MAYER • BROWN

Cautious Collaboration

Managing IP and Open Source Risks and Pitfalls

Richard M. Assmus
Partner

+1 312 701-8623
rassmus@mayerbrown.com

Paul A. Chandler
Counsel

+1 312 701-8499
pchandler@mayerbrown.com

Speakers

Rich Assmus

Partner – Chicago

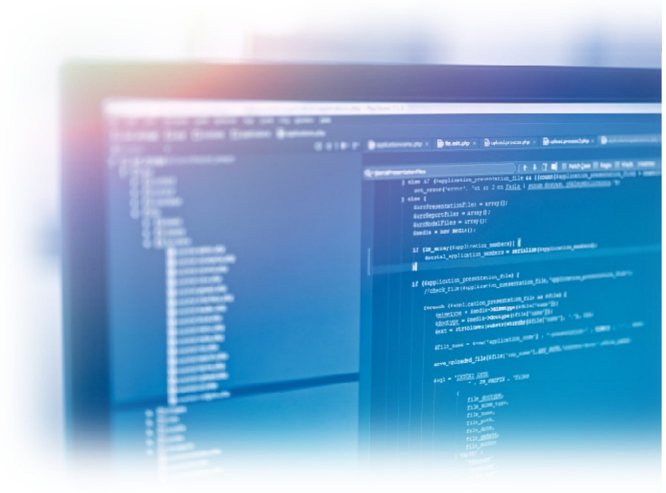
Paul Chandler

Counsel - Chicago

MAYER • BROWN

Agenda

- Background
  - Why talk about open source software (OSS) in collaborations?
  - What is OSS?
  - How is OSS licensed?
- What key risks should customers expect to face in collaborations involving OSS?
- What can a customer do to mitigate these risks?
- Additional protection for trade secrets under the federal Defend Trade Secrets Act
  - Special considerations for software



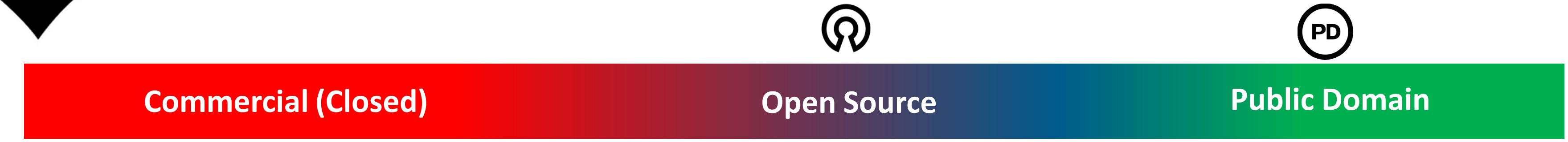
Why Talk About OSS in Collaborations?

- OSS is now enormously important
  - Comprises 36% (average) of code base and in 96% of applications (Black Duck)
  - Comprises 90% of new application code (Forrester Research)
  - 65% of companies are OSS contributors (Black Duck)
- OSS has become core/industry standard tech in some areas, driving demand

Why Talk About OSS in Collaborations? (con’t.)

- But appreciation of OSS risks has not caught up
  - According to a recent North Bridge / Black Duck survey:
    - Nearly 50% of companies:
      - Lack policies for approving OSS
      - Do not enforce their OSS policies
      - Lack processes for tracking OSS usage
- **Key Point** – Failure to appreciate OSS risks may have serious consequences –
  - Legal problems (e.g., OSS non-compliance, infringement and breach claims, M&A issues, impact on licensee IP enforcement, failure to protect trade secrets)
  - Remediation costs
  - Security vulnerabilities

What is OSS?



- No precise definition of “open source,” but understood to refer to software licensed *under an “open source license”*
- OSS licenses generally provide:
  - Source code availability
  - Modification rights
  - Redistribution rights
  - No license fees
  - Unlimited use
- OSS is **NOT** public domain.

What is OSS?

Free Software Foundation (FSF) and Open Source Initiative (OSI) Definitions

- FSF and OSI certify licenses to be “Free” or “Open Source” Software (F/OSS)
- Criteria overlap, but group viewpoints are different

FSF Criteria	OSI Criteria
• Freedom to **run** the program, for any purpose • Freedom to **study** how the program works, and **adapt** it to varying needs • Freedom to **redistribute** • Freedom to **improve** the program https://www.gnu.org/philosophy/free-sw.html	• Free **Redistribution** of Code • **Availability** of Source Code • **Creation** of Derivative Works • Integrity of The Author's Source Code • No Discrimination Against Persons or Groups • No Discrimination against Fields of Endeavor • **Distribution** of License • License Must Not Be Specific to a Product • License Must Not Restrict Other Software • License Must Be Technology-Neutral https://opensource.org/osd-annotated

How is OSS Licensed?

- OSI certifies more than 80 licenses, many variations
- Key differentiator – Reciprocal / Copyleft / Viral
  - Code changes must be made available in source code form under the same license as the base OSS code
  - “Copyleft” – using copyrights to keep code “free” and require distribution of source code
  - **Usually** triggered by “distribution”, but SaaS may also trigger
  - May prohibit license fees on distributed OSS code

How is OSS Licensed? (con’t.)

- Major OSS License Types
  - **Weak** Copyleft—e.g., Mozilla Public License (MPL)
    - Covers file-level code changes
    - May permit structural workarounds
  - **Strong** Copyleft—e.g., GNU General Public License (GPL)
    - Many focus on “viral” concerns, yet strong copyleft licenses are popular
    - Covers OSS code **changes** and **works that contain or are based upon** OSS code
    - Limited caselaw, but extensive debate
  - **Permissive** (No Copyleft) – e.g., Berkeley Software Distribution License (BSD)
    - No reciprocal effect
    - Minimal license requirements (e.g., attribution)

OSS Risks in Collaborations

- OSS may not be disclosed
- OSS licenses may be unacceptable
- OSS is “AS-IS,” without warranties or indemnities
  - May be greater risk of infringement claims
  - May include *unpatched* security vulnerabilities
- OSS may complicate negotiation of IP rights in deliverables
  - Supplier may want to contribute the IP back into an OSS project

OSS Risks in Collaborations (con't.)

- License compliance may be challenging – interpretational issues, unusual terms
- Non-compliance may result in *automatic* license terminations
- It may be unclear *which* OSS license actually applies
  - Provenance issues (may lead to license and code integrity issues)
  - Large file volumes
  - Revision options
- OSS licenses may conflict
  - **Key Point** -- Code may be *technologically* compatible, but *legal terms* conflict.

OSS Risks in Collaborations (con’t.)

- Some OSS licenses require patent licenses to be granted to downstream recipients. Many variations, such as:
  - Apache 2.0/MPL – patent license covers the contributor’s contributions (**but not** the original, unmodified OSS code)
  - GNU GPLv3 – patent license covers the entire code base if modified code is distributed (**but not** if unmodified OSS code is distributed)
- Some OSS licenses lack explicit patent licenses
  - E.g., GPLv2, BSD, MIT
  - Leads to uncertainty as to the scope of any *implied* patent license

OSS Risks in Collaborations (con't.)

- Patent "Retaliation" Clauses – OSS license terminates if you bring a patent infringement suit. Many variations, such as:
  - MPLv1.1 – suit against a **contributor** terminates your license *from that contributor* (even if unrelated to the MPL'd code)
  - MPLv2 – suit against **anyone** based on MPL'd code terminates your license to the MPL'd code (even as to contributors unrelated to the suit)
  - Apache 2.0 – suit against **anyone** based on Apache'd code terminates your *patent license* (but copyright license may continue)
- **Key Point**: Patent licenses and retaliation clauses may make an OSS license unacceptable, **even if** the license is not copyleft and you will not redistribute the OSS.

What Can Customers Do to Mitigate OSS Risks?

- **Understand the role of OSS in the collaboration.**
  - *Prior to signing*, obtain and fully analyze supplier’s list of proposed OSS and applicable licenses
  - Consider alternatives as needed (dual license models, substitutes)
  - Attach an exhibit that documents all approved OSS, licenses and uses—**Details matter!**
  - Have an OSS management process:
    - Compliance with customer’s or supplier’s **OSS** and **security** policies
    - Specify when customer’s consent (**legal** and **technical**) is needed – e.g., (i) new OSS or uses, (ii) new copyleft OSS, or (iii) “**RED FLAG**” OSS prohibited by either party’s policies
    - Identify documentation standards for OSS changes and usage

What Can Customers Do to Mitigate OSS Risks? (con't.)

- **Anticipate OSS problems in deliverables.**
  - Incorporate code scanning (e.g., Black Duck, Palamida, Fossology) in acceptance and audit processes
  - Require remediation of identified issues (e.g., unauthorized code, license conflicts, unpatched security vulnerabilities)
  - Tie milestone payments to demonstrated OSS compliance
- **Avoid Stealth License Conversions**—e.g., "*you agree to comply with all OSS licenses*"

What Can Customers Do to Mitigate OSS Risks? (con’t.)

- **Warranties and Indemnities.**
  - No unauthorized OSS or usage in any deliverable
  - OSS downloaded only from official sources (provenance)
  - Supplier compliance with all OSS licenses
  - Deliverables comply with specifications (even if OSS is included)
  - Supplier indemnification for:
    - Non-infringement covering (i) OSS **selected by supplier** and (ii) OSS modifications **created by supplier**
    - Supplier’s failure to comply with OSS licenses
  - Note: Indemnities are not substitutes for *warranties* in OSS collaborations

DTSA

Overview

- Defense of Trade Secrets Act (DTSA) Generally
- Causes of Action and Remedies Under the DTSA
- Impact on Restrictive Covenants and Confidentiality Agreements
- Considerations/Advantages Using the DTSA to Prosecute Trade Secret Misappropriation Claims
- Special Considerations for Software

Trade Secret Theft

- Trade secret theft is difficult to quantify precisely:
  - Businesses can be unaware that their secrets have been stolen
  - Trade secrets are difficult for businesses to value

$450 *billion*

Total US trade secret theft is estimated to be worth as much as $450 billion annually

85%

In over 85 percent of trade-secret cases, the alleged defendant is **someone the trade-secret owner knows**, typically either an employee or a business partner

Trade Secret Litigation

- Under state trade secret acts, there has been an explosion of trade secrets litigation over the past 20 years
- Although the majority of cases have been filed in state courts, an increasing number of cases are being filed in federal court
  - Trend will accelerate under DTSA
- Federal cases of trade secret theft doubled between 1995 and 2004 and will likely double again through 2017

DTSA Generally

- DTSA creates new federal, private (civil) cause of action for trade secret misappropriation
  - Amends Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-39)
- Covers acts of misappropriation on or after the enactment date (May 11, 2016)
- Trade secrets must be related to a product used in, or intended to be used in, interstate or foreign commerce
  - Software typically qualifies as a trade secret

DTSA Generally

- Remedies
  - Civil seizure (*ex parte*)
  - Damages
  - Injunction
- Increased criminal liability
- Immunity for certain disclosures
  - Impact on certain NDAs

DTSA v UTSA: Misappropriation

- Definition of trade secrets is similar to definition in UTSA:
  - Means “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
    - (A) the owner thereof has taken **reasonable measures** to keep such information secret; and
    - (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.”
  - If OSS risks not considered, can you prove “reasonable measures?”

DTSA v UTSA: Misappropriation (con’t)

- Acts of misappropriation of trade secrets are similar to UTSA:
  - Acquisition of trade secrets by person who knows or has reason to know that the trade secrets were acquired by improper means
    - “improper means” includes theft, bribery, misrepresentation, breach or inducement of breach of a duty to maintain secrecy, or espionage through electronic or other means
    - “improper means” *does not* include <u>reverse engineering</u>, independent derivation or any other lawful means of acquisition

DTSA v UTSA: Misappropriation (con’t)

- Acts of misappropriation of trade secrets:
  - Disclosure or use of trade secrets (without express or implied consent) by a person who
    - Used improper means to acquire knowledge of trade secrets; or
    - Knew or had reason to know that the knowledge of the trade secrets was
      1. derived from a person who used improper means to acquire the trade secrets;
      2. acquired under circumstances giving rise to a duty to maintain secrecy or limit use of the trade secrets; or
      3. derived from a person who owed a duty to maintain secrecy or limit use of the trade secrets.

DTSA v UTSA: Remedies

- Remedies are similar
  - Injunctive relief
  - Damages (including for actual loss, unjust enrichment or reasonable royalty)
  - Exemplary damages for willful and malicious misappropriation
    - Up to 2x amount of compensatory damages
- Reasonable attorney fees may be available to prevailing party under certain circumstances
- DTSA adds civil seizure remedy

DTSA: Injunctive Relief

- Injunctions:
  - May be granted to prevent actual or threatened misappropriation, but *may not*
    - Prevent a person from entering into an employment relationship;
    - Place conditions on employment that are based only on information the person knows (instead of actual evidence of threatened misappropriation); or
    - Otherwise conflict with a state law prohibiting restraints on the practice of a lawful profession, trade or business
  - May grant injunction requiring affirmative actions to be taken to protect the trade secrets
  - May condition future use of trade secrets on payment of reasonable royalty (in exceptional circumstances that render injunction inequitable)
  - Can be no longer than amount of time use could have been prohibited

DTSA: Immunity

- Immunity from liability for certain confidential disclosures
  - Disclosure of trade secrets to federal, state, or local government official, or attorney
    - Solely for purpose of reporting or investigating suspected violation of law
  - Disclosure of trade secrets in complaint or other filing in lawsuit or proceeding, if filed under seal
  - Disclosure of trade secrets in anti-retaliation lawsuit (for reporting by employee of suspected violation of law by employer)

DTSA: Immunity (con’t)

- Notice of immunity in agreements
  - Employers must provide notice of the foregoing immunities in agreements with employees (including contractors or consultants) that govern use of confidential info
  - Employer may comply by providing cross-reference to a policy document provided to employee
  - Notice requirement applies to contracts/agreements *entered into or updated* after the date of enactment
  - Penalty for non-compliance with notice requirement:
    - No exemplary damages or attorney fees for willful/malicious misappropriation and/or bad faith claim of misappropriation or motion (or opposition) to terminate injunction, in action against employee to whom notice not provided

DTSA: Trade Secret Best Practices

- Set procedures for maintaining trade secrets
  - Designations used to mark trade secret information
  - Review confidentiality agreements with employees and consultants
  - Policies on source code access, OSS use
  - Access limited to persons with a need to know
  - Security measures for accessing trade secret information
- Procedures for departing employees
  - Disabling access to company systems, accounts, equipment
  - Reminders/affirmations of confidentiality obligations
  - Written acknowledgements required on departure

DTSA: Considerations/Advantages

- DTSA adds predictability/breadth
  - Federal court:
    - Known rules and procedures
    - Broad subpoena power
    - More predictable results as case law develops and sets precedent
- DTSA does not preempt other laws
  - Adds protection to (instead of replacing) existing state laws
  - May still be advantageous to bring suit in state court
  - May be “growing pains” as courts struggle with both state and federal laws

QUESTIONS?

Richard M. Assmus
Partner

+1 312 701-8623
rassmus@mayerbrown.com

Paul A. Chandler
Counsel

+1 312 701-8499
pchandler@mayerbrown.com