Strafford

Presenting a live 90-minute webinar with interactive Q&A

Open Source Software: Guidance for Corporate and Technology Counsel on Mitigating Legal and Security Risks

THURSDAY, OCTOBER 12, 2017

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

James G. Gatto, Open Source Team Leader, **Sheppard Mullin Richter & Hampton**, Washington, D.C.

Luke K. Pedersen, Partner, **Baker Botts**, Washington, D.C.

Andrew Wilson, Esq., **Baker Botts**, Washington, D.C.

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-866-961-8499** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 35.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

Mitigating Legal and Security Risks of Open Source Software

Luke Pedersen | James Gatto | Andrew Wilson

October 12, 2017

SheppardMullin

BAKER BOTTS

Introduction to Presenters

James Gatto

Partner | Sheppard Mullin | Washington, DC | 202.747.1945 | jgatto@sheppardmullin.com

Head of Open Source Team, Sheppard Mullin

Author "Open Source Fundamentals" Lexis Practice Advisor

Luke Pedersen

Partner | Baker Botts | Washington, DC | 202.639.7730 | luke.pedersen@bakerbotts.com

- Head of IP Section, DC Office, Baker Botts L.L.P.
- Chair of firmwide Technology Transactions Practice
- Member of firmwide Tech Sector Committee

Andrew Wilson

Associate | Baker Botts | Washington, DC | 202.639.1312 | andrew.wilson@bakerbotts.com

- IP Associate, DC Office, Baker Botts L.L.P.
- Open Source Practice Focuses on Transactional FOSS Assessment and Remediation Counseling
- Member, IPO Open Source Committee

The opinions and views expressed in this presentation do not necessarily represent the opinions and views of Baker Botts or Sheppard Mullin.

OVERVIEW OF LEGAL ISSUES

1

James Gatto

SheppardMullin

BAKER BOTTS

Overview of Open Source Legal Issues

Open Source Risks Vary by Use Case and License

- How a Company Uses Open Source
  - manner of use (e.g. internal use, SaaS deployments, external distribution)
  - whether the open source software is used a standalone program, linked to proprietary software or compiled with proprietary software
  - whether it is used "as is" or modified
- The Particular Licenses that Govern the Open Source Components Used

Overview of Open Source Legal Issues

Open Source Risks Vary by Use Case

- Merely Using/Running Open Source Internally Rarely Imposes Significant Conditions and Obligations
- More Significant Conditions and Obligations Typically Arise When:
  - distributing
  - modifying
  - combining

Overview of Open Source Legal Issues

Tainting – The Impact on "Proprietary" Software

Potential Requirement to:

- license the proprietary software under the terms of an open source license
- make the source code for that proprietary software available to others
- grant others the right to copy, modify and redistribute the software for free.

Overview of Open Source Legal Issues

Patent Issues (to be covered in greater detail below)

- Patent License Grants
- Implied Patent Licenses
- Patent Retaliation/Non-Assertion Clauses

Overview of Open Source Legal Issues

Open Source License Compliance

- Open source Licenses are Often Free, but Have Various Contractual Obligations that Must be Fulfilled
- The Scope of the Obligations Vary from Maintaining License Notices that are Included with the Open Source Software, to More Fact-Specific Obligations Such as Providing Notice of any Modifications Made to the Open Source Software, the Nature of Such Modifications, and How to Obtain the Original (Unmodified) Open Source Software.
- Obligations Can Vary by Use Case

Overview of Open Source Legal Issues

Open Source License Incompatibility

When Multiple Open Source Components Governed by Different Open Source Licenses are Used Together, but the Licenses are Incompatible.

- Occurs when an Open Source License Includes Terms that Conflict with the Terms of Another Open Source License and Prevents Simultaneous Compliance with Both Licenses.
- For Example, the GPL v2.0 License Includes the Provision "You may not impose any further restrictions on the recipients' exercise of the rights granted herein." In Some Cases, this Provision Causes Incompatibility with Other Licenses that Impose Such "further restrictions."

Overview of Open Source Legal Issues

Warranty/Indemnities

- Most Open Source Licenses Include an Express Disclaimer of any Warranty or Indemnity
- Some Require that YOU Indemnify Upstream Developers for Your Modifications.

Overview of Open Source Legal Issues

Enforcements – There Have Been a Growing Number of Open Source License Enforcements

- Most Enforcements Have Been Successful.
  - Some Enforcements May Arise from Actions by Open Source Advocacy Groups (such as the Free Software Foundation or the Software Freedom Law Center)
  - More Recently in Connection with Commercial Litigation Between Competitors

OVERVIEW OF OSS LICENSE PROVISIONS

2

Andrew Wilson

SheppardMullin

BAKER BOTTS

Open Source License Types - Overview

- There are Hundreds of Different Open Source Licenses
  - The Open Source Initiative (OSI) Lists 83 Different Approved Open Source Software Licenses
  - Many Other New and Unapproved Licenses are Frequently Encountered
- Open Source License Terms Run the Gamut
  - Some Very Permissive
  - Some Dangerously Restrictive

Open Source License Types - Categories

- Categorize Open Source Software (OSS) Licenses into Three Buckets
  - Permissive Licenses
  - Permissive Copyleft Licenses
  - Restrictive Copyleft Licenses

Open Source License Types - Philosophies

- Free Software
  - Free as in Freedom for Users to Access, Modify, and Distribute
  - All software code should be made available to its users in human readable form
  - Restrictive Copyleft Licenses

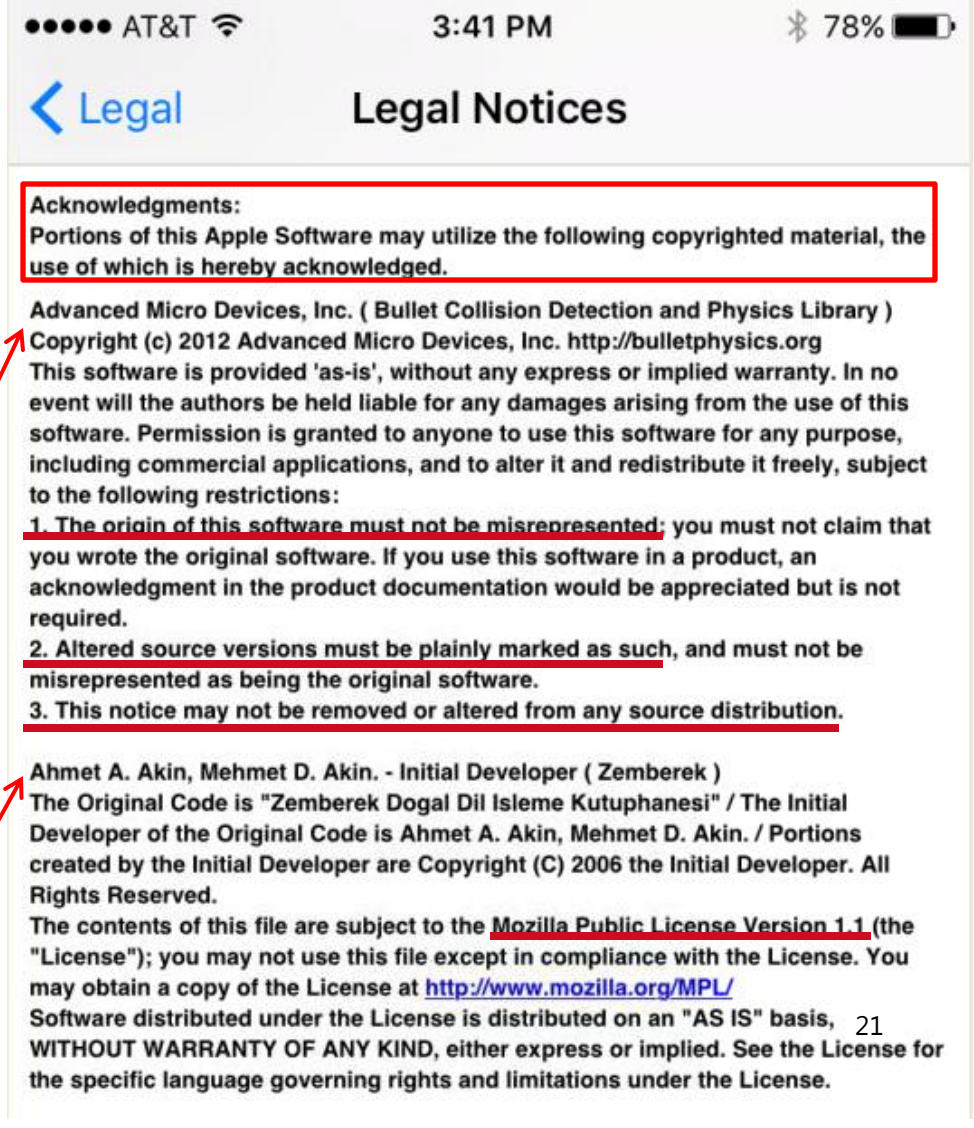
- Open Source
  - Goal is to Develop High Quality Software as Efficiently as Possible
  - Permissive Licenses

Open Source License Types - Permissive

- Very Few, Low Level Compliance Requirements
- Examples Include: MIT, BSD, Apache, etc.
- Copyright License
  - Grants Rights to "Reproduce," “Create Derivative Works,” etc.
  - Subject to Conditions
- Some Include Patent License

Open Source License Types - Permissive

- Typical Requirements
  - Copy of the License
  - Identify Modified Files
  - Retain Attribution Notices
  - NOTICE Text File
- Green Flag:
  - OK to Use and Modify
  - Ensure Compliance with Provisions



Open Source License Types - Permissive Copyleft

- Examples Include MPL, CDDL

- Requirement to "Make Available" the "Corresponding Source" of "Covered Software"
  - But "Covered Software" Only Includes:
    - The Original Open Source Code; And
    - Modifications to the Original Code

Open Source License Types - Permissive Copyleft

- Concerns:
  - Have I Incorporated Proprietary Code Into These Files?
  - Do Modifications Constitute Material Proprietary Information?

- Yellow Flag: Exposure is Limited But Analysis is Required

Open Source License Types - Restrictive Copyleft

- Examples Include GPL, LGPL, Affero GPL (AGPL)
- Difference with Permissive Copyleft Turns on Scope of "Covered Software"
  - Same Requirement to Make Available Corresponding Source Code of Covered Software
  - But "Covered Software" Includes Any Type of Linking
  - Derivatives Are Broadly Defined - If Any Doubt Treat as a Derivative
- Red Flag: Exposure is Much Greater

Restrictive Copyleft - GPL v.2

- GNU General Public License (GPL) v.2
  - "in Whole or in Part ***Contains*** or is ***Derived From*** the GPL Program"
  - If You Ship It, It's Contained in Your Program
  - If You Link to It: Clues from FAQ on Derived From
    - "intimate communication"
    - "sharing data structures"
    - "shared memory"
  - Ambiguity Here Begs for Caution

Restrictive Copyleft - GPL v.2

- What is the Distribution Model?
  - Problematic Distributions:
    - Traditional Shipping Software on Media
    - Download Link
    - Install/Installed on Client System/Client Private Cloud
    - Installed in Public Cloud?
  - OK:
    - Hosted Web Application/Website
    - SaaS Deployment

Restrictive Copyleft - LGPL

- GNU Lesser General Public License (LGPL)
  - Similar to GPL
  - Requirement to Either:
    1. "Convey the Corresponding Source"; OR
    2. "Use a Suitable Shared Library Mechanism for Linking with the Library"
       - Suitable Linking Mechanism - "one that uses ***at run time*** a copy of the Library ***already present on the user's computer system***."

Restrictive Copyleft - AGPL

- Eliminates the Hosted Software Loophole from GPL

13. Remote Network Interaction; Use with the GNU General Public License.

Notwithstanding any other provision of this License, if you modify the Program, your modified version must prominently offer all users interacting with it remotely through a computer network (if your version supports such interaction) an opportunity to receive the Corresponding Source of your version by providing access to the Corresponding Source from a network server at no charge, through some standard or customary means of facilitating copying of software. This Corresponding Source shall include the Corresponding Source for any work covered by version 3 of the GNU General Public License that is incorporated pursuant to the following paragraph.

Restrictive Copyleft - GPL v.3

- Designed to Eliminate Loopholes
  - Embedded Systems With No Access
  - Anti-Anti-Circumvention Law Provisions
    - Prevents Reliance On Digital Rights Management and Anti-Circumvention Laws to Avoid Providing Access to Embedded Software

Why Should You Care? - OSS is Everywhere

- Open Source is Everywhere*
  - 99% of Code Audits Find Open Source
  - 50% of Code Audits Find GPL Components
  - 67% of Open Source Code Identified Contains Known Security Vulnerability

*Statistics Courtesy of Black Duck

Why Should You Care? - Enforcement

- Enforcement Trends
  - Emergence of Copyright Trolls
    - McHardy German Lawsuits
    - Hellwig v. VMWare
  - Un-managed OSS Complicates Business Relationships
    - Versata v. Ameriprise - Ximpleware
  - Too Much Enforcement Kills a Project
    - BusyBox Project
  - Artifex Software, Inc. v. Hancom, Inc.
    - GPL v3 licensed Ghostscript PDF Interpreter
    - Prayer for specific performance relief survives 12(b)(6) motion to dismiss
    - But, remedy of specific performance is "extremely dubious"

Why Should You Care? - Enforcement

- Enforcement Trends (cont.)
  - Compliance is Goal of Organizations and Courts
    - gpl-violations.org
  - APIs are Copyrightable - Does Fair Use Apply?
    - NDCal Finding that "taxonomy" of API is Idea/Expression Merger and not Copyrightable - Overturned
    - Jury Found Fair Use (pending Federal Circuit Review)
  - GPL Claims by Non-Copyright Holders
    - CoKinetic Systems v. Panasonic - In Flight Entertainment Systems

Why Should You Care? - Security

- Recent Exploits of OSS
  - Equifax
    - Exposed 147.5 Million US Consumer's Data
    - Exploit of Open Source Apache Struts Vulnerability
    - Vulnerability Identified in March 2017
    - Patch Available in March 2017
  - OpenSSL Heartbleed
  - gSOAP Dveil's Ivy

- Reason to Avoid OR Call for Proactive Management?

Why Should You Care? - Additional Business Reasons

- Compliance Reduces Risk
- Maintain Good Relationships with Developer Community
  - Recruiting Tool
  - Avoid Being Target of Enforcers
- Demonstrate Competency

AREAS PRACTITIONERS ENCOUNTER OSS

3

SheppardMullin

BAKER BOTTS

Luke Pedersen

Areas Where Practitioners Encounter OSS

- M&A Context
  - Pre-Acquisition/Divestiture Diligence of Target
- Counseling
  - Installing Compliance Policies
  - Audit
- Enforcement Agency
  - Enforcement Groups Can Identify Project Artifacts in Binaries
  - Compliance is Usually the Goal

Areas Where Practitioners Encounter OSS

- Risk Assessment
  - Assessing the Standard of Care to Avoid Liability for Vulnerability Exploit
  - Creating Approved Project List
    - Identifying Poorly Maintained Projects
- Determining Whether to Contribute to Project
  - Benefits of Contributing/Supporting OSS

Where Does it Come From?

- Undisclosed But Embedded in Vendor Software
- In-House Developers
  - No Policy in Place
  - Not Trained on Importance, Identification, or Relevance
- Communication Gap Between Engineering, Management, and Legal Groups on:
  - Importance of Using
  - Cost Associated with Developing In-House
  - Weighed Against the Cost of Compliance

Ways to Identify Embedded Open Source

- Source code scan tools
  - Text-based (Proprietary, Open Source)
    - Low cost (*e.g.*, free) but otherwise resource intensive
    - Requires a higher level of user-sophistication
    - Better suited to identify unintentional “violations”
    - Text-based scans allow for a more comprehensive review and understanding of the code base and "false positives"
  - Signature-based (Proprietary)
    - High cost but otherwise low impact on user
    - Performed by third party
    - No special knowledge required
    - "False positives" can be difficult to run to ground

Software License - Implications of Open Source

- Potential Implications
  - Quality - functionality, cost to fix, maintain, improve
  - Malware exposure - bugs, virus, backdoor, time bombs
  - Infringement of 3rd party IP
    - copyright
    - patent
  - Copyleft trigger
  - Insufficient pass through rights (e.g., sublicense)

Key Open Source Related Deal Terms

- Comprehensive Definition of Open Source
- Schedule of All Open Source, License Information, and Use Cases Should be Created and Verified During Diligence
- Open Source Reps Should be Accurate and Complete
  - Rep as to Open Source Compliance
  - Rep as to Distribution of Source Code and Obligations to Do So
  - Rep as to Patent License Grants Resulting from Use of Open Source
  - Rep as to Obligation to Indemnify Resulting from Use of Open Source

Triage and Remediate

- Isolating Open Source Components
- Determining Scope of Modifications
- Determining Corresponding Source Code Distribution Requirements
- Determining Linking Configuration
- Removal of Components
- Attribution
- Follow-Up Scan

BEST PRACTICES FOR MANAGING OSS

4

James Gatto

SheppardMullin

BAKER BOTTS

Best Practices for Managing OS

- Develop Written Policies on OS Use and Educate Employees
- Log Use of OS
- Ensure Compliance Program
- Consider open source audit
  - assess remediation options
- Address OS issues in third party agreements (e.g., development agreements)
- Consider in M&A

What to Include in Open Source Policies

- Process for Approval To Use Open Source By Developers
  - Some licenses/uses cases can be pre-approved
  - Disclosure – which code, which license, how used, what used with, etc.
- Process to log what OS code is used in what products
- Compliance Process – need to ensure compliance with notices, licenses, making source code available, etc.
- Process for Approval to Release Code Under OS license
- Process for Approval to Contribute Code to OS Projects

PATENT ISSUES WITH OSS

5

James Gatto

SheppardMullin

BAKER BOTTS

Patent Issues With Open Source Licenses

Patent Rights

- Patent License Grants
- Implied Patent Licenses
- Patent Retaliation/Non-Assertion Clauses

Patent Issues With Open Source Licenses

Patent License Grants - The scope of the patent licenses can vary

- generally intended to ensure, at a minimum, if someone makes modifications or contributions to open source software, they cannot turn around and sue another user for patent infringement based on the use of those modifications or contributions
- Some patent license provisions go much further and permit other users to make additional modifications
- some cover future acquired patents

Patent Issues With Open Source Licenses

Implied Patent Licenses

- Some open source licenses arguably include an implied patent license.
- An open source license typically grants a right to *use* copyrighted software.
- Not much judicial precedent, but in one case, the Court suggested that the GPL's right to use under copyright implied a right to use under patent

Overview of Open Source Legal Issues

Patent Retaliation Clauses

- Patent retaliation clauses vary in scope
  - if you institute patent infringement action involving the open source software then your license to use the software terminates
- The termination of rights varies by license and can include termination of all rights granted by the open source license.
- These clauses are designed to discourage you from obtaining the benefits of using open source and enforcing your patents against others who do as well.

Overview of Open Source Legal Issues

- Litigation – open source and patents
  - Discovery issues

- Patenting open source software?


SheppardMullin


BAKER BOTTS