Advanced Licensing Agreements 2017

Volume Two

Co-Chairs
Marcelo Halpern
Ira Jay Levy
Joseph Yang

To order this book, call (800) 260-4PLI or fax us at (800) 321-0093. Ask our Customer Service Department for PLI Order Number 185480, Dept. BAV5.

Practising Law Institute
1177 Avenue of the Americas
New York, New York 10036
Open Source Issues and Opportunities (PowerPoint slides)

David G. Rickerby

Boston Technology Law, PLLC

If you find this article helpful, you can learn more about the subject by going to www.pli.edu to view the on demand program or segment for which it was written.
Open Source Issues and Opportunities

Practicing Law Institute

Advanced Licensing Agreements 2017

May 12th 2017
10:45 AM - 12:15 PM

David G. Rickerby
Overview

- Introduction to Open Source
- Enforced Sharing
- Managing Open Source
What is Open Source?

- “Open” “Source” – Any software licensing model that makes the source available to copy, distribute, modify, etc.
What is Source Code?

- The human readable version of the code.
- Exposes trade secrets, interfaces, and logic.
As opposed to Object Code...
Open Source is Big Business

ANDROID - Declared license: Apache 2.0
~185 components
~19 different OSS licenses - most reciprocal
Many Organizations
Solving Problems in Many Industries

- Healthcare
  - OSEHRA
- Mobile
- Financial Services
  - THE LODESTONE FOUNDATION
  - openMAMA
- Everything
  - ALLSEEN ALLIANCE
- Automotive
  - GENIVI
So, what’s the big deal? Why isn’t this just like a commercial license?

In many ways they are the same:

- Both commercial and open source licenses are based on ownership of intellectual property.
- Both grant certain rights and retain others.
- Both are governed by the same laws.
- Both may include provisions which may be incompatible with the other type of license, and, indeed with other licenses of the same type.
But…

Open Source Licenses:
- Tend to have different goals
- Are usually written by and for developers not lawyers
- Encourage uncontrolled combination and reuse of the IP
- Form a contract in a different way than most commercial licenses (in fact some argue they don’t form a contract at all – merely act as a permission)

AND

- Some open source licenses impose sharing obligations on users
Two Basic Schools of Open Source

- **FOSS (Free and Open Source Software)**
  - Requires licensor to make improvements or enhancements available under similar terms
  - Primary example is the GPL: Licensee must distribute “work based on the program” and cause such works to be licensed ... under the terms of the GPL

- **Academic/Permissive**
  - Modifications/enhancements may remain proprietary
  - Distribution in source code or object code permitted provided copyright notice & liability disclaimer are included and contributors’ names are not used to endorse products
  - Primary examples: Berkeley Software Distribution (BSD), Apache Software License
Free Software Definition
from the Free Software Foundation

“Free software” is a matter of liberty, not price. To understand the concept, you should think of “free” as in “free speech,” not as in “free beer.”

Free software is a matter of the users' freedom to run, copy, distribute, study, change and improve the software. More precisely, it means that the program's users have the four essential freedoms:

• The freedom to run the program, for any purpose (freedom 0).

• The freedom to study how the program works, and change it to make it do what you wish (freedom 1). Access to the source code is a precondition for this.

• The freedom to redistribute copies so you can help your neighbor (freedom 2).

• The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

Principles of Open Source Licensing
from the Open Source Initiative

1. Free \textit{[Unrestricted]} Redistribution
2. Program must include Source Code and must allow
distribution in source code as well as compiled form.
3. Must Allow Modifications and Derived Works
4. Integrity of the Author's Source Code
5. No Discrimination Against Persons or Groups
6. No Discrimination Against Fields of Endeavor
7. Distribution of License – no additional license can be required
   of others who redistribute the program
8. License Must Not Be Specific to a Product
9. License Must Not Restrict Other Software
10. License Must Be Technology-Neutral – not predicated on any
    individual technology

from \url{http://www.opensource.org/docs/osd}
<table>
<thead>
<tr>
<th>Current OSI Approved Licenses (<a href="http://www.opensource.org">www.opensource.org</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Academic Free License 3.0 (AFFL-3.0)</td>
</tr>
<tr>
<td>2. Affero General Public License 3.0 (AGPL-3.0)</td>
</tr>
<tr>
<td>3. Adaptive Public License (APL-1.0)</td>
</tr>
<tr>
<td>4. Apache License 2.0</td>
</tr>
<tr>
<td>5. Apple Public Source License</td>
</tr>
<tr>
<td>6. Attribution Assurance Licenses</td>
</tr>
<tr>
<td>7. Attribution Assurance Licence</td>
</tr>
<tr>
<td>8. BSD 3-Clause &quot;New&quot; or &quot;Revised&quot; License (BSD-3-Clause)</td>
</tr>
<tr>
<td>9. BSD 2-Clause &quot;Simplified&quot; or &quot;FreeBSD&quot; License (BSD-2-Clause)</td>
</tr>
<tr>
<td>10. Boost License 1.0 (Boost)</td>
</tr>
<tr>
<td>11. CDDL License 2.1 (CDDL-1.1)</td>
</tr>
<tr>
<td>12. Computer Associates Trusted Source Public License (CATOSL-1.1)</td>
</tr>
<tr>
<td>13. Common Development and Distribution License 1.0 ( CDDL-1.0)</td>
</tr>
<tr>
<td>14. Common Public Attribution License 1.0 (CPAL-1.0)</td>
</tr>
<tr>
<td>15. GNU Library or Lesser General Public License 3.0 (GLP-3.0)</td>
</tr>
<tr>
<td>16. GNU Library or Lesser General Public License 1.0 (GLP-1.0)</td>
</tr>
<tr>
<td>17. GNU Affero General Public License 3.0 (AGPL-3.0)</td>
</tr>
<tr>
<td>18. GNU General Public License 2.0 (GPL-2.0)</td>
</tr>
<tr>
<td>19. GNU General Public License 3.0 (GPL-3.0)</td>
</tr>
<tr>
<td>20. GNU Library or Lesser General Public License 2.0 (GLP-2.0)</td>
</tr>
<tr>
<td>21. Historical Permission Notice and Disclaimer (HPND)</td>
</tr>
<tr>
<td>22. IBM Public License 1.0 (IPL-1.0)</td>
</tr>
<tr>
<td>23. ICV License 1.1 (ICV-1.1)</td>
</tr>
<tr>
<td>24. ICV License 1.1 (ICV-1.1)</td>
</tr>
<tr>
<td>25. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>26. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>27. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>28. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>29. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>30. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>31. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>32. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>33. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>34. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>35. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>36. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>37. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>38. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>39. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>40. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>41. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>42. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>43. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>44. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>45. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>46. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>47. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>48. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>49. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>50. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>51. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>52. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>53. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>54. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>55. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>56. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>57. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>58. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>59. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>60. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>61. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>62. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>63. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>64. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>65. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>66. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>67. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>68. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>69. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>70. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>71. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>72. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>73. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>74. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>75. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>76. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>77. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
<tr>
<td>78. License Libre du Quebec (LBDQ-1.0)</td>
</tr>
</tbody>
</table>
## 10 Most Common Open Source Licenses

<table>
<thead>
<tr>
<th>License</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIT License</td>
<td>28%</td>
</tr>
<tr>
<td>GNU General Public License (GPL) 2.0</td>
<td>20%</td>
</tr>
<tr>
<td>Apache License 2.0</td>
<td>16%</td>
</tr>
<tr>
<td>GNU General Public License (GPL) 3.0</td>
<td>8%</td>
</tr>
<tr>
<td>BSD License 2.0 (3-clause, New or Revised) License</td>
<td>6%</td>
</tr>
<tr>
<td>Artistic License (Perl)</td>
<td>4%</td>
</tr>
<tr>
<td>GNU Lesser General Public License (LGPL) 2.1</td>
<td>4%</td>
</tr>
<tr>
<td>ISC License</td>
<td>4%</td>
</tr>
<tr>
<td>GNU Lesser General Public License (LGPL) 3.0</td>
<td>2%</td>
</tr>
<tr>
<td>Microsoft Public License</td>
<td>2%</td>
</tr>
</tbody>
</table>

Note: The table above lists the top licenses that are used in open source projects ranked by number of projects using the license, according to the Black Duck Software KnowledgeBase. This data was pulled on October 20, 2016.
An oversimplified summary:

- FOSS Licenses (GPL2, GPL3, Affero GPL, LGPL) are going to require you to make the source code available under the same license for the open source program and for any work you distribute which is based on the program.

- Many other Open Source licenses (Mozilla, CPL) are going to require you to make available modifications you make to the open source program, but not works which interface with it.

- A few open source licenses (Apache, BSD) are going to let you do pretty much whatever you want with the code as long as you give appropriate credit and disclaim all warranties and liability (there is no such thing as a free lunch).
Enforced Sharing: GPL v2

- “[T]he intent is to exercise the right to control the distribution of derivative or collective works based on the Program.”
- “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 all third parties under the terms of this License.”

http://www.gnu.org/licenses/gpl.html
5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License. However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library”. The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.
Enforced Sharing: LGPL

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work ...

b) Use a suitable shared library mechanism for linking with the Library. ...

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. ...

http://www.gnu.org/licenses/lgpl.html
Enforced Sharing: GPL v3

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License...

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.
Enforced Sharing: What is a Derivative Work?

The Copyright Act doesn’t really help for Software:

§ 101, A “derivative work” is a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted. A work consisting of editorial revisions, annotations, elaborations, or other modifications which, as a whole, represent an original work of authorship, is a “derivative work.”

§ 102(b), In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.
Enforced Sharing: What is a Derivative Work?

- Abstraction, Filtration, Comparison Test
  - 2nd, 5th, 10th and 11th Circuit, Computer Associates Intl., Inc. v. Altai, Inc., 982 F.2d 693 (2nd Cir. 1992);
    - Abstract from the original program its constituent structural parts.
    - Filter unprotected portions (incorporated ideas, expression necessary to those ideas, and public domain elements).
    - Compare any and all remaining creative expression with structure of 2nd program to determine whether derivative.
  - 1st Circuit has a modified version that applies the test only after filtering out § 102(b) unprotected elements – particularly methods of operation or control. (Lotus Development Corp. v. Borland Int’l., Inc., 49 F.3d 807 (1st Cir. 1995)).
Enforced Sharing: What is a Derivative Work?

Analytic Dissection Test

- The 9th Circuit has adopted the analytic dissection test (Apple Computer, Inc. v. Microsoft Corp., 35 F.3d 1435 (9th Cir. 1994))

- Are there substantial similarities in both the ideas and expressions of the works? Are the similar features (if any) protected by copyright?

- “Thin” protection is given to non-copyrightable facts or ideas that are protectable because of how they are combined/presented. “Broad” protection is given to copyrightable expression.

- Depending on the degree of protection, court sets standard for comparison of works as a whole to determine if derivative. “Thin” protection requires virtually identical; “broad” protection requires only a “substantial similarity.”
Enforced Sharing: What is a Derivative Work?

Oracle v. Google – protection of APIs

- In 2012, District Court decided that the command structure and taxonomy of the APIs were not protectable under copyright law.

- On May 9, 2014, the Federal Circuit partially reversed the district court ruling, ruling in Oracle's favor on the copyrightability issue, and remanded the issue of fair use to the district court.

- A petition for certiorari was denied by the United States Supreme Court on June 29, 2015.

- A second trial began on May 9, 2016 – Oracle requested 8.8B in damages.

- The trial jury sided in favor of Google, ruling the action to be fair use. (May 29, 2016).
Enforced Sharing: What is a Derivative Work?

> AN OVERSIMPLIFIACTION OF A COMPLEX CASE

- Google wrote its own version of Java for Android using the same “taxonomy of all the names of methods, classes, interfaces, and packages” as Oracle’s Java.

- Question as to copyrightability of a taxonomy/API. Argument that this element of software is purely functional and necessary for technology systems to speak to one another.

- Federal Circuit overruled District Court finding enough creativity for copyright purposes, but sent case back for retrial on the question of Fair Use.

- Google won the retrial ruling the action to be fair use.

- Broad implications for use open source. Does interoperability make everything derivative?
Keys to Open Source

- The key to any open source analysis is the same:
  - Know and understand the facts
  - Read the license
  - Know the norms of the community from which you are taking the source
  - Play nice
GPL v3, LGPL v3, AGPL

- Other commercial concerns:
  - Anti-DRM
    - “No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures. “
  - Anti-tivoization
    - If you convey an object code work ... in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source ... must be accompanied by the Installation Information.
  - Patent License Grant /Patent Non-Assertion as License Condition
  - AGPL Compatibility
Focus is Compliance

- Companies are adopting open source policies and processes:
  - To alleviate litigation concerns
  - As an important M&A Issue
  - To comply with Customer diligence
  - More participation in open source communities: what are your employees contributing?
Elements for an Open Source Program?

- Published Policy
- Open Source Process Owner
- Approval Processes
- Monitoring & Tracking Process
- Obligation Verification Process

And...

As much as I’d like to sell you my services, this is OPEN SOURCE, so check out http://www.linuxfoundation.org/programs/legal/compliance for sample policies.
Be Ready to Comply with the Letter of the Requirements

  - Monitor Software Acquisitions – ignorance is not an excuse.
  - Track you changes and releases – you need to be able to provide the exact code that is shipping.
  - Don’t have a “Build Guru” – users need to be able to successfully build your code. You need to provide the scripts and other materials that are necessary to build and install.
Common Mistakes

- Legalese: make it understandable
- Specific policy that ignores other issues
- Policy too strict so VOA: Violated on Arrival
- Does not allow for edge cases
- Does not provide for modification to meet changes in business model/products
Summary

- Treat the management of open source software as an integrated, cross-functional business process
- Establish policies, define the process and process owners
- Phase the deployment to yield near-term results
- Technology platforms can automate the process, enhance cross-functional collaboration and ensure validation
Questions?

David Rickerby, Esq.

David@bostontechlaw.com

617-848-2616
Cloud Computing Legal Issues

Peter J. Kinsella

*Perkins Coie LLP*

The information provided in this presentation does not necessarily reflect the opinions of Perkins Coie LLP, its clients or even the author.

If you find this article helpful, you can learn more about the subject by going to www.pli.edu to view the on demand program or segment for which it was written.
BIOGRAPHICAL INFORMATION

Pete Kinsella is a partner in Perkins Coie’s Technology, Transactions & Privacy practice. He advises clients on domestic and international licensing, technology and intellectual property matters and is a frequent lecturer on these topics. He has been repeatedly recognized for his legal excellence and was recently named, for the third time in the past four years as Best Lawyer’s “Denver Technology Lawyer of the Year.” Prior to joining Perkins Coie, Pete was a partner with Faegre & Benson and held various in-house legal positions with U S WEST (now CenturyLink) and Honeywell.

Contact Information

Peter J. Kinsella
pkinsella@perkinscoie.com
303-291-2300
1. WHAT IS CLOUD COMPUTING?

a. Although cloud computing has many definitions, generally, cloud computing is the delivery of shared resources or services via the internet. Typically, the resources that are used to provide the cloud computing services:
   i. are pooled;
   ii. can be rapidly adjusted;
   iii. are location independent;
   iv. are widely accessible; and,
   v. are paid for based on usage.

b. A variety of computing services and resources are available as cloud services, including: content (such as streaming audio, video or other information), storage, computing resources, and security threat detection.

c. In many applications, users access the cloud services by either using a web browser or a special application from their computer or portable device.

2. SIGNIFICANT FACTORS DRIVING THE GROWTH OF CLOUD COMPUTING

a. There are several factors driving the growth of cloud computing.
   i. Costs associated with maintaining a traditional internal data center can be reduced by using cloud services, because the cloud resources are typically shared with other customers.
   ii. Cloud services provide the ability to quickly increase or reduce resources to meet demand. This allows a customer to use computing power or storage, on an as needed basis, rather than having to permanently build out their own data center.
   iii. Cloud services provide the ability to have a third party monitor and rapidly deploy security patches and other upgrades.
   iv. Many small and medium sized businesses find that cloud service providers have more expertise than the business can independently hire.
3. DIFFERENT WAYS TO CATEGORIZE CLOUD COMPUTING SERVICES

a. Single Tenant vs. Shared Multi-Tenant
   i. Single Tenant Model
      1. Resources may be administered on a customer by customer basis (e.g., patches could be applied as required by each customer)
      2. Model may be more costly may present scalability issues
   ii. Shared Multi-Tenant
      1. Application is comprised of a single integrated code base that is delivered to multiple customers (e.g., each customer gets the same thing, but different functions may be enabled or disabled)
      2. May be more difficult to implement customizations on a customer by customer basis

b. CaaS vs. Saas vs. PaaS vs. IaaS
   i. Content as a Service (CaaS) - Delivers content to users
      1. Examples: Amazon downloadable books; Wall Street Journal mobile application
   ii. Software as a Service (SaaS) - Provides access to software over the internet, thereby eliminating the need to install and run the software application on the user’s machine
      1. Examples: Google Apps, Gmail
   iii. Platform as a Service (PaaS) - Delivers a platform (a cloud operating system) via the internet and allows “cloud applications” to be built on top of it
      1. Examples: Windows Azure
   iv. Infrastructure as a Service (IaaS) - allows customers to rent underlying computer resources, such as servers, storage and firewall protection
      1. Examples: Box, Dropbox, Amazon EC2
c. **Private vs. Public Cloud Computing**
   i. A public cloud infrastructure provides resources (such as computer applications or storage services) that are shared between multiple unrelated customers.
   
   ii. A private cloud infrastructure typically provides dedicated resources for a single organization. Those resources may be located at the organization’s facilities or from an external location.
   
   iii. A community cloud infrastructure provides shared resources between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.).
   
   iv. A hybrid cloud has combined elements of private, community, or public cloud services.

4. **FREQUENTLY RAISED ISSUES IN CLOUD SERVICE CONTRACTS**

a. **Enforceability of Clickwrap and Browsewrap.**
   
   i. Courts apply traditional principles of contract law to assess the enforceability of online agreements, focusing on whether the party challenging enforcement had reasonable notice of and manifested assent to the terms.\(^1\) Generally, courts differentiate online agreements between “clickwrap” agreements and “browsewrap” agreements. A clickwrap agreement appears on an internet webpage and requires that a customer agree to any terms or conditions by engaging in some affirmative act, such as by clicking on a check box on the screen, in order to proceed with the internet transaction. In contrast, a “browsewrap” agreement occurs where the website provides customers with the ability to view the terms of the agreement, such as through a hyperlink at the bottom of a web page, but does not otherwise require that the customers take any affirmative action to signify their assent to the agreement.

---

ii. Courts routinely enforce clickwrap agreements because notice and assent are more easily established. In contrast, the enforceability of browsewrap agreements involves a more fact-sensitive inquiry in which courts determine whether the customer has “actual or constructive knowledge” of the contract prior to being bound. Actual knowledge is most often obtained through a defendant’s admission of knowledge of the site terms or through the presence of a cease and desist letter that advises the defendant of the existence of such terms. Alternatively, constructive knowledge is typically found where reasonable notice of the terms is provided such that the court can impute knowledge of their existence to the customer. Courts have found notice to be sufficient to impute knowledge where a website provided prominent notice of the hyperlinked terms with easy access to the full agreement. In contrast, courts have held browsewrap


4. See id.


6. See, e.g., Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004) (imputing knowledge of web site’s terms of use to repeated user of Register.com’s database); Major v. McCallister, 302 S.W.3d 227 (Mo. Ct. App. 2009) (upholding browsewrap agreement where each web page contained “immediately visible notice of existence of license terms” and hyperlink to those terms); Southwest Airlines Co. v. BoardFirst, L.L.C., 2007 WL 4823761 (N.D. Tex. 2007) (holding that the defendant had knowledge of and therefore was bound by Southwest’s website Terms and Conditions of Use at least as of the time it was sent a cease and desist letter); Hotels.com, L.P. v. Canales, 195 S.W.3d 147, 154-56 (Tex. App. 2006) (holding that notice of hyperlinked terms
agreements unenforceable where customers were required to scroll down below the fold (i.e., to a secondary or submerged screen) to see the hyperlinked notice, an action which was not necessary to complete their transaction.  

b. Authority to Bind

i. Generally, an agent can bind his principal when the agent has either actual or apparent authority or if the principal ratifies the agent’s agreement. Actual authority may be express or implied, and is triggered by the principal’s objective manifestations to the agent. With apparent authority, the manifestations are made to a third person, and must be made by the principal rather than the purported agent. The principal’s manifestations will support a finding of apparent authority only if (1) they cause the one claiming apparent authority to actually or subjectively believe that the purported agent has authority to act for the principal and (2) the claimant’s actual, subjective belief is objectively reasonable. Such objective manifestations to third parties do not necessarily need to come directly from the principal, but rather can also arise “from authorized statements of the agent.”

Whether apparent authority exists is normally a question of fact. A principal ratifies an agent’s agreement if the principal,

immediately above an “I agree” button next to a click box may be sufficient notice and manifestation of assent).


9. Carl’s Italian Restaurant, 183 P.3d at 640-41; Gaines, S.W.3d at 182-83; King v. Riveland, 125 Wn. 2d at 507.


with full knowledge of the facts: (1) receives, accepts, and retains benefits from the contract; (2) remains silent or fails to repudiate the contract; or (3) otherwise exhibits conduct demonstrating adoption and recognition of the contract.\textsuperscript{14}

ii. Courts generally will apply these same agency contract law principles when evaluating authority to bind in the context of online agreements. For instance, a Massachusetts District Court held that there was no apparent agency as a matter of law where the only relevant conduct by defendant was that it issued the purported agent an e-mail address with the defendant’s corporate domain name.\textsuperscript{15} In denying the plaintiff’s claim of apparent agency in this context, the court cited opinions finding that giving someone a business card with the company name or logo, access to a company car, or company stationery, by themselves, did not create sufficient indicia of apparent authority.\textsuperscript{16} Similarly, a Tenth Circuit Court refused to infer that a corporation’s ownership of an IP address used in connection with an online purchase was sufficient to establish that the individual who agreed to the user agreement from that IP address had authority to bind the corporation.\textsuperscript{17} Finally, where a plaintiff company expressly notified both its employees and the defendant that only three executives were authorized to bind the plaintiff to an online agreement, the court held that unauthorized employees had no actual or apparent authority to bind the plaintiff when they used defendant’s website and agreed to defendant’s online agreements.\textsuperscript{18}

c. **Goods vs. Services laws**

i. Many cloud service contracts have evolved from a software licensing model that in the past were governed by the Uniform Commercial Code (UCC) Article 2. While UCC obligations may be triggered by the delivery of software applications that are used to access the cloud services, generally the UCC doesn’t apply to a pure services contract. This can lead to questions concerning the enforceability of various exculpatory clauses,

\textsuperscript{14} Barnes v. Treece, 15 Wn. App. 437, 443 (1976).
\textsuperscript{16} Id.
\textsuperscript{17} Health Grades, Inc. v. Decatur Memorial Hosp., 190 Fed. Appx. 586 (10th Cir. 2006).
since most case law concerning the interpretation of such clauses arises under the UCC rather than the common law.

ii. Using a traditional license grant clause in a cloud services contract may cause confusion, because it may grant a user rights in the underlying software used to provide the service (i.e., the cloud provider’s software infrastructure) rather than a right to obtain the services provided by the software. Therefore, many cloud service contracts are drafted in the form of a service contract rather than as a license.

1. Compare:
   a. Provider hereby grants customer a non-exclusive right to use the software/services
   b. Provider will use commercially reasonable efforts to provide access to the services set forth in Exhibit A.

d. **Ownership of Custom Developments**
   i. Shared Multi-Tenant – it is difficult for the vendor to convey IP ownership of any service feature, because all customers must use the same service
      1. This is the tradeoff for obtaining the efficiency of using a cloud service model
   ii. Single Tenant - customer ownership of improvements is at least possible, as the customer is able to use a personalized instance of the software

e. **Pricing/Payment**
   i. Many service providers will seek annual payment in advance (may need to address refund issues for certain breaches and termination issues)
   ii. Pay for use - How is “use” determined?
      1. Actual use / number of users/ number of employees
   iii. Price Changes
      1. How frequently can the vendor change pricing?
      2. Are there any limits on the amount that prices can increase?
iv. Does the customer have any rights to obtain prices lower? (e.g., benchmarking right, and obligation on provider to match benchmark price)

v. MFN?

f. **Services Description**
   i. A services description protects both the customer and the provider so that each party understands what services will be provided (and what services will not be provided)
   
   ii. Common items that are included in the services description: technical specifications; published materials; FAQs; and, bug and technical reports


g. **Service Evolution**
   i. The contract should specify the process to changing the service
   
   ii. Can the customer refuse or delay a change?
       1. Changes are often deployed simultaneously to all users in a shared multi-tenant architecture.
   
   iii. What is the process for changing the platform, operating system or application?
   
   iv. Notification?
   
   v. How does pricing work?
   
   vi. Is the data accessible by the customer for other purposes?

h. **Service Levels**
   i. How are service metrics defined? Does the entire service have to be unavailable or only particular portions of the service?
   
   ii. How are service metrics reported?
       1. Does the customer have to request reports or will the reports be automatically delivered?
       2. Does the customer need to complain in order to receive the credit or is the credit applied automatically?
   
   iii. Does the customer need to have access to any vendor tools?
       1. Does the vendor have the necessary rights to allow customers to use the tools?
iv. Does the customer need to report a service issue to obtain a service credit or will a credit be automatically generated?

v. What is the process for strengthening service metrics over time?

vi. Are service credits the sole and exclusive remedy arising from a performance breach?

1. Frequently, vendors will provide service credits as the sole and exclusive remedy for issues concerning the service.

vii. Vendors often want to reserve the right to “immediately” suspend the service in the event of an “emergency” issue. However, the standard for what constitutes an emergency may not be clearly defined other than an event that has or could have the potential of causing a material disruption in service or potential risk to data integrity.

viii. Service Levels Agreements typically have two components:

1. A service component - defines how the services will be provided. Common SLA service components include:
   a. Identification of the services that are to be provided
   b. May identify the services that are not provided
   c. Identification of assumptions underlying service availability
   d. Establishment of service standards (e.g., the timeframes in which services will be provided)
   e. Definition of the responsibilities of both parties

2. A management component - defines the management procedures for tracking the delivery and modification of the services. Common SLA management components include procedures for:
   a. Tracking the availability of the services
   b. Reporting service issues
   c. Resolving service issues
   d. Revising services or service metrics
i. **End User Conduct**
   
i. Cloud service provider contracts often require that customers “ensure” that their end users comply with the vendor’s terms of service. Many sophisticated customers will attempt to soften this requirement. For example, a customer may only want to undertake an obligation to use “commercially reasonable efforts” to cause its users to comply with the terms of service, or simply “inform” its users of the obligations. Other customers may want the vendor to directly contract with the end users.
   
   ii. Vendor terms of service typically prohibit the customer and its end users from engaging in inappropriate activities or using the services to store or process inappropriate content (which activities and content may, or may not be, identified in further detail).
   
   iii. Vendor contracts may require the customer to notify the vendor in the event the customer terms of service are breached.
   
   iv. Vendor contracts typically allow the vendor to suspend or terminate the customer or its users in the event the terms of service are breached, and require the customer to indemnify the vendor against any third party claims arising from the breach. Customers will often try to limit the suspension to: (1) material violations or violations that significantly threaten the security or integrity of the cloud service; and, (2) those end users that actually caused the breach (rather than the customer itself). Customers will also request advance notification of any suspension.
   
   v. Cloud vendor agreements may incorporate by reference additional terms and policies posted to the vendor’s website, such as policies addressing privacy practices and end user obligations concerning the use of the service, which are typically are subject to the vendor’s unilateral amendment. Customers will frequently attempt to require the vendor to provide direct notice in advance of the effective date of any amendments to incorporated terms, along with the right to terminate if such amendments are materially detrimental to the customer’s interests.
   
   j. **Termination and Transition**
   
i. Every contract will end at some time
   
   1. It is important to plan for termination issues prior to contract execution
ii. Contract should address
   1. Duration of termination services
   2. Payment for post-termination services
   3. Transition assistance including data migration
      a. Format of data?
      b. It may not be easy to copy or download the data

k. Disaster Recovery and Mitigation
   i. Does the service provider:
      1. have a business continuity plan?
      2. provide redundant operations from different sites?
      3. routinely test its back-up capability?
      4. routinely attempt to restore data?
   ii. Contract may require the service provider:
      1. to have a data/computing back-up plan
      2. to routinely test its back-up capability
      3. to store back-up on servers located at a separate location
      4. to provide redundant operations from different sites
      5. Consider the impact of bankruptcy on the ability to access data and the ownership of back-up media
   iii. Disaster Recovery
      1. What events cause the service provider to engage in data recovery operations?
      2. Does the contract contain data recovery goals?
      3. What are the consequences if the data is not recovered within the specified time frames?
      4. Who takes priority if multiple customers of the service provider are affected?
      5. How will a force majeure event impact contractual obligations?

l. “Force Majeure” Events
   i. Parties can bargain for effects of “FME”
ii. Consider scope and wording (what is/is not considered FME)

iii. What form of relief is granted (excused from performance, suspension of performance, termination, etc.)?

iv. Does the FME clause override disaster recovery and service level credits?

v. What are the disaster recovery obligations during an FME?
   1. Are some customers contractually prioritized?

m. Data Protection Laws

   i. Data protection and privacy laws should be considered when evaluating a cloud services offering. Different laws may be implicated depending on the nature of the content that is being stored or processed by vendor or the location where the data originates or is processed. Generally, cloud service providers will attempt to shift some or all of the compliance obligations to the end users, because the cloud service provider may be unaware of the actual content being processed or stored in its services. Depending on the circumstances, some of these laws may impose specific security requirements and, may require the imposition of various obligations on subcontractors. Some frequently implicated laws include:

   1. Export Administration Regulations (EAR) / International Traffic in Arms Regulations (ITAR) prohibit the unlicensed “export” of information to foreign nationals and to certain prohibited persons for national security reasons or protection of trade. These laws can be triggered if the employee of the provider has foreign nationals who can access the stored data.


      a. Health Information Technology for Economic and Clinical Health (HITECH) Act. Contains incentives related to development of health care information technology and adoption of electronic health record systems. This Act also widens the scope of privacy and security obligations imposed on service providers
(including their subcontractors) that process or store information.

3. **Family Educational Rights and Privacy Act** (“FERPA”) 20 U.S.C. § 1232g; 34 CFR Part 99 protects the privacy of student education records. Many universities take the position that any education information, including student information databases and faculty and staff email constitutes “education records” for purposes of FERPA and therefore may be outsourced only to vendors that have been designated, and are willing to accept obligations associated with being a “school official” with “legitimate educational interests” in the data under FERPA.


7. **Patchwork of evolving state laws.** Many states impose data security requirements on entities operating in a state or who process data for its residents. For example, Massachusetts has enacted the “Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth” that requires all individuals, corporations, associations, partnerships and other legal entities (regardless of where they are located) that own, license, store or maintain personal information about a Massachusetts resident to develop, implement, maintain and monitor a comprehensive, written information security program applicable to such information.

   ii. **EU Data Protection Act** prohibits export of personally identifiable information from EU to countries that have inferior (as viewed from an EU perspective) data protection laws.
1. Rule: Data must not be transferred to countries outside the EU that do not offer an “adequate level of protection”
   a. Currently only: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay
   b. Exceptions:
      i. ask permission from every “data subject” involved
      ii. US/EU Privacy Shield Adopted by European Commission on July 12, 2016 (US Companies can certify compliance August 1, 2016)
      iii. EU model contract clauses
      iv. “Binding Corporate Rules”

2. From a cloud perspective, EU data protection law will apply when a “controller” is located in its territory; or, when a “controller” outside the EU uses “equipment” within the EU territory. When applied to cloud computing, EU law can be triggered when using an EU-based data center. Many authorities interpret “equipment” in an extremely broad way (e.g., browser cookies).
   iii. Sophisticated customers will often want to review a service provider’s internal security and control policies, audit security and control procedures and impose contractual obligations on the service provider to ensure that the service provider is in compliance and remains in compliance with the applicable laws. Many cloud service providers may have difficulty imposing contractual obligations on their subcontractors. For example, cloud service providers will often subcontract with very large data storage providers (such as Amazon) to provide underlying storage or computing resources.
   iv. Note: Some vendors will attempt to minimize the impact of various laws by: (i) refusing to comply with laws that are triggered by specific content; (ii) providing each customer with encryption tools that do not allow the vendor to access the customer data; and (iii) requiring the customer to warrant that it is legally permitted to have the vendor process the information provided by the customer.
n. **Data Issues**
   i. It is important to
      1. define “data” (e.g., does the definition cover only information that is stored by customer, or does it including information that is created or collected by the cloud service provider in the course of providing the services)
      2. specify ownership rights in the data
      3. specify purposes for which the data may be used
      4. identify the obligations of the parties to comply with data and privacy laws
   ii. Will the vendor be permitted to use the data (or subsets of the data) for other purposes?

o. **Subcontracting**
   i. Does the service provider use subcontractors?
   ii. Can the service provider impose contractual obligations on the subcontractors?
   iii. Does the customer have a right to approve new subcontractors? (or a category of subcontractors, such as those that have access to that data in either encrypted or unencrypted form?)
   iv. What does the approval/disapproval process look like?
   v. Should the customer have a subcontractor termination right rather than an approval right?

p. **Data Center Issues**
   i. Location - Some cloud provider contracts expressly reserve the right to store customer data in any country in which the provider does business. While dispersed geographical storage may be beneficial from a data back-up perspective, it can raise security issues.
   ii. What are the characteristics of the data center?
      1. Security?
      2. Redundant telecommunications, power, and cooling?
   iii. How is data backed-up? On-site? Off-site? How is off-site data protected?
iv. Where is the data stored?

v. Is the data and back-up data encrypted?

q. Security

i. Cloud service providers may offer to provide “commercially reasonable” security for data. In some instances, contracts may also offer to adhere to “industry standard” security practices, without specifying the specific standard. For some customers, it may be beneficial to specify an actual, specific security requirement (e.g., data subject to HIPAA, Gramm-Leach-Bliley, PCI DSS, or the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth) or industry standard (e.g., ISO 27001) that must be followed.

ii. Customers may want to consider the following factors when evaluating the cloud provider’s security:

1. What physical security measures does the vendor use to protect the underlying data centers? Can third parties access the data centers?

2. Is the customer data encrypted in transit and at rest?

3. Does the provider hold the decryption keys or are the keys held only by the customer? If the provider holds the keys, how are the keys protected?

4. Will foreign nationals be able to access the data or decryption keys? If so, this may create export control issues.

5. Who has access to: facilities, infrastructure, platforms, applications, and data?

6. Does the cloud service provider perform background checks on employees who have access to encrypted or unencrypted customer data?

7. Will dedicated equipment, shared equipment or some combination be used to store or process the data?

8. Does the vendor use access controls to prevent unauthorized access to facilities and stored data?
9. Does the vendor regularly perform security audits and penetration testing? Is the vendor under a contractual obligation to take any action if the security audit reveals a deficiency?

r. Security Events
   i. In more complex agreements, it may be important to distinguish between an actual security breach (“Security Incidents”) and a vulnerability (“Security Issues”) and provide different rights, obligations and remedies for each category of issues.

1. Security Issues – are issues with the system that could give rise to a security breach
   a. How are security issues defined?
   b. Objective vs. subjective definition
   c. Are issues in the vendor’s control and those in the control of its subcontractors differentiated?
   d. Does every problem need to be investigated?
   e. Does every problem need to be fixed?
   f. What is the process for fixing the issue?
   g. Is there a specified time frame?
   h. How is the time frame adjusted for fixes that take longer to implement?

2. Security Incidents – are breaches of security
   a. Notice requirement to other party or to end users?
   b. Remediation efforts?
   c. Who does what?
   d. Who pays for remediation efforts?
   e. Does the breach require end-user notification?
   f. Who has legal liability for the incident?
   g. May want to address liability caused by third parties (e.g., hackers)

s. Confidentiality Clauses
   i. May impose a back door security obligation on the service provider
ii. Is the service provider obligated to keep a customer’s information “confidential”?

iii. Some providers will state that they will employ “commercially reasonable efforts” to “protect” a customer’s confidential information

t. Subpoenas/E-Discovery

i. Customers and vendors of cloud services can be compelled to produce data under several mechanisms. It is important to note that in some circumstances, certain categories of vendors are not allowed to voluntarily disclose information to the government.

1. Warrants and Subpoenas

   a. U.S. Law - Fourth Amendment - “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons of things to be searched.”

2. Electronic Communications Privacy Act (ECPA)

   a. The Wiretap Act
   b. Stored Communications Act
   c. The Pen register/Trap & Trace Act

3. Patriot Act (including National Security letters and FISA Warrants)

ii. Typically vendors will:

   1. Try to shift costs and obligations of responding to the client
   2. Expressly reserve the right to disclose information as required by law

u. Data Retention

   i. Customers may want two conflicting obligations:

   1. Vendor should keep the data as long as customer needs it
2. Vendor should promptly destroy it when it is no longer needed

ii. Depending on the service, vendor may not know the content of the data and will be unable to assess legal retention requirements

iii. Contract should specify when data is destroyed

v. **Compliance Requirements**

i. Customer may want the contract to contain procedures for auditing compliance issues:
   1. Does the vendor data center facility allow visitors?
   2. Will the audit disclose too much security information?
   3. Will a customer’s auditor have access to other customers’ data?

ii. Customer may want to impose compliance obligations on the vendor

w. **Risk Mitigation**

i. Typically, the customer wants to impose a combination of the following obligations on the service provider:
   1. Operating procedures
   2. Warranties
   3. Indemnities
      a. Provider contracts rarely include any form of indemnification, but customers frequently ask for such protections in connection with third party intellectual property infringement and inappropriate disclosure or data breach. If the provider provides an indemnity, such obligation will typically cover:
         i. Defense and payment finally awarded judgment
         ii. It will want to exclude combinations created by the customer and data issues arising from the specific data content

4. Software Escrows
   a. Typically, software escrows have little value in many cloud service arrangements, because the customer
will not have the equipment/data center infrastructure to actually utilize the escrow

5. Service Escrows: Situation may be different if service is an “app” running on commercial third party platform

6. Data Escrows?
   a. Data stored with a third party that can be accessed separately by customer

7. Insurance
   a. Contract may require a party to carry certain levels of insurance
   b. CGL policy may not be enough to cover many cyber liability issues
   c. Cyber liability policy may have lower limits for certain categories of damages (e.g., breach notification, credit reporting services)
   d. Requires consultation with broker/agent

x. Warranty Disclaimers
   i. In some jurisdictions, warranty disclaimers must be explicitly negotiated or bargained for.\textsuperscript{19} It is unclear what constitutes adequate negotiation in the commercial context. Cases frequently note that the parties did not discuss the disclaimer term—suggesting a high bar for negotiation—but involve distinguishable factual scenarios where the disclaimer was first presented in a post-sale invoice.\textsuperscript{20} Consumer cases applying the negotiation rule vary; some suggest that knowledge and understanding of the term is sufficient, while others insist that actual


knowledge of the term is not sufficient if the negotiation does not address the terms of the disclaimer and possible defects.21

ii. Other jurisdictions allow a seller to disclaim warranties.22 For example, in Texas, to exclude the implied warranty of merchantability, the contract “must mention merchantability and in case of a writing must be conspicuous[.]”23 In Colorado, implied warranties may be excluded “by a conspicuous writing which states generally that there are no warranties extending beyond the description in the contract.”24

iii. To be conspicuous, a warranty exclusion must reasonably give notice to the person against whom it will operate.25 For example, Texas courts determining conspicuousness consider capitalization, prominent placement,26 setoff from surrounding text, and larger or contrasting type or font.27 Courts are more likely to find a disclaimer conspicuous when the transaction is between commercial entities.28

y. Limitation of Liability

i. Three Categories of Damages

1. Direct damages (basic measure of damages)
   a. Difference between what was promised and what was delivered – service providers will often want to limit their damages to direct damages

23. Id.
26. See id. at 1183-85.
28. See id.
2. Incidental damages
   a. Costs directly associated with obtaining replacement goods or services

3. Consequential damages
   a. Lost profits
   b. Unauthorized disclosure of data will often result in consequential damages (and direct damages too)

4. Issues to consider:
   a. Caps on the “type” of damages
   b. Direct vs. Consequential vs. Incidental
   c. Caps on the “amount” of damages
   d. Exceptions to the one or both of the caps?
      i. Indemnification
      ii. Security Breach

z. Exclusionary Clauses
   i. The enforceability of exclusionary clauses (which include both remedy limitations and disclaimers of liability) can vary widely from jurisdiction to jurisdiction. In most jurisdictions, they are largely enforceable under unless unconscionable. For example, under Washington law, “Exclusionary clauses in purely commercial transactions ... are prima facie conscionable and the burden of establishing unconscionability is on the party attacking it.” When the party seeking to avoid the limitation argues that it should be not be enforced, the court first considers where there are any “indicia of unfair surprise.” That is, was the buyer advised of the limitation term, was the contract short and clear, and was this an arm’s length transaction among competent parties. Compare this to Colorado, which also allows

30. Am. Nursery Prods., 115 Wn. 2d at 222.
general disclaimers of tort liability for the manufacture and sale of products. But, it disfavors such disclaimers, however, and requires that they be “specifically agreed to in negotiations between a commercial seller and commercial buyer.”

ii. Courts may sometime not enforce limits on remedies if the only available remedy fails of its essential purpose. The doctrine is driven generally by concern that contracts should provide at least a fair quantum of remedy for breach of the contract. Many jurisdictions apply two-part test: (1) identify essential purpose of limited remedy; and, (2) identify whether or not limited remedy in fact failed to meet such essential purpose

iii. Cases are mixed as to whether the failure of Essential Purpose Doctrine applies to pure services agreements.

1. Cases declining to apply failure of essential purposes doctrine in a services context

a. Pichey v. Ameritech Interactive Media Services, Inc., 421 F. Supp. 2d 1038 (W.D. Mich. 2006) (“Under Michigan law, the failure-of-the-essential-purpose doctrine applies only to matters falling under Article 2 of the Uniform Commercial Code (“UCC”), Article 2 of the UCC, however, applies only to transactions in goods, not transactions for services. … [T]he doctrine of unconscionability more properly provides the vehicle for determining whether the terms of a services contract are sufficiently one-sided as to undermine the purpose of the agreement.”)

b. Wells v. 10-X Manufacturing Company, 609 F.2d 248 (6th Cir. 1979). (“Article 2 of the Code is intended to have broad application. However, it also follows from the Code’s continued focus on ‘goods,’ the definition of which is cast in terms of a ‘contract for sale,’ that a contract which calls merely for the rendition of services is not subject to the sales provisions of the Code.”)


32. United States Aviation Underwriters, 358 F. Supp. 2d at 1024 (citation omitted).
c. *San Francisco Bay Area Rapid Transit v. GE Transportation Systems Global Signaling, LLC*, 2010 WL 2179769 (N.D. Cal. 2010). ("There simply is no parallel provision in the common law as applied to services contracts and although ‘courts are free to reason by analogy to [the U.C.C.],’ the only other court addressing this particular issue has held that the U.C.C. cases do not apply directly to the limitation of liabilities clauses of a services contract.")

2. Cases that apply the failure of essential purpose doctrine to a services agreement

a. *Jacada (Europe), Ltd. v. International Marketing Strategies, Inc.*, 2004 WL 24267645 (W.D. Mich. 2003) (Court upheld the arbitration award, reasoning that, “the case law does not strictly limit the application of ‘the failure of an essential purpose’ to cases involving the sale of goods.”)


NOTES