9	5 Security Vulnerabilities
		Higher Risks: LGPL 3.0 (1)	74 Outdated Libraries

Open Source – Quick Guide

	Low Risk	Medium Risk	High Risk
Distributed Modified in Products	BSD, MIT, Apache	Artistic, Eclipse	GPL, LGPL, MPL, CDDL
Distributed Unmodified	BSD, MIT, Apache, Artistic	GPL, LGPL, Mozilla (MPL), Eclipse	
Used in Hosted Software	Most others		AGPLv3, AFL – 3.0, OSL 3.0
Internal Use Only	Almost all		
Contributed Only	BSD, MIT		GPL, LGPL, MPL, Apache

Some Options for Remediation

- Commercial Dual Licensing
- Commercial Substitute
- Private Re-Licensing
- Remove/Re-Code



Questions?

Contact Us



David Greenberg

Shareholder, New York

212.801.6545

GreenbergDM@gtlaw.com



Sandy Chiu

Associate, Miami & New York

305.579.0558

ChiuS@gtlaw.com