Morgan Lewis

GLOBAL DIGITAL TRANSFORMATION
— WEBINAR SERIES —

OPEN SOURCE SOFTWARE

March 8, 2023
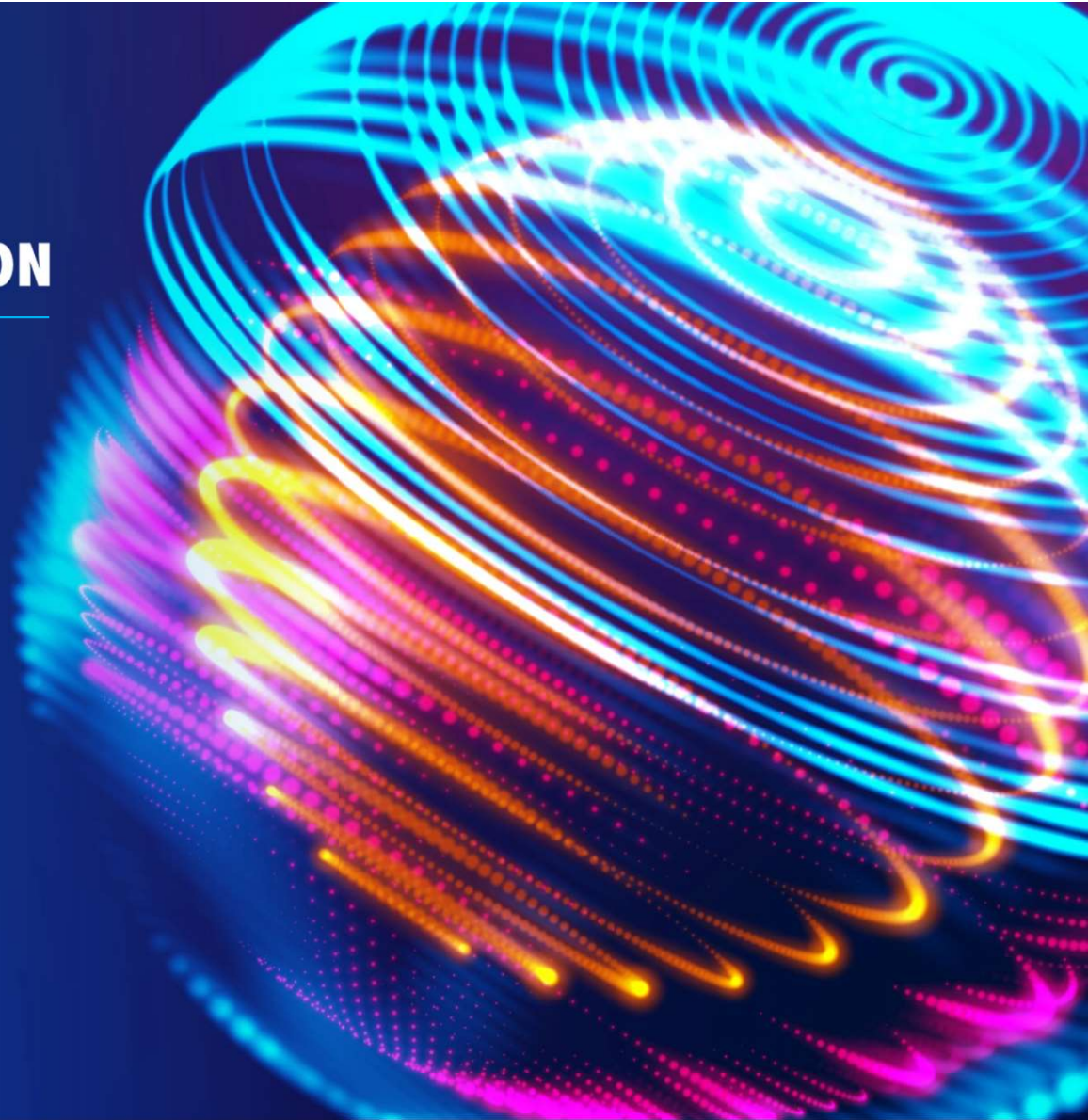
Presenters

Ksenia Andreeva

Rahul Kapoor

Shokoh Yaghoubi

Before we begin

Tech Support

If you are experiencing technical difficulties, please contact WebEx Tech Support at +1.866.779.3239.

Q&A

The Q&A tab is located near the bottom right hand side of your screen; choose "All Panelists" before clicking "Send."

CLE

We will mention a code at some point during the presentation for attendees who requested CLE. Please make note of that code, and insert it in the pop-up survey that will appear in a new browser tab after you exit out of this webinar. You will receive a Certificate of Attendance from our CLE team in approximately 30 to 45 days.

Audio

You will hear sound through your computer speakers/headphones automatically. Make sure your speakers are ON and UNMUTED.

To access the audio for by telephone, please click the "phone" icon below your name on the Participants Panel for teleconference information.

Outline

- Open Source Software Overview
- OSS Benefits & Risks
- Case Studies
- Common OSS Licenses
- Discussion of Specific OSS Licenses
- Community Norms & Best Practices
- OSS Use and Guidelines
- OSS Audits and Compatibility
- OSS in M&A Transactions

Morgan Lewis

What is Open Source?

- Source code freely shared with other programmers subject to an Open Source License
- It is ubiquitous
  - Per Synopsys, 84 open source components per commercial application in 2016 to 528 in 2020
  - Used in all types of industries, agencies, institutions, products
- For example:
  - Linux (operating system) (GPL v2)
  - Apache (web server) (Apache License 2.0)
  - MySQL (relational database) (GPL v2)
  - Perl (scripting language) (Artistic License and GPL v2)
  - OpenStack (cloud computing platform) (Apache 2.0)
  - Apache Hadoop (framework for big data) (Apache 2.0)
  - R (statistical computing language) (GPL v2)

Morgan Lewis

How We Help Clients

- Evaluate proposals to use OSS – internal, customer facing/cloud, on-premises, embedded
- Evaluate proposals to contribute proprietary software to Open Source
- Prepare Open Source Policies that manage risks/benefits and are efficient to administer
- Provide Developer Training
- Evaluate Open Source Development Tools
- Assist with Open Source Audits (e.g., by Software Freedom Conservancy)
- Defend clients accused of Open Source License Violations
- Perform Open Source Due Diligence (investments, acquisitions)
- Evaluate Open Source Code Composition Reports (e.g., Black Duck)
- Draft/Advise on Open Source Agreement Provisions

Morgan Lewis

Software Licensing

- Four different types of software from a licensing perspective:
  - Proprietary Software
    - Typical commercial software
    - Distributed as binary code under proprietary license – typically for a fee - source code not provided – no right to copy, make derivative works, reverse engineer, repair, etc. – unless allowed in license
  - Open Source Software
    - Source code always available, even if distributed as binary code – no license fee – distributed under an open source license
    - Practical, commercially acceptable *(OS license characteristics defined by Open Source Initiative, or OSI)*
    - OSS Licenses can be restrictive/risky (e.g., copyleft licenses), permissive/safe or somewhere in between
  - Free Software
    - Computer software distributed under terms that allow users to run the software for any purpose as well as to study, change, and distribute it and any adapted versions ("Think of 'free speech,' not 'free beer'")
    - Rooted in philosophy, not practical/commercial considerations *(Concept defined by Richard Stallman)*
  - Public Domain Software
    - Dedicated by copyright owner to the public or expired copyright (pre-1928)
    - Free for anyone to copy and use without license restrictions

Morgan Lewis

Software Licensing - OSS

- Open Source Software (OSS) is original work of authorship - > subject to Copyright

- OSS can only be used per License Terms imposed by owner of the Copyright

- Check Copyright/License Notice to confirm owner of work and applicable open-source license

- Review License Terms and be sure to comply with them

- Violation of license could expose company to breach of contract and Copyright misappropriation claims

- Could result in injunction, monetary damages, including statutory damages, and contamination of code base with unlicensed third-party code

Morgan Lewis

Open Source Benefits

- Rapid Development

- Low Cost

- Open
    - Available
    - Modifiable
    - Maintainable
    - Reliable
    - Secure

- Community
    - Pride of Ownership
    - Peer Development
    - Partnership (individual/non-profit/corporate)
    - Outsource Coding

- Continual Improvement

- Open Standard

Open Source Risks – Code

- OSS Provenance?

- No support

- No warranty

- Poorly funded → poorly maintained

- No differentiation
  - Common features
  - Hard to customize

- Vulnerabilities are public

- Out of synch with company needs

  - Bug fixes?
  - New features?
  - Roadmap?
  - Need to update every new release with company customizations/patches

- Community

- Taint proprietary code base and vice-versa if intermingled

Morgan Lewis

Open Source Risks - Licenses

- Could be viral (e.g., GPL/copyleft licenses)
- Non-negotiable
- As is
- Quirky
  - can include explicit patent licenses
  - can include publicity conditions (i.e., if publicize feature enabled by OSS, need to credit author)
  - can limit use to specific situations (e.g., academic but not commercial uses)
- Gotchas
  - distribution trigger (no copyleft effects unless distributed – and definition of "distribution" varies)
  - code combination (entire work subject to OSS license (GPL), or just derivatives of licensed files (MPL))
- Ambiguous (rarely enforced or subjected to legal interpretation)
- Enforcement
  - "political"
  - public – can be embarrassing even if risk is manageable

Morgan Lewis

Case Study 1 – Microsoft Hyper-V (2009) (License Risk)

- Linux driver code (GPL v.2) incorporated in Microsoft's proprietary Hyper-V Linux driver code
- Discovered by user of Hyper-V driver code and reported on Linux Internet blog:
  - "This saga started when one of the user's [sic] on the Vyatta forum inquired about supporting Hyper-V network driver in the Vyatta kernel. A little googling found the necessary drivers, but on closer examination there was a problem. The driver had both open-source components which were under GPL, and statically linked to several binary parts." *Network Plumbers Journal*, July 20, 2009. http://linux-network-plumber.blogspot.com/2009/07/congratulations-microsoft.html
- Result – Microsoft open-sourced its Hyper-V drivers:
  - "Nice. Microsoft has released the Hyper-V drivers as GPLv2." (Id.)
- Lesson 1: Training is important – Coder apparently had access to GPL code and then used it inappropriately.
- Lesson 2: Misuse of GPL can generate a firestorm in community – may be hard to avoid open sourcing proprietary code combined with GPL code.
- Lesson 3: Maybe developers of proprietary code should not have access to GPL code.

Morgan Lewis

Case Study 2 – Heartbleed Bug (2014) (Code Risk)

- Heartbleed
  - Bug in OpenSSL (open source toolkit used to provide secure communications between web clients/browsers and websites)
  - Could be used to capture passwords
  - Affected nearly 2/3 of Internet (not banks or gov't)
  - Public announcement at Openssl.org:
    - "A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64kB of memory to a connected client or server (a.k.a. Heartbleed)." "Fixed in OpenSSL 1.0.1g (Affected 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)." http://openssl.org/news/vulnerabilities.html
- Lesson 1: Ubiquitous OSS component was vulnerable.
- Lesson 2: OpenSSL community was transparent about the bug and released fix same day as discovered and announced (April 7).
- Lesson 3: Review level of support for key projects – in 2014, OpenSSL project, used by thousands of companies, had one developer and was earning no more than $2,000 in donations each year. https://www.theregister.com/2021/05/10/untangling_open_sources_sustainability_problem/

Morgan Lewis

Case Study 3 - SCO Group (2003) (License Risk, Code Risk, Litigation Risk)

- SCO Group claimed to own some rights in Unix System V.

- Alleged that Unix licensees had impermissibly incorporated Unix code (ranging from "hundreds of lines" to over a million lines) into Linux (over 30 million lines of code) and other open source software.

- In 2003, sued Unix licensee for violation of Unix license, copyright infringement and trade secret misappropriation, seeking license termination and damages - and also sued Linux customers for copyright infringement.

- Unix licensee counter-sued, alleging that SCO suit was violation of GPL (due to SCO's own distribution of Linux and incorporation of Linux features into SCO UNIX distribution).

- Lesson 1: Users of open source software are exposed to copyright infringement claims if a contribution to the open source software was infringing.

- Lesson 2: Before releasing software to the open source community, a company needs to confirm it has the legal rights to do so.

Morgan Lewis

Common Open Source Licenses

Top Licenses (color indicates potential risk)

- MIT (32% of open source projects)
- GPL General Public License v2.0 (18%)
- Apache 2.0 (14%)
- GPL General Public License v3.0 (7%)
- BSD (Berkeley Software Distribution) 2.0 (6%)
- Artistic License (Perl) (4%)
- LGPL (Lesser/Library GPL) – v2.1 (4%)
- LGPL (Lesser/Library GPL) – v3.0 (2%)

Morgan Lewis

GNU GPL v.2

- **GPL is the strictest of all Open Source Licenses**
  - Any work that, in whole or in part, contains code licensed under the GPL is governed by the GPL
  - Freedom to modify and distribute stipulates that changes to the GPL code can only be made with notice of such changes and identification of who made the changes
  - The GPL must accompany copies of the program that are distributed, including the disclaimer of warranties with respect to the software
- Modification of a copy of the program is allowed → a "work based on the program"
- Combination of the program with other code results in the combined works being covered by the GPL too ("tainted")
- No license fee charged for the license of rights under the GPL
- Workarounds: (a) costs of distribution, (b) additional warranties offered, or (c) additional services offered

Morgan Lewis

GNU GPL v.2

- General industry standard:

  - Combining Source Code   **No**

  - Static Linking   **No**

  - Dynamic Linking   **Maybe OK**

  - Distribution of proprietary code with GPL code as a separate program   **OK**

  - Running combined code of any type on a server   **OK**

- Supporters are true believers in Free Software – not likely to compromise when OSS misused by big corporations (see at http://www.gnu.org/philosophy/philosophy.html)

Morgan Lewis

GNU GPL v.3

- GPL v.3 was created to address loopholes in v.2
- Basic activities that do <u>not</u> trigger viral effects under GPL v.3:
  - Internally running unmodified program
  - Internally running program with your modifications
  - Redistributing unmodified source code must comply with GPL v.3 requirements, but does not affect other code
  - Running GPL v.3 software in an ASP environment does not constitute "conveying" the software (i.e., no requirement to provide ASP users with code of such software), but Section 13 of Affero GPL v.3, a GPL v.3 extension, does impose such a requirement

    NB! GPL v.2 does not address the ASP issue

Morgan Lewis

GNU LGPL v.2.1

- **Less restrictive than the GPL**
- Proprietary code can be used in connection with GPL code through the use of programming Libraries
- If LGPL governed Libraries (without modification) do not co-mingle with proprietary code (either in source or though linking) prior to distribution, it's necessary to make notice of the license for the Library and a copy of the source code for it
- If you modify the Library, then: (1) the modification itself must be a Library; (2) notification for users is required (including dates of the changes); (3) the modified work must be licensed for free; (4) the modified Library shall not depend on any other code
- If you co-mingle the code of the Library with the proprietary code, you must: (1) supply source code of everything; **OR** (2) use a shared library mechanism and provide the source code for the Library; **OR** (3) provide a written offer valid for at least 3 years to do (1); **OR** (4) offer the code for download if applicable

Morgan Lewis

BSD

- **Less restrictive than the GPL**

- Redistribution of source code of the licensed software, with or without modification, requires:
  - Retention of applicable copyright notice
  - Retention of conditions and disclaimer contained in license

- Redistribution of binary form of the licensed software, with or without modification, requires:
  - Reproduction of the applicable copyright notice
  - Reproduction of conditions and disclaimer contained in the license in the documentation and/or other materials provided with binary form

- No obligation to provide the source code

- Derivative works can be commercialized

Morgan Lewis

Apache v.2.0

- **Perpetual, worldwide, non-exclusive, no-charge, royalty-free irrevocable**
  - copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and Derivative Works in Source or Object form
  - patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license only applies to those patent claims licensable by a given Contributor that are necessarily infringed by such Contributor's Contribution alone or in combination with the Work
- **Obligations**
  - provide a copy of the Apache License with all distributions of the Work or Derivative Works
  - retain prominent notice at all modified files

- retain all notices from the source form of the Work at all Derivatives
- if the Work contains a Notice file as part of its distribution, then any Derivative Works must include a readable copy of the attribution notices in such Notice file
- modifications to the Work contributed back to the licensor are governed by the terms of the Apache license (includes license to patent claims infringed by use of Contributors modifications)
- if add own terms to licenses, must indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of accepting any such warranty or additional liability

Morgan Lewis

Common Open Source Licenses

Resources
- Top 20 Licenses
  - (https://www.blackducksoftware.com/resources/data/top-20-open-source-licenses)
- Enforcement
  - https://www.gnu.org/licenses/gpl-violation.html
  - (GPL Compliance Lawsuit) https://sfconservancy.org/news/2015/mar/05/vmware-lawsuit/
  - http://www.fsf.org/news/conservancy-and-christoph-hellwig-gpl-enforcement-lawsuit

Morgan Lewis

Your CLE Credit Information

For <u>ALL</u> attorneys seeking CLE credit for attending this webinar, please write down the alphanumeric code on the right >>

Kindly insert this code in the **pop-up survey** that will appear in a new browser tab after you exit out of this webinar.

THE CLE CODE IS:

JZE9879

Morgan Lewis

Community Norms-Free Software Foundation

- Primary goal in GPL enforcement is to bring about GPL compliance. "Copyleft enforcement done in this spirit focuses on stopping incorrect distribution, encouraging corrected distribution, and addressing damage done to the community and users by the past violation."

- Legal action is the last resort. The goal is to educate users on the use of OSS.

- Confidentiality can increase receptiveness and responsiveness. Enforcers should initiate compliance discussions in private unless the user is using confidentiality to cover inaction and unresponsiveness.

- Community-oriented enforcement must never prioritize financial gain, but it is reasonable to request compensation for the cost of providing compliance education to accompany constructive enforcement action.

- Community-oriented compliance work does not request nor accept payment to overlook problems.

- Community-oriented compliance work starts with carefully verifying violations and finishes only after a comprehensive analysis.

- Community-oriented compliance processes should extend the benefit of GPLv3-like termination, even for GPLv2-only works.

Morgan Lewis

Open-Source similarity to ESG and Privacy Issues

- Risk: like ESG open-source software license violations pose PR issues and internal costs.

- Expansion: OSS is not going away; it's only expanding like privacy.

Morgan Lewis

Best Practices for Using Open Source Software

- Overall goal: promote safe use of OSS to leverage benefits and mitigate risks.

- Keep accurate records

- Establish internal processes
  - Review and approve OSS use requests
  - Track use of open source software

- Involve legal and developer organizations

- Training program

- Limited scope of approval

- Different review tracks for different uses/licenses

- Consider fast track approval process
  - Limited set of licenses
  - Limited set of uses

- Reevaluate if OSS use changes

- Audit OSS use

OSS Audits

- An open-source software audit helps your business, legal, and engineering teams find open-source software, third-party code, and license obligations.

- Companies commonly run a Black Duck, WhiteSource or similar scan of their source code.

- Company uploads code onto auditor's servers, auditor analyzes the code and provides a software bill of materials which identifies the OSS components in the codebase and the associated OSS license.

Open Source Use Requests

- Request to Use OSS for Company Project Should Identify:
  - OSS version
  - Proposed OSS use:
    - Company product
    - Modified?
    - Internal use only?
    - Combined with proprietary code?
    - Server only?
    - Distributed?
    - Part of SAAS offering?
  - Known vulnerabilities
  - Applicable license
 - Availability of same code under non-open license

Morgan Lewis

Open Source Use Guidelines

- Generally safe:
  - Using OSS under BSD or MIT licenses
  - Running company code on Linux OS
  - Using LGPL libraries without modification
  - Running OSS only on servers with no distribution
  - Caveat (risky to combine any OSS with proprietary code)

- Be cautious:
  - Developing non-GPL software that is compatible with functionality of GPL software (use "clean room" process – check GPL header files)
  - Calling an executable GPL program via an API (check header files)

- What's risky (Prohibit):
  - Allowing developers to use GPL source code
  - Accepting any third-party code for use in one of your software products without understanding where it came from, under what license

Morgan Lewis

Best Practices for Contributing to Open Source Software

- Adopt Internal Review Process/Committee
- Open Source Contribution Request:
  - Reasons for contributing:
    - Improve functionality of strategic OSS
    - Promote wider use of company technology
    - Add customizations to open source project
    - Outsource coding to OS community
    - Improve standing with OS community, press, customers
  - What license will apply?
  - Is contribution subject to third party encumbrances?
  - Does contribution use company patents?
  - Strength of open source community?
  - Level of company commitment to OSS code in future?
  - Need two source code trees in future?
  - Harm to revenue?

Morgan Lewis

Compatibility

License compatibility allows for pieces of software with different licenses to be distributed together. Not all open source software licenses are compatible with each other.
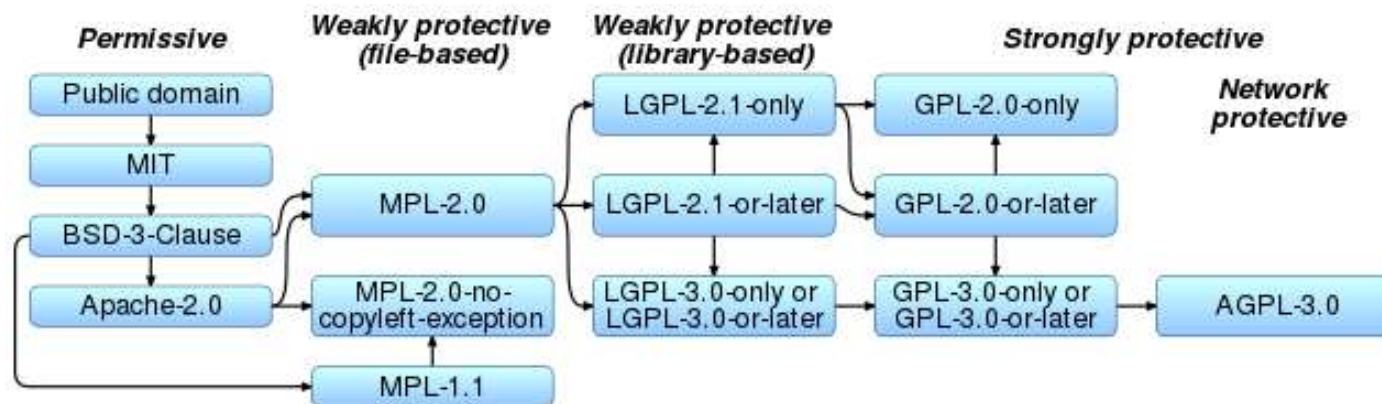
By David A. Wheeler, et al. - The Free-Libre / Open Source Software (FLOSS) License Slide by Dwheeler (2007-09-27)About MPL 2.0: Revision Process and Changes FAQ — Mozilla, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=93181991

Morgan Lewis

Challenges

- Understanding the licenses – language is often very unclear
- Analyzing how the code components are linked
  - Dynamically
  - Statically
- Outdated software components: determining which license applies to which version of the software
- What if the licenses are not compatible?
- What if the code component is not governed by a license at all? The copyright holder did not include one when they released the code
- Previous versions of the software have already been released under a different license

Morgan Lewis

OSS in M&A Transactions

- Ferret out any information related to the use of OSS by a Target
- Often, Target is not very organized about the documentation and OSS licenses that relate to their use of OSS materials
- Having a representation as to OSS in the APA/SPA helps force the Target to disclose all relevant information
- Client is then in a better position to evaluate/re-negotiate the monetary/other terms of the deal

Morgan Lewis

OSS Reps

- Get a full list of Company's use of OSS for diligence purposes

- *Section 1.1(u)(i) of the Disclosure Schedule sets forth a true, correct and complete list (in the format requested by Parent) of each item of Open Source Software incorporated into, integrated, bundled, or linked with, distributed with or used in the development or compilation of, or otherwise used in or with any Company Product and (A) a description of the license terms (and version) under which such Open Source Software is licensed; and (B) the manner in which such Open Source Software is incorporated into, integrated, bundled, or linked with, distributed with or used in the development or compilation of, or otherwise used in or with any Company Product.*

Morgan Lewis

OSS Reps

- OSS Compliance Rep & Contribution Rep

- *The Company has taken sufficient steps to (A) identify Open Source Software used by the Company or otherwise included in the Company Products, and (B) regulate the use, modification, and distribution of Open Source Software in connection with the Company Products, <u>in compliance with</u> the applicable licenses. The Company has <u>complied in all material respects</u> with the terms of the license agreements applicable to any Open Source Software that Company has used in its business. Company <u>has not contributed any Company proprietary software</u> to an open source project or made such proprietary software available as Open Source Software.*

Morgan Lewis

OSS Reps

- OSS Policies

- *Any written Open Source Software policies of the Company are listed in Section 1.1(u)(iii) of the Disclosure Schedule, and complete and accurate copies thereof have been delivered to Parent. There has been no material deviation from or violation of such policies with respect to Open Source Software.*

OSS Reps

- No use of Viral OSS

- *The Company has not modified, included, incorporated or embedded in, linked to, combined or distributed with or used in the delivery, or provision of any Company Product any Open Source Software in a manner that: (a) requires or purports to require any Company proprietary Software be disclosed or distributed <u>in source code form</u>; (b) requires or purports to require any Company proprietary Software be licensed for the purpose of <u>making derivative works</u>; (c) requires or purports to require any restriction on the consideration to be charged for the distribution of any Company proprietary Software; or (d) creates any obligation for Company to grant to any third party any rights or immunities to Technology or under Intellectual Property Rights owned by Company.*

OSS Definition

- *"Open Source Software" means any Software that is subject to or licensed, provided, or distributed under any "open source," "copyleft," or other similar types of license terms, including without limitation any GNU General Public License; Library General Public License; Lesser General Public License; Mozilla license; Berkeley Software Distribution license; MIT, Apache, Public Domain licenses, including any license meeting the Open Source Definition (as promulgated by the Open Source Initiative) or the Free Software Definition (as promulgated by the Free Software Foundation), or any substantially similar license.*

Morgan Lewis

Questions?

Morgan Lewis | **GLOBAL DIGITAL TRANSFORMATION** WEBINAR SERIES
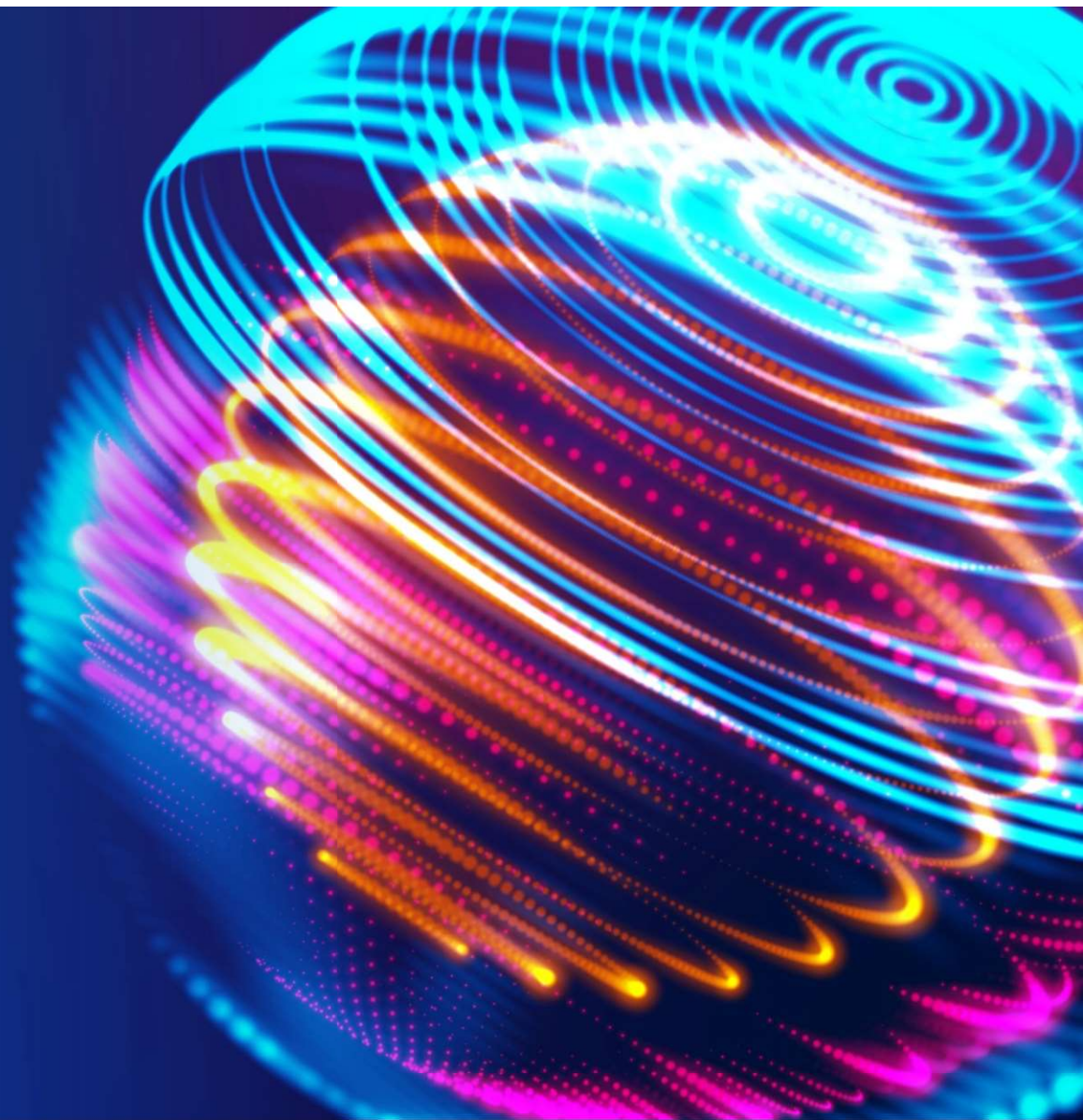
Ksenia Andreeva

Ksenia Andreeva

Dubai, United Arab Emirates

+971.4.312.1865

ksenia.andreeva@morganlewis.com

Ksenia Andreeva counsels clients on intellectual property, information technology, and cybersecurity the context of their business transactions.

Ksenia is experienced in drafting and negotiating a broad range of IP and technology-related agreements and commercial contracts, including complex software licenses, technology transfer and development agreements, and e-commerce agreements, service level agreements (SLA), franchise agreements, IP licenses and assignments and other. Her clients include companies in media, technology, telecommunications, consumer products, financial services, insurance and many other industries.

As a complement to her transactional practice, Ksenia advises clients on data protection compliance, including with respect to the General Data Protection Regulation (GDPR) and GCC privacy laws.

Biography

Rahul Kapoor
Silicon Valley/ San Francisco
+1.650.843.7580
rahul.kapoor@morganlewis.com

With a focus on commercial, intellectual property (IP), and technology transactions, Rahul Kapoor counsels clients on strategic alliances, joint ventures, and corporate partnering transactions in the technology and life science industries. He also handles standards body licensing structures, patent licensing, open source software strategy, e-commerce and privacy, supply and distribution agreements, consignment agreements, spinoffs and core technology licenses, and IT outsourcing transactions.

Rahul is the local practice group leader of the Silicon Valley and San Francisco corporate and business transactions practice, leader of the India initiative and previously served as the firmwide hiring partner, a member of the firm's Advisory Board, and on the firm's Diversity Committee.

In addition to practicing law, Rahul taught an IP Strategy class for 10 years at UC Berkeley School of law.

Morgan Lewis

Biography

Shokoh Yaghoubi

Silicon Valley

+1.650.843.7252

shokoh.yaghoubi@morganlewis.com

Shokoh H. Yaghoubi counsels clients on intellectual property issues and strategy involved in mergers and acquisitions, initial public offerings, and financings. She represents clients in transactions relating to technology, including technology and content licensing, transfers of intellectual property rights, joint development and joint venture arrangements, and distribution and sales arrangements. She also advises on supply, service and outsourcing agreements, manufacturing and foundry relationships, and cross-border licensing and strategic alliances.

As part of her practice, Shokoh drafts website privacy policies and terms of use, and advises clients on related Internet privacy law issues.

Prior to joining Morgan Lewis, Shokoh drafted and negotiated technology licensing agreements, assisted in revising template agreements, and advised clients on confidentiality matters and obligations as a consulting lawyer in the licensing and technology group of a Fortune 100 technology company. She is fluent in English and Farsi.
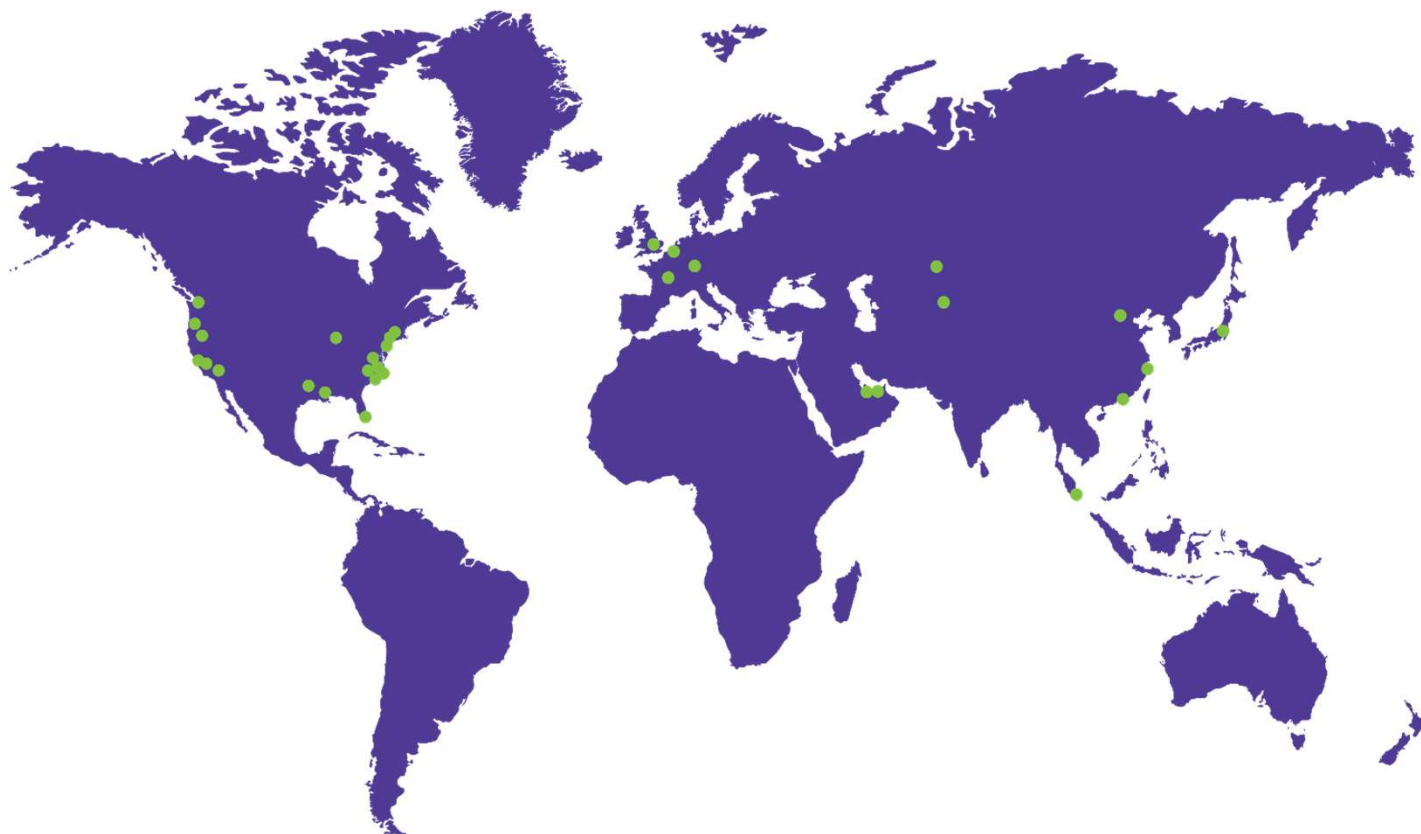
Morgan Lewis

Our Global Reach

Africa	Latin America
Asia Pacific	Middle East
Europe	North America

Our Locations

Abu Dhabi	Miami
Almaty	New York
Astana	Orange County
Beijing*	Paris
Boston	Philadelphia
Brussels	Pittsburgh
Century City	Princeton
Chicago	San Francisco
Dallas	Seattle
Dubai	Shanghai*
Frankfurt	Silicon Valley
Hartford	Singapore*
Hong Kong*	Tokyo
Houston	Washington, DC
London	Wilmington
Los Angeles	

Morgan Lewis

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU