



White Paper

Algo IP: Rights in Code

2020 Update

Richard Kemp, Deirdre Moynihan, Chris Kemp

April 2020



ALGO IP: RIGHTS IN CODE – 2020 UPDATE: TABLE OF CONTENTS

A. INTRODUCTION	1
1. Introduction	1
B. APIs: <i>GOOGLE V ORACLE</i>	1
2. Introduction	1
3. The story so far	2
4. What Google copied – a technical example	2
5. The ‘compareTo’ method	3
6. Declarations	3
7. Implementing code	3
8. Methods in the broader context of the Java API	3
9. Two copyright questions for the Supreme Court	3
10. Question one – is the Java API copyrightable?	4
11. Software copyright and the idea-expression dichotomy	4
12. Contrast the EU view – <i>SAS v World Programming</i>	4
13. The ‘merger doctrine’	4
14. Question one – Google’s view	4
15. Question one – Oracle’s view	4
16. Question two – does Google’s use of the Java API constitute ‘fair use’?	5
17. In the US, a jury decides fair use	5
18. Question two – Google’s view	5
19. Question two – Oracle’s view	5
20. Conclusion	5
C. INDIRECT LICENSING: <i>SAP V DIAGEO 3 YEARS LATER</i>	6
21. Introduction	6
22. <i>SAP v Diageo</i> : case summary - facts	6
23. <i>SAP v Diageo</i> : case summary: ruling	6
24. SAP’s new digital access model	7
25. SAP’s new digital access model: comment	8
26. Recommendations	9
D. OPEN SOURCE SOFTWARE: THE AFFERO GPL, THE ‘AS A SERVICE’ WORLD AND THE CAL	10
27. ‘Open Source is eating the software world’	10
28. Shift in OSS benefits from cost to speed	10
29. Shift in OSS risks from licence compliance to security	10
30. Rise of OSS permissive licences and decline of copyleft licences	10
31. Reprise: the FSF, the four freedoms, the GPL and ‘copyleft’	11
32. The ‘border dispute’	11
33. GPLv2/GPLv3 and SaaS	12
34. The AGPL	12
35. The AGPL and ‘modify’	12
36. AGPL and MongoDB	13
37. Recent OSS developments – Holochain and the Cryptographic Autonomy Licence	13
38. A post-OSS world?	13
E. ALGO IP: IP IN ALGORITHMS, COMPUTER GENERATED WORKS AND COMPUTER IMPLEMENTED INVENTIONS	14
39. AI algorithms, software and data	14
40. AI: a set of technologies	14
41. Machine learning: deep, supervised and unsupervised learning	15
42. Machine perception: natural language processing, expert systems, vision and speech	15
43. Machine control: robotics and planning	15



44. AI and intellectual property: software – works/ inventions generated/ implemented by computer	15
45. Copyright – ownership of works generated by AI algorithms	15
46. Copyright – addressing the practical difficulties	16
47. Database right.....	16
48. The Commission’s April 2018 report on database right	16
49. Confidential information and trade secrets	17
50. Patents and inventions	17
51. Recent developments – UK: Formalities Manual, chapter 3.05	17
52. Recent developments – UK: Thaler and DABUS	17
53. Recent developments – EPO: Thaler and DABUS	18
F. ALGO IP: IP IN AI DATASETS, INSIGHTS AND OUTPUTS – THE GROWING IMPORTANCE OF TRADE SECRETS	18
54. Introduction	18
55. Rights of confidence	19
56. The EU Trade Secrets Directive.....	20
57. UK implementation – the join between the TS Directive and UK law of confidence.....	20
58. Trade secrets are emerging as an important way to protect AI data.....	20
59. IP and data – practical points	21
G. COPYRIGHT: TEXT AND DATA MINING - NEW RULES?.....	22
60. The DSM Directive	22
61. Text and Data Mining.....	22
62. Permissible TDM under the DSM Directive	22
63. Article 3’s research exception	22
64. Article 4 and the ‘express reservation’ of TDM rights in an ‘appropriate manner’	23
65. Emerging best practice	23
H. COPYRIGHT: HYPERLINKS AND THE COMMUNICATION TO THE PUBLIC RIGHT	23
66. The InfoSoc Directive and hyperlinking	23
67. Background	24
68. Infringing hyperlinks	24
69. Status/intent of the hyperlinker	25
70. The DSM Directive – press publications and OCSSPs	25
71. Conclusion.....	26
I. CLOUD IP: THE PATENT TROLL THREAT	26
72. Growth of the cloud.....	26
73. The cloud and NPEs	26
74. The NPE perspective	27
75. The perspective of the CSP and its customers.....	27
76. Muted regulatory response to cloud IP issues	27
77. Contractual protection to counter the NPE threat.....	28
J. BREXIT: CODE IP POST-BREXIT TRANSITION	29
78. Introduction	29
79. The Withdrawal Agreement	29
80. Sources of EU copyright-related laws.....	29
81. Implementation into UK law	30
82. ‘Retained EU Law’	30
83. IP rights created on or after 1 January 2021	30
84. New EU legislation	31
K. CONCLUSION	32
85. Conclusion.....	32



ALGO IP – RIGHTS IN CODE: 2020 UPDATE

A. INTRODUCTION

1. **Introduction, scope and purpose.** Even with the rise of the Cloud, SaaS, AI and digital transformation and the growing importance of data, we have perhaps got used in recent years to the idea of software copyright law being relatively stable, with the software directive in the EU and lines of cases in key jurisdictions on ‘look and feel’ settling around generally accepted and workable norms. But the hearing of the Google v Oracle case in the US Supreme Court (now scheduled to take place later in 2020 or perhaps even 2021) pulls the focus back to where the borders of software copyrightability actually now lie, and this, coupled with extraordinary and rapid advances in information technology we’re now living through, prompted us to focus in more detail on what’s happening in the software copyright and related spaces. And when we started to look at the detail, it struck us just how much there is going on. This was the rationale for our 23 April 2020 webinar on ‘Algo IP: Legal Aspects of Software – 2020 Update’, for which this white paper is a companion piece. Building on a collection of blogs on each individual topic, we look at:

- the journey of Google v Oracle to the US Supreme Court, the copyright questions it raises and how the decision could impact software development whichever way it goes (Section B);
- the UK SAP v Diageo case three years on, and what that has meant in practice for indirect licensing (Section C);
- current open source software trends and a more detailed look at the Affero GPL and the ‘as a service’ world and the Cryptographic Autonomy Licence (Section D);
- the questions of who owns IP in algorithms as computer-generated works (copyright) and computer implemented inventions (patents) (Section E);
- the related question of the IP that arises in AI datasets, insights and outputs, with a particular focus on the growing importance of trade secrets (Section F);
- recent copyright developments in the area of text and data mining (Section G);
- recent developments in copyright and the communication to the public right (Section H);
- the patent Troll threat to cloud IP (Section I); and
- a quick crystal ball gaze at Brexit and what it may mean for Algo IP (Section J).

B. APIs: GOOGLE V ORACLE

2. **Introduction.** We billed Google v Oracle as the biggest item on the software legal agenda for 2020 in our ‘Trends in IT Law: looking ahead to 2020’ blog [post](#) back in January. The impact of COVID-19 on the US Supreme Court’s March session means there is a chance the case will figure prominently in our 2021 update too. Few doubt the significance of Google v Oracle. For Google, a judgment in Oracle’s favour would throw “a devastating one-two punch at the software industry” and “wreak havoc on copyright law”.¹ For Oracle, if the decision goes the other way, the Supreme Court will have sanctioned “an egregious act of

¹ Petition for a Writ of Certiorari, Google LLC v Oracle America, Inc. (24 Jan 2019): https://www.supremecourt.gov/DocketPDF/18/18-956/81532/20190124110509177_Google%20cert%20petition.pdf.



plagiarism” and “rewritten” copyright law.² This section, which gives a broad update on the case, is arranged as follows: Paragraph 3 briefly recaps the story so far. Paragraphs 4 to 8 look in detail at a short computer program called the ‘compareTo’ method, which illustrates what Google copied from Java (and what it didn’t). Paragraphs 9 to 18 consider the questions put to the Supreme Court.

3. **The story so far.** The battle between Google and Oracle has been running for so long³ that substantial historical accounts are now beginning to emerge.⁴ But it can be summarised in a few sentences:
 - The key events took place amid the blistering competition for the world’s booming smartphone market in the mid-2000s.
 - Apple released the first iPhone in January 2007, but Google was late – it was still developing Android which it would not release until that November.
 - To spur the adoption of Android by developers, Google copied parts of Java into Android. This meant that developers already using Java wouldn’t need to learn another language to write Android apps.
 - Java was well-established. It had been written by Sun Microsystems in the mid-1990s. Sun was an easy target after the 2008 financial crisis, and was bought by Oracle in 2010.
 - Oracle sued Google for infringing copyright in the Java API a short time later. The litigation has been progressing up (and down) the US courts system since.
4. **What Google copied – a technical example.** Paragraphs 4 to 8 explain the technical aspects of what Google copied from the Java API. The key point is that Google copied the ‘declarations’ (and the broader organisational structure) of parts of the Java API but wrote its own ‘implementing code’.

Figure 1: the ‘compareTo’ method

Oracle JDK 1.5 String.compareTo	Android String.compareTo
<pre>public int compareTo(String anotherString) { int len1 = count; int len2 = anotherString.count; int n = Math.min(len1, len2); char v1[] = value; char v2[] = anotherString.value; int i = offset; int j = anotherString.offset; if (i == j) { int k = 1; int lim = n + 1; while (k < lim) { char c1 = v1[k]; char c2 = v2[k]; if (c1 != c2) { return c1 - c2; } k++; } } else { while (n-- != 0) { char c1 = v1[i++]; char c2 = v2[j++]; if (c1 != c2) { return c1 - c2; } } } return len1 - len2; }</pre>	<pre>public int compareTo(String anotherString) { // Code adapted from K&R, pg 101 int o1 = offset, o2 = string.offset, result; int end = offset + (count < string.count ? count : string.count); char[] target = string.value; while (o1 < end) { if ((result = value[o1++] - target[o2++]) != 0) { return result; } } return count - string.count; }</pre>

² Brief in Opposition, *Google LLC v Oracle America, Inc.*, No. 18-956 (27 Mar 2019): https://www.supremecourt.gov/DocketPDF/18/18-956/93436/20190327160337558_190311%20for%20E-Filing.pdf.

³ Ten years in August.

⁴ For a masterly example, see: Menell, Peter S., ‘Rise of the API Copyright Dead?: An Updated Epitaph for Copyright Protection of Network and Functional Features of Computer Software’ *Harvard Journal of Law & Technology* (2018), Vol. 31, pp. 307-490: <https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech305.pdf>.



5. **The ‘compareTo’ method.** Figure 1 is the centrepiece of our explanation. It is a cutting from a slide deck shown by Google’s lawyers at the first instance trial in 2012. It shows two versions of a short computer program known as a ‘method’ – one from Java (left-hand side), the other from Android (right). The thing to note is that the first lines of each are identical, and the highlighted code differs.

Methods are shortcuts that allow developers to use pre-written code to carry out specific, commonly performed tasks. The method in Figure 1 is called ‘compareTo’. ‘compareTo’ enables a computer to calculate the alphabetical order of different sequences of text. The functionality is like the ‘Sort A to Z’ button you might use when filtering search results on an online shopping website. Even though the code in the different versions of ‘compareTo’ is different, the output is identical – alphabetical order.
6. **Declarations.** The first line of a method is known as the ‘declaration’. This is because it identifies (‘declares’) the method by citing its name and identifying some of its functionality. A developer can use the functionality of compareTo in the program they are writing by ‘calling’ it using a shorthand command derived from compareTo’s declaration: “public int compareTo(String anotherString)”.
7. **Implementing code.** The highlighted code in the main body of compareTo is the ‘implementing code’. This is the code that gives a computer the step-by-step instructions how to execute (‘implement’) compareTo. Clearly there are differences between the implementing code in the Java and Android versions of compareTo. This is because Google rewrote⁵ the implementing code for the Java methods it used in Android, fearing that copying them *would* be an infringement of Oracle’s copyright. Google was also keen that Android was optimised for smaller smartphone processors – hence why the implementing code it wrote is shorter than the Java version.
8. **Methods in the broader context of the Java API.** Stepping back, in simple terms the Java API is a collection of methods which are carefully organised into a logical hierarchy. There are organisational units above methods: classes and packages. The first instance judge described this as “like a library. Each package is like a bookshelf in the library. Each class is like a book on the shelf. Each method is like a how-to-do-it chapter in a book.”⁶ As well as the method declarations, Google replicated the functionality and organisational structure of parts of this library in Android. Google argues that to preserve the functionality of Java in Android (thereby helping developers already familiar with Java) the rules of Java required these aspects to be identical: “to work on the Android platform, Google had to replicate the syntax and structure of the Java API declarations *exactly*”.⁷ The copyright issue at the heart of Google v Oracle lies in the tension between Google’s literal copying on the one hand, and the prescriptive rules of Java on the other.
9. **Two copyright questions for the Supreme Court.** Google has put two copyright questions to the Supreme Court: One – does copyright protection extend to a software interface? Two – does Google’s use of the Java API constitute “fair use”? The following paragraphs set out the law and summarise the positions. Paragraphs 10 to 14 look at question one. 15 to 18 consider question 2.

⁵ In fact, Google’s implementing code pointedly refers to a precedent that pre-dates Java entirely. The first line of the Android implementation of ‘compareTo’ reads: “// Code adapted from K&R, pg 101”. The double forward slashes indicate that this line is a coding note left by the Google developers. “K&R” refers to a book (first published in 1978) called ‘The C Programming Language’ by Brian Kernighan and Dennis Ritchie.

⁶ *Oracle America, Inc. v Google Inc.* (N.D. Cal. 2012): <http://www.groklaw.net/pdf3/OraGoogle-1202.pdf>.

⁷ Petition for a Writ of Certiorari, *Google LLC*.



10. **Question one – is the Java API copyrightable?** The statutory provision at play is Section 102(b) of the 1976 Copyright Act, which sets the boundary for copyright protection in the US. While s.102(a) provides that “original works of authorship” are generally copyrightable, s.102(b) keeps this in check:

“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.”

Part of the answer to question one lies in whether the aspects of the Java API Google copied (the declarations and the organisational structure mentioned at paragraph 4) fall within one of these categories. If they do, they aren’t copyrightable in the first place. The likely candidate is “method of operation”

11. **Software copyright and the idea-expression dichotomy.** But the boundary set by s.102(b) is a fraught one, particularly as it relates to copyright in software. This is because the utilitarian nature of software treads a fine line between the creative expression of original ideas (which copyright can protect) and the ideas themselves (which it cannot) – the so-called ‘idea-expression dichotomy’. In simple terms, it is eminently arguable which is which.

For this reason, courts in the US (and the U.K. and elsewhere) have been reluctant to draw broad conclusions about which bits of software are copyrightable, preferring to reach narrow conclusions on a case-by-case basis. The US Court of Appeals for the Second Circuit neatly captured this perennial uncertainty in a software copyright case from the early 1990s: “... compared to aesthetic works, computer programs hover even more closely to the elusive boundary line described in s 102(b)”.⁸

12. **Contrast the EU view – *SAS v World Programming*.** It will be interesting to see if the US Supreme Court is influenced by the view of the Court of Justice of the European Union (“CJEU”) that “copyright in a computer program does not protect either the programming language in which it is written or its interfaces (specifically, its data file formats) or its functionality from being copied.”⁹
13. **The ‘merger doctrine’.** The merger doctrine is a related aspect of Google’s copyrightability argument. In short, the merger doctrine means that if you can only express an idea or some functionality in one way, that expression is not copyrightable if it would have the effect of extending copyright protection to the idea or functionality itself. The question is whether merger doctrine applies to the declarations and organisational structure (which can only be expressed in one way under the rules of Java – see paragraph 8) that Google copied.
14. **Question one – Google’s view.** Google’s view is that the copied parts of the Java API “easily fit” within s.102(b): “they are a method of operation because they are for *developers* to use.” On the merger doctrine, Google’s position is that “the dispositive, undisputed fact” is that the copied parts of the Java API “cannot be written in any other way”, and that the merger doctrine therefore applies.¹⁰
15. **Question one – Oracle’s view.** Unsurprisingly, Oracle argues the opposite: it “does not seek to protect the ideas embodied in Java”. Instead, it “claims rights only in its particular expression of those ideas.” On the

⁸ *Computer Associates International, Inc. v Altai, Inc.* (2d Cir. 1992): <https://cyber.harvard.edu/people/tfisher/IP/1992%20Altai.pdf>.

⁹ Per *SAS Institute Inc v World Programming Limited* [2013] EWHC 69 (Ch), following *C-406/10 SAS Institute Inc v World Programming Limited*, ECLI:EU:C:2012:259).

¹⁰ Reply Brief for the Petitioner, *Google LLC v Oracle America, Inc.* (11 Mar 2020): https://www.supremecourt.gov/DocketPDF/18/18-956/137903/20200311194254554_18-956%20rb.pdf.



question of merger: “The merger doctrine applies only in the narrow situation where there are very few ways to express an idea. That is not this case.”¹¹

16. **Question two – does Google’s use of the Java API constitute ‘fair use’?** If the Supreme Court finds that the Java APIs are copyrightable, Google will not have infringed Oracle’s copyright if it can prove fair use. Again, the statutory position is codified in the 1976 Copyright Act, at Section 107: “the fair use of a copyrighted work... is not an infringement of copyright”. In determining fair use, s.107 provides that four equally weighted “fair use factors” must be used to guide the analysis. These factors include whether the use is “of a commercial nature” and “the nature of the copyrighted work”. Fair use has been described as “the most troublesome [doctrine] in the whole law of copyright.”¹²
17. **In the US, a jury decides fair use.** There are constitutional reasons for this, but it is also because “juries are simply better positioned than judges to decide the sort of issues that arise in fair use cases”¹³ – which is to say that fair use cases require a complex set of subjective judgments that turn on cultural understandings and norms that are better suited to a diverse jury. One of the reasons *Google v Oracle* is so remarkable from a procedural perspective is that the US Court of Appeals for the Federal Circuit, in finding that Google’s use was not fair in 2018, reversed a jury’s earlier decision that it was – an almost unprecedented step in US judicial history.
18. **Question two – Google’s view.** In Google’s view, the appeals court’s finding that its use of the Java APIs was not fair use “is a dangerous misapplication of the fair-use doctrine with breathtakingly broad implications”. Notwithstanding the reversal of the jury decision, Google argues that the appeals court failed to factor the functional nature of the copied Java APIs into its fair use analysis. This will hand Oracle a “government-granted monopoly” over the functional elements of the Java APIs.¹⁴
19. **Question two – Oracle’s view.** Oracle’s argument is that the scale and purpose of Google’s copying precludes a finding of fair use: “No court has found fair use where, as here, someone copied so much valuable expression into a competing product to serve the same purpose as the original in the marketplace.”¹⁵
20. **Conclusion.** In Google’s characterisation, the global software industry relies on a settled assumption that an API’s implementation (see paragraph 7) benefits from copyright protection but the declarations and organisational structure do not (see paragraph 8). Upsetting this apple cart will, in Google’s words, “impose debilitating retroactive liability” on software developers who reuse aspects of other APIs in this way: they will suddenly find that there is copyright in these declarations and structures, and it belongs to someone else.¹⁶

¹¹ Brief for Respondent, *Google LLC*.

¹² *Oracle America, Inc. v Google Inc.* (Fed. Cir. 2014): <https://cases.justia.com/federal/appellate-courts/cafc/13-1021/13-1021-2014-05-09.pdf?ts=1411173375>.

¹³ Snow, Ned, ‘Who Decides Fair Use – Judge or Jury?’ *Washington Law Review* (2019), Vol. 94, pp. 275-332: <https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=5058&context=wlr>.

¹⁴ Petition for a Writ of Certiorari, *Google LLC*.

¹⁵ Brief for Respondent, *Google LLC*.

¹⁶ Reply Brief for the Petitioner, *Google LLC*.



C. INDIRECT LICENSING: SAP V DIAGEO 3 YEARS LATER

21. **Introduction.** Contractual language to define the scope of permitted software use and to determine charging basis may have been agreed years ago. That language now finds itself applied to new technologies and interfaces in a way that was unanticipated when the agreement was signed. Increasingly, providers are scrutinising customers’ use of their software to ensure that use is in accordance with the terms of the licence and that the charges paid by the customers reflect actual usage of the software. This calls for a combined complex and nuanced legal and technical analysis to establish whether or not day-to-day use of the software is compliant with the permissions and restrictions of the applicable licence.
22. **SAP v Diageo: case summary – facts.** This trend for heightened scrutiny of customer compliance with licence terms is the background to the 16 February 2017 judgment of Mrs Justice O’Farrell in a [case](#) between SAP UK Limited (‘**SAP**’) and Diageo Great Britain Ltd (‘**Diageo**’). Briefly, the facts are as follows:
- From May 2004, Diageo was licensed to use various SAP products, including mySAP ERP (‘**SAP ERP**’) and SAP Process Integration (‘**SAP PI**’). SAP ERP provides a suite of enterprise resource planning functions for managing operations, finance and HR. SAP PI facilitates communication between different SAP systems or between a SAP system and a non-SAP system. The licence to access and use the software – directly or indirectly – was on a Named User basis. Fees for SAP ERP were calculated by reference to various fees for categories of Named User. Fees for SAP PI were calculated on the volume of messages processed by SAP PI. Diageo paid SAP between £50 million and £61 million by way of licence and maintenance fees for the period up to November 2015.
 - In 2011/2012, Diageo used a system that enabled customers to place and review orders and manage their accounts directly with Diageo rather than (as previously) through a call centre (‘**Connect**’) and a platform provided by Salesforce.com to develop an iPad app for the management of customer visits and calls (‘**Gen2**’). Connect and Gen2 interacted with SAP ERP via SAP PI. Messages were passed back and forth between Connect or Gen2 and SAP ERP a few times a day when the SAP ERP was polled for information by Connect or Gen2.
 - SAP claimed that Connect and Gen 2 “used” or “accessed” the SAP systems “directly” or “indirectly” and that Diageo owed additional licensing and maintenance fees totalling in excess of £54million. Diageo contended that SAP PI was a “gatekeeper” for the other SAP applications and that no extra fees were due.
23. **SAP v Diageo: case summary – ruling.** In a trial on liability – but not the amount of damages – the English High Court ruled in favour of SAP. On the plain and obvious meaning of the words in the licence only ‘Named Users’ (as defined) were authorised to access and use SAP ERP, and the extent of their permitted access and use then depended on their user category set out in a schedule to the agreement. Although the terms “access” and “use” were not defined in the licence:

“the plain and obvious meaning of “use” in the context of the Agreement is application or manipulation of the mySAP ERP software. The plain and obvious meaning of “access” in the context of the Agreement is acquiring visibility of, or connection to, the mySAP ERP software.”¹⁷

As regards the Connect customer software:

- The interactions between the SAP ERP and Connect amounted to “indirect” access to the SAP ERP on the

¹⁷ [2017] EWHC 189 at para.77.



basis that each stage of the order process carried out through Connect involved transmissions between Connect and the SAP ERP and that Diageo’s customers (who were not ‘Named Users’ for the purposes of the SAP ERP) accessed or used SAP ERP indirectly through SAP PI when using Connect.

- SAP PI was not a “gatekeeper” for access to other SAP applications. The charges for the SAP PI were in addition to, not instead of, named user charges for the underlying applications.
- The court distinguished the Connect system from the previous system (in which Diageo Named Users would place orders in the SAP ERP) on the basis that there was no interaction between Diageo’s customers and the SAP ERP when orders were placed via the call centre – Diageo Named Users were interacting with the SAP ERP in that situation. Using Connect, however, involved access or use by Diageo customers of the SAP ERP indirectly through the SAP PI.
- No ‘Named User’ category in the schedule applied to the type of access created by Connect to the SAP ERP as the Connect users:

“[did] not have access to source or object code. They [did] not have access to the functionality provided by mySAP ERP in support of the wider operation of Diageo’s business. They [accessed] business process functions and information from the database for the purpose of ordering products and managing their own personal accounts only.”¹⁸

- The amount of any additional licence fees due to SAP would need to be assessed during the damages phase of the trial.

For Gen2 the court reached a similar conclusion.

SAP was therefore entitled to charge Diageo for the access and use of the SAP ERP.

The issues at trial focussed solely on the terms of the agreements between Diageo and SAP. No claims of copyright or database right infringement were brought against Diageo and no claims based on representations as to the scope of the licence were brought against SAP.

24. **SAP’s new digital access model.** Following the decision and discussion and consultation with customers and industry, SAP launched a new digital pricing model for the “use” of its software.¹⁹ This new model gives customers the option to move to a new licensing and pricing model catering for:

- Direct/Human access, chargeable based on named human users; and
- Indirect/Digital Access, access via third party, Internet of Things (IoT), bots and/or other digital access: licensed based on number of transactions/documents processed by the SAP software.

“Use” under the new model is defined broadly, as illustrated by Figure 2. Figure 3 shows the differences between the legacy and new digital access models.

¹⁸ [2017] EWHC 189 at para.89.

¹⁹ See, e.g., https://news.sap.com/wp-content/blogs.dir/1/files/DA_Offer_External-Master_V11_050619.pdf.



Figure 2: use under the new SAP model²⁰

Use of ERP and types of access

One definition of Use and three types of access

“Use” is defined as: “to activate the processing capabilities of the Software, load, execute, access, employ the Software, or display information resulting from such capabilities”.

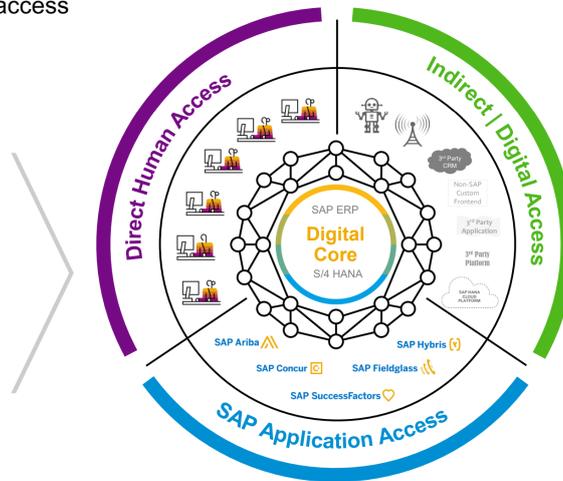
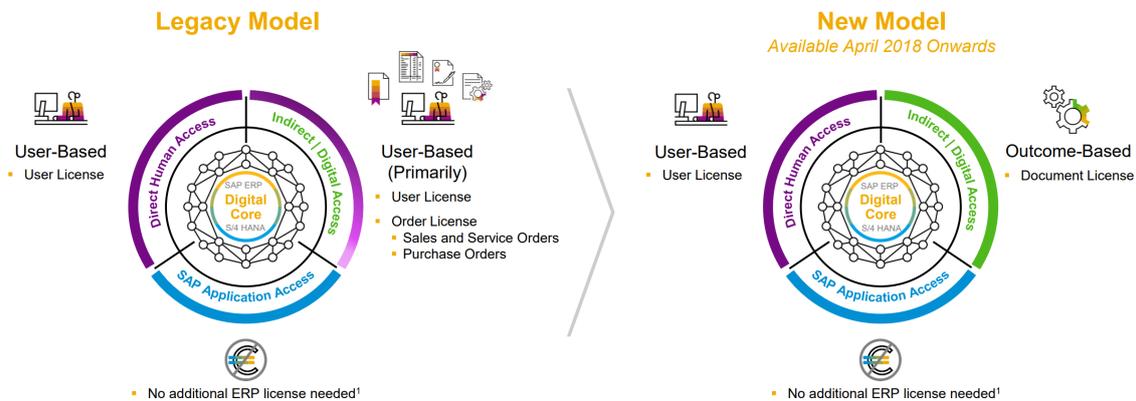


Figure 3 : differences between legacy and new models²¹

SAP modernized ERP Pricing for 21st Century Use

New model for **Indirect | Digital Access** was introduced in April 2018



25. **SAP’s new digital access model: comment.** Although SAP’s stated intention when introducing the new digital access model is to “make it easier and more transparent for customers to use and pay for SAP software licenses”²², the new model remains complex and requires significant analysis to assess whether legacy customers should move to the new licensing model. Neither does the new pricing model reduce the requirement to critically assess whether the actual or intended use is permissible under the terms of SAP’s complex Software Use Rights. Casting a critical and circumspect eye over the relationship between the Ts&Cs and actual use is key – particularly as providers and customers grapple with the fast pace of technological development and the move towards cloud based, customisable, and interoperable IT systems

²⁰ https://news.sap.com/wp-content/blogs.dir/1/files/DA_Offer_External-Master_V11_050619.pdf.

²¹ https://news.sap.com/wp-content/blogs.dir/1/files/DA_Offer_External-Master_V11_050619.pdf.

²² <https://news.sap.com/2018/04/sap-unveils-first-of-its-kind-new-pricing-model/>.



easily accessed via APIs or browser interfaces.

26. **Recommendations.** We therefore continue to recommend that particular attention is paid to the language used in Ts&Cs and how it may apply to different use cases or access rights. Customers should carefully review at the outset of the contract the nature and extent of the rights granted under any licence and the methodology applicable to the calculation of licence and maintenance fees. In these times of rapid technological change, customers should also consider putting in place a structured process to ensure that their use cases across the organisation continue to map to the licence grant and charging clause across the licence lifecycle. The issues for the software provider are the obverse – ensuring a genuine understanding by customers of licence scope and charging terms and backing up the primary contractual obligations with workable audit rights to verify compliance.

For both sides, contractual terms dealing with the following issues should be express, precise and clear so that each party is aware of its obligations:

- types of user – what categories of employees and/or contractors require access?
- nature of access – is it direct log-in via user ID or access via a plug-in, API or other specified indirect method?
- type of access – is it merely pulling information from the customer’s database within the provider’s offering? does it involve use of the functionality provided by the software? If the latter, exactly what functionality is involved?
- scope of licence – what rights are granted to each category of users? Is this linked to the nature and type of access?
- will the contract software interact with other systems in a way that could give rise to licence scope or charging issues for the contract software or the contracts governing the other systems? This will become important as systems built around Artificial Intelligence (AI) and Robotic Process Automation (RPA) increasingly interact with each other indirectly, automatically and without direct human intervention.
- how are the charges calculated? How frequently can the provider increase the charges?
- what rights does the provider have to audit or verify the customer’s use of the software? How frequently can it exercise these rights? In what circumstances should an audit be permitted?
- what changes does the customer intend to make to its IT estate over the life of the contract? Will any of these require changes to the rights granted by the provider and oblige the customer to increase amounts payable to the provider? Can any of these costs be reduced or will they ultimately be passed on to the end customer?
- in what circumstances and on what terms can a customer terminate its licence? How easy is it for the customer to migrate from the incumbent system/software to that offered by a new provider if the charges payable to the incumbent provider increase dramatically? Will the costs of termination and transition be less than the increased costs payable to the incumbent provider?
- pricing model – how does the provider price use? Are there different pricing models for different use types? What’s best value for the customer? How are legacy on premise license fees factored into any move to cloud-based deployments and indirect access subscription-based models?

The analysis is not simply a matter of the legal team reviewing the Ts&Cs – a proper, measured and informed analysis requires a cross functional team of lawyers, software engineers, IT and other relevant business groups. It’s also not a once-off analysis at a single point in time – changes to use will need to be



assessed against the existing use rights to ensure that no additional fees are payable.

D. OPEN SOURCE SOFTWARE: THE AFFERO GPL, THE ‘AS A SERVICE WORLD’ AND THE CAL

27. **‘Open Source is eating the software world’.** As far back as 2013, code audit provider Black Duck observed that “if software is eating the world, open source is eating the software world”.²³ Since then OSS has continued to carry all before it, and in its 2019 analysis²⁴ Synopsys (which acquired Black Duck in December 2017) noted of the codebases it had scanned that:

- OSS was present in 96% of scans, rising to over 99% where the codebase exceeded 1,000 files;
- OSS made up more than 50% of the codebase across 13 out of 17 industry sectors (the exceptions were telecoms, manufacturing, transportation and EdTech); and
- the most common OSS components were JQuery (in 56% of codebases) and Bootstrap (40%).

28. **Shift in OSS benefits from cost to speed.** In the 2010s the key benefit of OSS shifted from cost to speed. Research company Forrester noted in 2019:

“Developers face the challenge of creating differentiated, customized, and compelling customer experiences quickly. As a result, they no longer write all of their own code to solve every problem. Instead, they assemble, configure, and automate their code and often rely on common open source components to quickly add application functionality.”²⁵

29. **Shift in OSS risks from licence compliance to security.** Over the same period key OSS risks also shifted, from licence compliance to security vulnerability. Licence compliance developed in the 2000s:

“as companies played catch up to remedy a landscape of rampant non-compliance ... often in panic, at great expense and managerial angst”.²⁶

But, as the time between disclosure of a vulnerability and its exploitation was constantly shrinking, the continuous rise in OSS uptake led to growing concerns around the time taken to remediate these OSS security issues. In addressing them, the OSS code audit providers became the natural home for OSS security vulnerability auditing and remediation, adding them to their OSS licence, policy management and reporting services as Software Composition Analysis (‘SCA’) providers.²⁷

30. **Rise of OSS permissive licences and decline of copyleft licences.** Within the OSS world there were big changes too, and the 2010s saw a notable rise in the popularity of permissive licences (up from 41% in 2012 to 67% in 2019) and a corresponding drop in use of copyleft licences (down from 59% in 2012 to 33% in

²³ ‘The Future of Open Source 2016’, p.10, Black Duck – <https://www.slideshare.net/blackducksoftware/2016-future-of-open-source-survey-results>.

²⁴ ‘2019 Open Source Security and Risk Analysis’, Synopsys – <https://www.synopsys.com/software-integrity/resources/analyst-reports/2019-open-source-security-risk-analysis.html>.

²⁵ The Forrester Wave: Software Composition Analysis, Q2 2019 – available for example at <https://www.whitesourcesoftware.com/forrester-wave-software-composition-analysis-sca-report/>.

²⁶ Heather Meeker ‘AGPL: Out of the shadows’, 20 September 2016 – <https://www.synopsys.com/blogs/software-security/agpl-affero-gpl-3/>.

²⁷ The Forrester Wave analysis at the preceding but one footnote identified WhiteSource and Synopsys leading a field of ten SCA specialists including Snyk, Sonatype, WhiteHat, Flexera, Veracode, GitLab, FOSSA and JFrog.



2019).²⁸ In particular, between 2012 and 2019 the permissive MIT licence rose from 11% to 27% and Apache from 13% to 23%.²⁹ As shown in Figure 4 below, WhiteSource’s 2020 OSS Licence Guide ranked the top 10 OSS licences in 2019 by share as permissive (MIT, Apache-2.0 and BSD, copyleft (GPLv3, GPLv2 and LGPLv2.1) and weak copyleft (Microsoft Public and Eclipse).

Figure 4: Top 10 OSS Licences in 2019 by share (source: WhiteSource)

	Permissive (non-copyleft)					Copyleft			Weak copyleft	
Licence:	MIT	Apache-2.0	BSD3	BSD2	BSD	GPLv3	GPLv2	LGPLv2.1	MS Public	Eclipse 1.0
Share:	27%	23%	5%	2%	1%	13%	10%	5%	2%	1%

31. **Reprise: the FSF, the four freedoms, the GPL and ‘copyleft’.** By way of quick reprise, OSS is software provided under licence granting the licensee certain freedoms – the difference between OSS and other software lies not in the code but in the licensing terms applied to the code. As espoused by the Free Software Foundation (‘FSF’) set up in 1985 by ex-MIT academic Richard Stallman, these four freedoms are to develop software that is free (i) to run for any purpose, (ii) to be studied and adapted through source code access, (iii) to be redistributed and (iv) to be improved, and for those improvements to be freely redistributable.

Although OSS licensing has raised complex questions around patents, the key innovation in the GPL³⁰ family of licences adopted by the FSF was ‘copyleft’ or ‘inheritance’, the idea that the freedoms guaranteed by the GPL would also apply to new works derived from the original GPL-licensed software. In the FSF’s words:

“copyleft is a general method for making a program free software and requiring all modified and extended versions of the program to be free software as well.”³¹

The legal propagation mechanism for this idea is the GPL licence term that states, broadly, where you modify software originally licensed under the GPL and pass on the modified software, the modifications must also be licensed under the GPL.

32. **The ‘border dispute’.** That the copyleft licensing term ‘works’ is now no longer in doubt, although complex questions remain as to the precise border between modifications that trigger copyleft and those that do not. The copyright analysis of some of these questions is before the US Supreme Court in *Google v Oracle* analysed at Section B. The border also depends to an extent on whether it is GPLv2³² (published by the FSF as long ago as 1991) or GPLv3³³ (2007) that applies.³⁴

Briefly under GPLv2, the copyleft trigger is ‘distribution’; and when the trigger is pulled, the answer to the question ‘*what does GPLv2 cover?*’ is (i) the original program licensed under GPLv2 and (ii) any ‘work based

²⁸ ‘The Complete Guide for Open Source Licences 2020’, White Source – <https://resources.whitesourcesoftware.com/white-papers-datashets/the-complete-guide-for-open-source-licenses-2020>.

²⁹ Source: BlackDuck Software’s top 20 licences of 2012, no longer available.

³⁰ GPL stands for the GNU General Public License, where ‘GNU’ is a recursive acronym for ‘GNU’s Not Unix’, a reference to the FSF’s first project of creating a full operating system to replace Unix.

³¹ <https://www.gnu.org/licenses/licenses.html#WhatIsCopyleft>.

³² <https://www.gnu.org/licenses/old-licenses/gpl-2.0.html>.

³³ <https://www.gnu.org/licenses/gpl-3.0.html>.

³⁴ The third popular licence in the GPL family is the Lesser GPLv2.1 (‘LGPLv2.1’).



on [that] program’ (effectively, a derivative work under copyright law). Under GPLv3, the copyleft trigger changes from ‘distribution’ to ‘conveying’ and when the trigger is pulled, the answer to the question ‘*what does GPLv3 cover?*’ is (i) the original program licensed under GPLv3; and (ii) the ‘Corresponding Source’ (as defined in GPLv3). Effectively, the language of GPLv2 around ‘distribution’ and ‘work based on the program’ changes in GPLv3 to ‘conveying’ and ‘Corresponding Source’.

33. **GPLv2/GPLv3 and SaaS.** GPLv2 was largely pre- ASP (application software provision, or accessing my software on your remote server) and SaaS (software as a service, or accessing your software on your remote server). The correct interpretation of GPLv2 has always been considered to be that use of GPL software on an ASP or SaaS basis was not ‘distribution’ within GPLv2. GPLv3 put this point beyond doubt where it states expressly that:

“mere interaction with a user through a computer network, with no transfer of a copy, is not conveying”.

34. **The AGPL.** Applying copyleft to SaaS to remove this gap was addressed by the GNU Affero GPL version 3 of 2007 (‘AGPL’).³⁵ The AGPL is identical to GPLv3 except for clause 13, which states that making software available over a network triggers the copyleft:

“... if you modify the Program, your modified version must prominently offer all users interacting with it remotely through a computer network (if your version supports such interaction) an opportunity to receive the Corresponding Source of your version by providing access to the Corresponding Source from a network server at no charge”

Clause 13 effectively applies a double condition for copyleft to apply where the AGPL is used. The first is use by remote interaction through a computer network (i.e. covering ASP and SaaS). The second is that the AGPL program has to be ‘modified’. SaaS use of an unmodified AGPL program – most SaaS use – therefore does not trigger copyleft.

35. **The AGPL and ‘modify’.** ‘Modify’ is defined in the AGPL (as it is in GPLv3) as meaning to:

“copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy.”

What this means in turn throws you back on the detailed, technical copyright law questions of the type being considered in *Google v Oracle*:

- has code been copied?
- if so is that copying substantial?
- has functionality been replicated in a way that potentially infringes copyright?
- does the fair use doctrine apply?

In the international context (where ‘modifying’ AGPL code takes place outside the US), the following additional questions also apply:

- which country’s laws will apply to determine infringement? (This is normally the country where the alleged infringement took place. The question is relevant because ‘adaptation’ in a copyright sense has different meanings under UK and US law for example); and

³⁵ <https://www.gnu.org/licenses/agpl-3.0.html>.



- where the AGPL is invoked by way of defence to infringement proceedings, under which US state's or country's laws will the AGPL be interpreted as a contract or copyright licence?
36. **AGPL and MongoDB.** The AGPL achieved early success, being adopted by the popular 'NoSQL' cross-platform database program MongoDB in 2009. However, uptake has been inhibited by challenges in extending conventional OSS licence compliance and internal policies – which largely addressed distribution to outside the organisation – towards imposing internal use controls on the 'as a service' access envisaged by AGPL clause 13. AGPL adoption was also dealt a blow when MongoDB, Inc. moved away in October 2018 from the AGPL to a new licence (MongoDB's Service Side Public Licence³⁶) so that now, according to TechRepublic, AGPL's share of open source projects is "virtually zero (as in "none")."³⁷
37. **Recent OSS developments – Holochain and the Cryptographic Autonomy Licence.** One of the most recent OSS licences to be approved by the Open Source Initiative ('OSI') as meeting the requirements of the Open Source Definition ('OSD') is Holochain's [Cryptographic Autonomy Licence](#) ('CAL'). By way of background, Holochain is:
- "is an energy efficient post-blockchain ledger system and decentralized application platform that uses [P2P] networking for processing agent centric agreement and consensus systems between users."³⁸
- On 20 February 2020 Holochain [released](#) the CAL as "the first licence specifically designed to protect end users' rights and ownership of data and control of their cryptographic keys – and by extension their security". The licence can be described as 'AGPL +' as, like the AGPL, it requires a redistributor providing either the software or access to it over a network to make available source code to any modifications it makes (clause 2.1) under the terms of the CAL or compatible licence (clause 4.1.2).
- The '+' in the CAL is novel requirement at clause 4.2 to "maintain user autonomy" of data processed using the Holochain software: effectively, the licence bars use of Holochain with distributed ledger applications that restrict a user from accessing cryptographic keys controlling their own data:
- "We want Holochain apps to be trusted as maximizing end-user autonomy and control. As that starts to happen, we can't let someone claim their software is a "Holochain" app if they are actually maintaining central control of end-user cryptographic keys."³⁹
- The CAL went through a number of iterations before OSI approval and prompted lively debate around the implicit extension of OSS freedoms and principles beyond software copyright to APIs and data. The last point to be settled was whether requiring sharing of the user's own data was compatible with the bar on field of use restrictions at OSD paragraph 6. Although the OSI decided that it was compatible, the point caused sufficient controversy to lead to the resignation of OSI co-founder [Bruce Perens](#) in January 2020 shortly before the CAL was approved.
38. **A post-OSS world??** The decline of the GPL licence family from a share of just under 60% in 2012 to 33% a few years later, coupled with their effective absence from the SaaS world, are striking and show little sign of changing. Developer convenience and the desire to avoid complexity, whether in licensing or platforms,

³⁶ <https://www.mongodb.com/licensing/server-side-public-license>.

³⁷ Matt Asay 'Don't believe the hype, AGPL open source licensing is toxic and unpopular', TechRepublic, 5 September 2017, <https://www.techrepublic.com/blog/10-things/dont-believe-the-hype-agpl-open-source-licensing-is-toxic-and-unpopular/>.

³⁸ 'WTF is Holochain', 9 March 2017.

³⁹ Arthur Brock, [Understanding the CAL](#), 22 February 2020.



appear to be behind this powerful trend. It would certainly explain why the MIT License – at less than 200 words⁴⁰ – is the most popular software licence on the GitHub software development version control platform. In fact as the TechRepublic article noted, “this shift toward permissive licensing has become so pronounced that on GitHub it’s still far too common for projects not to have a license [and] the GitHub generation is having to be coaxed into slapping on a license at all.”⁴¹

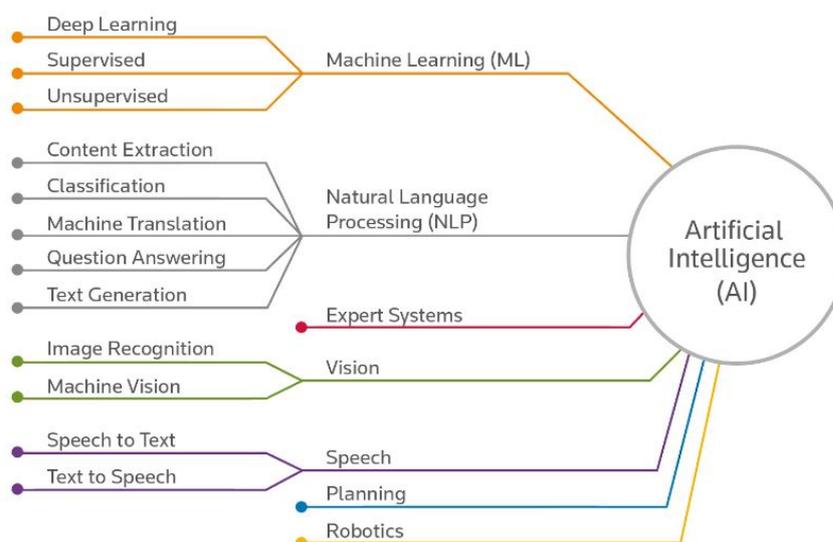
E. ALGO IP: IP IN ALGORITHMS, COMPUTER GENERATED WORKS AND COMPUTER IMPLEMENTED INVENTIONS

39. **AI algorithms, software and data.** “It’s only AI when you don’t know what it does, then it’s just software and data” remains a useful heuristic to get to grips with AI algorithms. In legal terms, AI is a combination of software and data. An algorithm is a set of rules to solve a problem. The implementation in code of the algorithm is the software that gives instructions to the computer’s processor. What distinguishes an AI algorithm from traditional software is first, that the algorithm’s rules and software implementation are themselves dynamic and change as the machine learns; and second, the very large datasets (‘big data’) that the AI algorithm processes. The data is (i) the input training, testing and operational datasets; (ii) that input data as processed by the computer; (iii) the output data from those processing operations; and (iv) insights and data derived from the output data.

This section of looks at IP rights in algorithms and section F considers the IP rights that arise in relation to AI input and output data, insights and derived data, particularly from the standpoint of trade secrets.

40. **AI: a set of technologies.** AI is a set of technologies not a single one and is best observed as a number of streams as shown in Figure 5. The main streams are machine learning, natural language processing, expert systems, vision, speech, planning and robotics.

Figure 5: The main AI streams⁴²



⁴⁰ <https://opensource.org/licenses/MIT>

⁴¹ See previous footnote.

⁴² FullAI at <http://www.fullai.org/short-history-artificial-intelligence/> citing Thomson Reuters as source.



41. **Machine learning: deep, supervised and unsupervised learning.** Machine learning is the technique by which computers learn by example or by being set goals and then teach themselves to recognise patterns from the examples or reach the goal without being explicitly programmed to do so. The three main subsets of machine learning are deep, supervised and unsupervised learning. **Deep learning** has emerged as AI's 'killer app' enabler and uses large training datasets to teach the AI algo software to accurately recognise patterns from images, sounds and other input data. In **supervised learning**, the AI algorithm is programmed to recognise a sound or image pattern and is then exposed to large datasets of different sounds or images that have been labelled so the algorithm can learn to tell them apart. Labelling is time consuming, expensive and not easily transferable, so in **unsupervised learning** the data is unlabelled and the system is set a particular goal – to reach a high score in a game for example – and the algorithm is then exposed to large unlabelled datasets that it instructs the computer to process to find a way to reach the goal.
42. **Machine perception: natural language processing, expert systems, vision and speech.** Machine learning techniques when combined with cameras and other sensors are accelerating machine perception – the ability of AI algorithms to recognise, analyse and respond to the data around them and 'see', 'hear', 'listen', 'speak' and 'reason'. **Natural language processing** has emerged as a primary human user interface for AI. Enabled by accurate voice recognition, NLP algorithms respond to one-way user input requests and interact in two-way conversations. An **Expert System** emulates human decision-making skills by applying rules (from its 'inference engine') to the facts in the system (its 'knowledge base'). **Vision** is currently the most prominent form of machine perception, with AI algorithms trained to recognise faces, objects and activity. Machine perception has developed quickly in **speech**, where the error rate now matches humans'.
43. **Machine control: robotics and planning.** Machine control is the design of robots and other automated machines using control mechanisms to enhance the speed and sensitivity of machine response in 'sensing→planning→acting'. Machine control adds movement in and manipulation of an interactive environment to the combination of machine learning and machine perception in a static environment.
44. **AI and intellectual property: software – works/inventions generated/implemented by computer.** AI will provide a significant impulse to the development of intellectual property law, particularly as dynamic AI algorithms start to enable computers to generate new works (in terms of copyright) and invent and discover novel ways of doing things (in terms of patent law).
45. **Copyright – ownership of works generated by AI algorithms.** Who owns copyright works generated by AI algorithms without immediate or direct human intervention? Here the background is that s.9 of the UK Copyright Designs and Patents Act 1988⁴³ ('CDPA') provides that that author of software (as a literary work) is the person who creates it (s.9(1) CDPA) and that the author is the work's first owner (s.11) unless it was created by an employee in the course of his employment, when the employer is the first owner (s.11(1)). By s.9(3) CDPA:

"[i]n the case of a literary, dramatic, musical or artistic work which is computer-generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken"

where "computer-generated" is defined at s.178 CDPA as meaning "that the work is generated by computer in circumstances such that there is no human author of the work."

⁴³ <http://www.legislation.gov.uk/ukpga/1988/48/contents>



46. **Copyright – addressing the practical difficulties.** These operative terms are fraught with difficulty in a practical sense. There has been no significant UK case law to date to clarify what is meant by “undertaking necessary arrangements” for the creation of the work where “there is no human author” so the growing ubiquity of AI algorithms is likely to lead to clarification of these terms through the courts. Parties to agreements for AI algorithm system development and use that could result in new copyright works should consider including any necessary express terms as to their ownership, assignment and licensing. Consideration should therefore be given to a range of questions including addressing and recording:
- the extent of the work(s) concerned, particularly in the case of a dynamic AI algorithm;
 - whether or not one or more human authors can be identified;
 - if so, who they are and how ownership will be addressed. This will be important bearing in mind the UK rules on joint authorship and co-authorship at ss. 10 and 11 CDPA and the intricate position of copyright co-ownership under UK law; and
 - if not, what are “arrangements necessary for the creation of the work” for the purposes of s.9(3) and how they are “undertaken”.
47. **Database right.** Database right is separate from copyright and applies only in the EU to confer on the maker of a database there the right to prevent unauthorised extraction or reutilisation of the database’s contents.⁴⁴ A “database” is essentially a searchable, systematically arranged collection of independent works or data (s.3A(1) CDPA). The maker of the database is the first owner of database right (Reg. 15 CRDR) and the database “maker” is “the person who takes the initiative ... and assumes the risk of investing” in its contents (Reg. 14(1) CRDR). Unlike copyright, the rules on ownership of database right do not envisage computer-generated databases, but the ownership position still raises a number of considerations. For example, it could mean that the maker of a database using data generated by sensors or other technology is the manufacturer of the sensor/technology rather than the entity deploying or using the sensor/technology for specific purposes.
48. **The Commission’s April 2018 report on database right.** Database right has proved to be a thorny issue for the EU particularly in the AI context. A Commission staff evaluation report of 25 April 2018 concluded that database right should be retained, although highlighting widely articulated issues around creating and obtaining data, especially in the era of IOT sensor and machine generated databases and the very large datasets processed by AI/ML software:
- “... it is assumed that [database] right does not apply to databases that are the by-products of the main activity of an organisation. This means that [database] right does not apply broadly to the data economy (machine-generated data, IoT devices, big data, AI, etc.); it only covers databases that contain data obtained from external sources (for example industries like publishers, who seek out data in order to commercialise databases).”⁴⁵

⁴⁴ Directive 96/9/EC of 11 March 1996 on the legal protection of databases - <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML>, implemented into UK law by the Copyright and Rights in Databases Regulations 1997 (‘CRDR’) – <http://www.legislation.gov.uk/ukxi/1997/3032/contents/made>

⁴⁵ Page 2, Executive Summary of the the Evaluation of Directive 96/9/EC on the legal protection of databases, European Commission, 25 April 2018 - <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-and-executive-summary-evaluation-directive-969ec-legal-protection>.



49. **Confidential information and trade secrets.** AI algorithms and software are most likely to be confidential to and trade secrets of the developer, and secrecy provides another and increasingly important string to the bow of IP protection. These aspects are considered in greater detail at section F below in relation to AI datasets.

50. **Patents and inventions.** Use of algorithms may result in new inventions and the question arises whether computer implemented inventions are capable of patent protection. S.1(2)(c) Patents Act 1977 ('PA') excludes "a program for a computer" from patent protection to the extent that the patent application "relates to that thing as such".⁴⁶ This has led to a line of cases in the UK since 2006 which has sought to establish and clarify a test for determining the contribution that the invention makes to the technical field of knowledge (potentially patentable) beyond the computer program "as such" (not patentable).⁴⁷ If the invention is potentially patentable on this basis, s.7(3) PA provides that:

"[i]n this Act "inventor" in relation to an invention means the actual deviser of the invention and "joint inventor" shall be construed accordingly"

and s.7(2)(a) PA provides that a patent for invention may be granted "primarily to the inventor or joint inventors". US law is more specific in defining (at 35 USC §100(f) and (g)) "inventor" as "the individual or, if a joint invention, the individuals collectively who invented the subject matter of the invention". The context of s.7(3) PA means that the "actual deviser of the invention" should be a "person" and there is no regime similar to that for copyright for computer-generated works.

Again, the takeaway from the patent law perspective is also that it is worth considering expressly covering in AI contracts the ownership, assignment and licensing aspects of AI-generated inventions and patent rights as well as copyright works.

51. **Recent developments – UK: Formalities Manual, chapter 3.05.** The UK Intellectual Property Office ('IPO') recently updated its Formalities Manual to specifically provide that an AI cannot be listed as an inventor of a patent in a patent application because an AI is not a person and that failure to list a human person as an inventor will lead to withdrawal of the patent application under s13(2) of the Patents Act 1977:

"Where the stated inventor is an 'AI Inventor', the Formalities Examiner request a replacement F7. An 'AI Inventor' is not acceptable as this does not identify 'a person' which is required by law. The consequence of failing to supply this is that the application is taken to be withdrawn under s.13(2)."⁴⁸

52. **Recent developments – UK: Thaler and DABUS.** In a decision on 4 December 2019 (Thaler/DABUS), the applicant, Mr Thaler, filed statements of inventorship stating that the inventor was "an AI machine called 'DABUS'" and that the applicant acquired the right to grant the patents in question by "ownership of the creativity machine DABUS". The Hearing Officer concluded:

"I have found that DABUS is not a person as envisaged by sections 7 and 13 of the Act and so cannot be considered an inventor. However, even if I am wrong on this point, the applicant is still not entitled to

⁴⁶ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/354942/patentsact1977011014.pdf.

⁴⁷ Starting with *Aerotel Ltd v Telco Holdings Ltd* and *Macrossan's Patent Application* [2006] EWCA Civ 1371.

⁴⁸ UK IPO, Formalities Manual (28 October 2019), Chapter 3.05 – <https://www.gov.uk/guidance/formalities-manual-online-version/chapter-3-the-inventor>.



apply for a patent simply by virtue of ownership of DABUS, because a satisfactory derivation of right has not been provided. The applications shall be taken to be withdrawn"⁴⁹

53. **Recent developments – EPO: Thaler and DABUS.** In decisions on applications at EPO level with effectively the same subject matter,⁵⁰ the European Patent Office ('EPO') also refused Mr Thaler's application in relation to DABUS:

"In both applications a machine called "DABUS", which is described as "a type of connectionist artificial intelligence", is named as the inventor. The applicant stated that he had acquired the right to the European patent from the inventor by being its successor in title, arguing that as the machine's owner, he was assigned any intellectual property rights created by this machine.

In its decisions, the EPO considered that the interpretation of the legal framework of the European patent system leads to the conclusion that the inventor designated in a European patent must be a natural person. The Office further noted that the understanding of the term inventor as referring to a natural person appears to be an internationally applicable standard, and that various national courts have issued decisions to this effect.

Moreover, the designation of an inventor is mandatory as it bears a series of legal consequences, notably to ensure that the designated inventor is the legitimate one and that he or she can benefit from rights linked to this status. To exercise these rights, the inventor must have a legal personality that AI systems or machines do not enjoy.

Finally, giving a name to a machine is not sufficient to satisfy the requirements of the EPC mentioned above."⁵¹

The patent law position, both in the UK and more generally, therefore currently provides greater clarity than the copyright and database rights positions.

F. ALGO IP: IP IN AI DATASETS, INSIGHTS AND OUTPUTS – THE GROWING IMPORTANCE OF TRADE SECRETS

54. **Introduction.** Whether a large cloud operator providing AI as a Service, a specialist AI developer licensing its AI software on premise to its customers, or a customer looking to capture the most value from the AI systems it uses, organisations are attributing increasing value to the data that their AI algorithms process. The data may be characterised as:

- input data – training, testing and operational datasets input into the AI software;
- that data as processed by the AI;
- output data – from those processing operations; and
- insights and data derived from the output data.

⁴⁹ UK IPO, BL O/741/19, Applicant: Stephen L Thaler (4 December 2019) <https://www.ipo.gov.uk/p-challenge-decision-results/o74119.pdf>.

⁵⁰ Grounds for the Decision relating to EP 18 275 163 (27 January 2020) – <https://register.epo.org/application?documentId=E4B63SD62191498&number=EP18275163&lng=en&npl=false>; Grounds for the Decision on EP 18 275 174 (27 January 2020) – <https://register.epo.org/application?documentId=E4B63OBI2076498&number=EP18275174&lng=en&npl=false>.

⁵¹ 'EPO publishes grounds for its decision to refuse two patent applications naming a machine as inventor, 28 January 2020', EPO Press Release, 28 January 2020 – <https://www.epo.org/news-issues/news/2020/20200128.html>.



Legally inert in and of itself, an increasingly wide range of rights and duties arises in relation to data.⁵² As regards IP, these are principally copyright, database right (in the EU), confidentiality and (since 2018) trade secrets. IP rights in relation to data are broad, as they are enforceable the whole world (*'in rem'*), but shallow, as they are currently of uncertain scope and infringement is challenging to prove. On the other hand, contract rights relating to data are narrow, as they are only enforceable against a contracting party (*'in personam'*), but deep, as breach is proved as a question of fact once the contractual obligation has been established. In practice, contract remains king in data land: the \$30bn global financial market data industry has grown up over the last 40 years around stable contract norms with little litigation.

55. **Rights of confidence.** Copyright and database right each protect the expression and form of information not its substance. This, coupled with the dynamic nature of AI data as inputs, outputs and insight, can make copyright and database rights challenging to apply to data. Equitable rules protecting confidentiality of information may however provide a better form of IP protection as they can protect from disclosure the substance of data that is not publicly known. Under UK law, protection extends in three steps. The first is the classic statement of the requirements for a successful breach of confidence action by Megarry J. in the 1969 case *Coco v AN Clark (Engineers) Ltd*.⁵³

“in my judgement, three elements are normally required if, apart from contract, a case of breach of confidence is to succeed. First, the information itself... must “have the necessary quality of confidence about it.” Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it.”⁵⁴

To be protectible in this way, the information must therefore be shown both to be confidential and acquired under a duty of confidence.

In the second step, protection can extend to the aggregation of information even where parts of it are in the public domain and so not otherwise confidential. This is the result of a line of cases⁵⁵ in the last three of which – called the ‘wireline’ cases – the information concerned was essentially in the public domain but the courts held that the structure of the information in its aggregated form was not and so was protectible as confidential.

As the duty of confidence goes to the substance, and not just the form, of data, the third step is that protection can extend to trace through to later generations of data derived from the initial confidential data, potentially through the mechanism of a constructive trust.⁵⁶

⁵² For further detail, please see our white paper, ‘Legal Aspects of Managing Data’, 14 November 2019 – <http://www.kempitlaw.com/white-papers/legal-aspects-of-managing-data/?id=80>.

⁵³ [1969] RPC 41 (HC).

⁵⁴ See ‘Gurry on Breach of Confidence’, second edition, OUP 2012, paragraph 2.139, page 70.

⁵⁵ *Albert (Prince) v Strange* ([1849] 1 M&G 25); *Exchange Telegraph Co. Ltd v Gregory & Co.*, ([1896] 1 QB 147); *Exchange Telegraph Co. Ltd v Central News Ltd* ([1897] 2 Ch 48); *Weatherby & Sons v International Horse Agency and Exchange Ltd*, ([1910] 2 Ch 297). The last three are the ‘wireline’ cases.

⁵⁶ See ‘Gurry on Breach of Confidence’, supra, paragraphs 20.17 - 20.25, pages 787 – 790.



56. **The EU Trade Secrets Directive.** The EU Trade Secrets Directive⁵⁷ (**'TS Directive'**) brings EU law more closely into line with Article 39 of the WTO TRIPS Agreement⁵⁸ (which gives IPR protection to trade secrets as undisclosed information) and the US Uniform Trade Secrets Act⁵⁹. Article 2(1)(a) TS Directive sets out that a trade secret has three elements – secrecy, commercial value and steps taken to keep it secret. It defines a trade secret as:

“information which ...

- (a) ...is secret in the sense that it is not as a body or in the precise configuration and assembly of its components generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- (b) has commercial value because it is secret; and
- (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.”

57. **UK implementation – the join between the TS Directive and UK law of confidence.** The TS Directive came into effect in the UK on 9 June 2018 through the Trade Secrets (Enforcement, etc.) Regulations 2018 (**'TS Regs'**).⁶⁰ As to the 'join' between the TS Directive and the UK law of confidence, the Explanatory Notes to the TS Regs confirmed that:

“the issue of whether the acquisition, use or disclosure of a trade secret is unlawful is determined by reference to the principles of the law of confidence” (i.e. UK law deals with disclosure and breach);

and

“[w]here the measures, procedures and remedies available in an action for breach of confidence offer wider protection to a trade secret holder than that offered under the [TS Regs], the trade secret holder may apply for, and a court may grant, them provided they comply with [certain safeguards set out in Article 1 of the TS Directive]” (i.e if UK law gives broader rights, a claimant can invoke them).

58. **Trade secrets are emerging as an important way to protect AI data.** In a study in 2017, the EU Intellectual Property Office (**'EU IPO'**) found⁶¹ that (i) the use of trade secrets to protect innovation was higher than patents for most companies, in most sectors and in all EU Member States; (ii) trade secrets were more likely to be used than patents in innovation in process and services; and (iii) trade secrets were preferred to patents in strongly competitive markets. In a legal environment where attaching IP rights to data is challenging, trade secrecy is therefore emerging as the most likely candidate right, especially in a more digitally connected, AI- and cloud- enabled world. This is because the area of trade secrecy is relatively structured and harmonised and interoperates benignly with national (common or equitable) laws of confidence. However, there remain significant challenges, with a number of key questions to be addressed:

⁵⁷ Directive 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L157/2016) - <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943&from=EN>.

⁵⁸ World Trade Organisation Agreement on Trade-Related Aspects of Intellectual Property Rights https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.

⁵⁹ <http://www.uniformlaws.org/Act.aspx?title=Trade+Secrets+Act>.

⁶⁰ SI 2018/597 - <http://www.legislation.gov.uk/ukSI/2018/597/made>.

⁶¹ 'Protecting innovation through trade secrets and patents: determinants for European Union firm', EU IPO, 2017 - https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade%20Secrets%20Report_en.pdf



- how do you evidence ownership?
- how do you show secrecy and prevent erosion in a world where big data is increasingly digitally accessible?
- how do you identify a trade secret when, as in AI, dynamic and changing variables are a key feature of the algorithm or dataset?
- what constitutes reasonable steps to keep data secret – must you apply standards similar to the GDPR and NIS Directive to take ‘appropriate technical and organisational measures’?
- how do you document and keep trade secret records when the algo or dataset is dynamic and changing?

The next few years are likely to see sustained efforts to remove these perceived impediments to a robust and efficient trade secret legal regime.

59. **IP and data – practical points.** Market participants aiming to maximise their data IP rights should consider the following steps:

- asserting (by contract and by website, documentation and other relevant notices) copyright, database right, confidentiality and trade secrets for input, output and insight data;
- ensuring across all website and other notices and contracts that all relevant data is stated to be confidential and trade secret in order to minimise leakage;
- documenting the secrecy of data, its commercial value and steps taken to keep it secret (perhaps by an ‘appropriate technical and organisational measures’ standard similar to GDPR and the NIS Directive) to maximise the availability of trade secret protection;
- taking a contractual acknowledgement from the counterparty that information disclosed is confidential to the organisation, that the organisation is the trade secret holder and that the information is secret, has commercial value and has been subject to reasonable steps in the circumstances to keep it secret;
- asserting in written methodologies and specifications that the way in which the contents of database(s) and dataset(s) concerned are selected and arranged is the product of the author’s own intellectual creation in order to maximise the likelihood of database copyright availability;
- ensuring relevant documentation shows substantial ‘OVP-ing’ investment in collecting the data in the database as well as creating it so as to maximise the likelihood of database right availability;
- considering the copyright position as a whole, taking into account literary copyright in information architecture and documents associated with the data;
- taking effective assignments of present and future copyright and database right (and as necessary, trade secrets and confidential information) in all relevant contracts; and
- reviewing the contractual definitions of:
 - confidential information so as to assess what data is included and ensure it covers trade secrets;
 - IP rights so as to assess whether confidential information and trade secrets are included; and ensure consistency of treatment between data as confidential information and data as IP rights; and
 - derived data to ensure that it aligns to your interests.



G. COPYRIGHT: TEXT AND DATA MINING - NEW RULES?

60. **The DSM Directive.** The new EU Directive on Copyright in the Digital Single Market⁶² (the ‘**DSM Directive**’) has been fraught with controversy and discussion. Many have argued it will lead to the death of the Internet as we know it because of its provisions on upload filters and the link tax. Those points are outside the scope of this section which focuses on a new and potentially valuable right in the data analytics field but you can find more information on them on our blogs and vlogs at www.kempitlaw.com.

61. **Text and Data Mining.** Article 2(2) of the DSM Directive defines text and data mining (‘**TDM**’) as:

“any automated analytical technique aimed at analysing text and data in digital form in order to generate information which includes but is not limited to patterns, trends and correlations”.

The ability to legally perform TDM is becoming increasingly important as new methods and technologies are created to perform sophisticated data analytics and provide new services based on such analytics. Technically, most TDM software/activities require a copy of the content to be TDM-ed. Currently, however, in the UK and EU, there is no blanket exception from copyright or database right protection that allows TDM: copying third party text or data for analytics purposes requires a licence from the rightsholder or reliance on the limited and narrowly construed fair dealings defences. (This is in contrast to the US position where TDM is generally regarded as “fair use” if there is a licence to the underlying work.⁶³)

62. **Permissible TDM under the DSM Directive.** The DSM Directive aims to address the restrictions on copying for TDM by introducing two new exceptions.

Articles 3 and 4 of the DSM Directive permit reproduction of copyrighted works and extraction of information from databases where the user performing TDM has “lawful access” to the protected work.

Lawful access is described as “access to content based on an open access policy or through contractual arrangements between rightsholders and research organisations or cultural heritage institutions, such as subscriptions, or through other lawful means”⁶⁴.

63. **Article 3’s research exception.** Article 3 expressly permits “reproductions and extractions made by research organisations and cultural heritage institutions in order to carry out, for the purposes of scientific research, text and data mining of works or other subject matter to which they have lawful access”.

“Research organisations and cultural heritage institutions” are defined as: universities, research institutions or any other entities, the primary goal of which is to conduct scientific research or to carry out educational activities involving also the conduct of scientific research on a not-for-profit basis or by reinvesting all the profits in its scientific research; or pursuant to a public interest mission recognised by a Member State.

⁶² Directive (EU) 2019/790 of the European Parliament and of the Council Of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directive 96/9 and 2001/29 – <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0790&from=EN>.

⁶³ See, e.g., *Authors Guild v. HathiTrust*, 755 F.3d 87 (2d Cir. 2014), *White v. West* (S.D.N.Y. 2014), *Fox v. TVEyes* (S.D.N.Y. 2014), *Authors Guild v. Google*, 770 F.Supp.2d 666 (S.D.N.Y. 2011), *Kelly v. Arriba-Soft*, 336 F.3d 811 (9th Cir. 2003), *A.V. v. iParadigms, LLC* (4th Cir. 2009), *Perfect 10 v. Amazon*, 508 F.3d 1146 (9th Cir. 2007), and *Field v. Google*, 412 F.Supp.2d 1106 (D. Nv. 2006).

⁶⁴ Per recital 14 of the DSM Directive.



64. **Article 4 and the ‘express reservation’ of TDM rights in an ‘appropriate manner’.** Article 4 permits reproductions of, and extractions from, “lawfully accessible works” for TDM for any purpose provided that this activity has not been “expressly reserved by rightsholders in an appropriate manner”.

Little guidance is given in the DSM Directive on what amounts to an “appropriate” “express” reservation of TDM rights, aside from the following:

- where works are made publicly available online, the DSM Directive stipulates that it will only be “considered appropriate to reserve those rights by the use of machine-readable means, including metadata and terms and conditions of a website or a service”; and
- in other arrangements, the reservation can be included as a contractual term or a unilateral declaration by the rightsholders.

In light of the above, and the fact that the DSM Directive will need to be implemented in each member state for it to be effective, it’s not clear at this stage whether the generally accepted shorthand approach of stating “all rights reserved” or “all rights not expressly granted are reserved by the copyright/database right holder” will be sufficient to prohibit TDM or whether more explicit wording specifically restricting TDM is required to amount to an “express” reservation in “an appropriate manner”.

65. **Emerging best practice.** To address this uncertainty, we expect that, as a matter of best practice and to avoid any issues of interpretation, where rightsholders wish to restrict TDM, they will introduce wording: (a) expressly prohibiting TDM, (b) incorporating an acknowledgement from the user that the prohibition on TDM is made/given in an “appropriate manner”, and (c) that permits the rightsholders to check that the prohibition has been complied with. It’s therefore key for users to check the terms of licences or notices accompanying protected works to establish if TDM is permitted.

While superficially the TDM exceptions in the DSM Directive appear to grant new exceptions to copyright and database right infringement, in our view, it’s likely to have little impact on users’ rights on a day-to-day basis, simply because rightsholders will be able to circumvent the exception by specifically and expressly prohibiting it.

For the position in the UK post-Brexit transition, please see section J below

H. COPYRIGHT: HYPERLINKS AND THE COMMUNICATION TO THE PUBLIC RIGHT

66. **The InfoSoc Directive and hyperlinking.** Article 3 of the EU’s Information Society Directive⁶⁵ (**‘InfoSoc Directive’**) grants to rightsholders the exclusive right to authorize or prohibit any communication to the public of their works. This right and the scope of Article 3 has been the subject of a large number of cases, not all of which are reconcilable.⁶⁶ A full overview and analysis of all Article 3 case law is outside the scope of this section; our intention instead is to focus exclusively on the relationship between Article 3 of the InfoSoc Directive and the dissemination of protected works via hyperlinks.

⁶⁵ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society – <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0029&from=EN>.

⁶⁶ See, e.g., “Communication to the public” under EU copyright law: an increasingly Delphic concept or intentional fragmentation? E.I.P.R. 2016, 38(12), 715-717; and ‘Communication to the public or accessory liability? Is the CJEU using communication to the public to harmonise accessory liability across the EU?’ E.I.P.R. 2018, 40(5), 289-294.



67. **Background.** The structure and use of the Internet has made it significantly easier to share content in different forms (including protected works) among large groups of people. Any Internet user can share a simple hyperlink to a video or article and, if that link goes viral, thousands of people will have viewed the shared content, often without consultation with or approval of the content owner. The inherent open and permissible functionality in the Internet is often therefore at odds with those aspects of copyright law that control exploitation of protected works. This tension has resulted in the CJEU considering whether the making available/sharing of a hyperlink amounts to copyright infringement under Article 3 of the InfoSoc Directive on the basis that making the hyperlink available cuts across the rightsholder’s ability to control communication of the relevant works to the public.⁶⁷

68. **Infringing hyperlinks.** At first glance, it’s difficult to envisage scenarios where sharing a hyperlink gives rise to copyright infringement⁶⁸ – hyperlinks are essentially functional in nature and simply make it easier to navigate through the Internet in a more direct and efficient way by directing the user specifically to the content they require without the need to visit other areas of the website first (or in some cases, the link avoids the need to log-in or subscribe).⁶⁹ It’s this functional aspect of hyperlinks that clashes with the rightsholder’s ability to control the communication of its works to the public – Internet users who share hyperlinks are also “communicating” content.

There are 2 elements to the infringement: (1) a communication and (2) that communication is made to a “public”.

It’s permissible to share content already made freely available by the rightsholder via hyperlink if the “public” to whom the original content was made available does not change or is not “new”,⁷⁰ however, liability for making content available via a hyperlink will arise in the following circumstances:

- the content shared via the hyperlink is made available to a “new” public not within the contemplation of the rightsholder when the original distribution/making available occurred (e.g. content made available to a limited group is communicated outside that group without consent);
- the hyperlink is to paywalled content or content otherwise not generally available/accessible and the hyperlink avoids the need to purchase a subscription to the shared content; or
- the hyperlink is to content illegally published online and the hyperlinker was aware (or ought to have been aware) of that illegality.⁷¹

⁶⁷ There appears to be a distinction in the case law of the CJEU depending on the nature of the allegedly infringing activity: cases that relate to broadcasting and re-transmission appear to be dealt with slightly differently than those relating to hyperlinking. See the articles cited at the footnote immediately above for more details. For the purposes of this section, we are concentrating on hyperlinking only.

⁶⁸ In addition to the fact that sharing a hyperlink may infringe copyright, the text (e.g. headline or title) included in a hyperlink may also infringe the rightsholder’s reproduction right if the text quoted is the author’s own intellectual creation. See, e.g., *Infopaq International v Danske Dagblades Forening* (Case C-5/08) [2012] Bus LR 102 and *Newspaper Licensing Agency Ltd and others v Meltwater Holding BV and others* [2011] EWCA Civ 890.

⁶⁹ At least 1 US court has held that hyperlinking *per se* does not infringe copyright as no copying is involved – the user who clicks on the hyperlink is referred to the “genuine” article. (*Ticketmaster Corp., and others v. Tickets.com, Inc.*, No. CV 99-7654-HLH (BQRx), 2000 WL 1887522 (C.D. Cal. Mar. 27, 2000).

⁷⁰ *Svensson and others v Retriever Sverige AB* (Case C-466/12) [2014] Bus LR 259.

⁷¹ *GS Media BV v Sanoma Media Netherlands BV* (C-160/15) EU:C:2016:644.



69. **Status/intent of the hyperlinker.** In addition to the nature of the content and the audience, a key component of the analysis concerns the status of the hyperlinker: if the hyperlinker making the hyperlinked content available does so for commercial purposes, it is presumed to have knowledge of the infringing content whereas if the “links are provided without the pursuit of financial gain by a person who did not know or could not reasonably have known the illegal nature of the publication”, no infringement will be deemed to have occurred.⁷²

It’s therefore key to establish if the hyperlinker pursues financial gain, although it’s not clear what level of “financial gain” is required to trigger the presumption of infringement – it’s an open question if the threshold requires that direct revenue flows from the act of hyperlinking or simply requires that hyperlinker is a revenue generating business.

If the posting of hyperlinks is for financial gain, then:

“it can be expected that the person who posted such a link carries out the necessary checks to ensure that the work concerned is not illegally published on the website to which those hyperlinks lead, so that it must be presumed that that posting has occurred with the full knowledge of the protected nature of that work and the possible lack of consent to publication on the internet by the copyright holder. In such circumstances, and in so far as that rebuttable presumption is not rebutted, the act of posting a hyperlink to a work which was illegally placed on the internet constitutes a ‘communication to the public’ within the meaning of Article 3(1) of [the InfoSoc Directive].”⁷³

Profit-making businesses who share content via hyperlinks will need to rebut the presumption of infringement by showing that they have carried out checks to ensure that the linked-to content is non-infringing – these checks may resemble the “upload filters” envisaged by the new DSM Directive, reviewing published terms and conditions and reservation of rights statements on the linked-to content, as supplemented by a notice and takedown procedure that allows rightsholders to inform the hyperlinker of the infringing nature of the linked-to content.

70. The DSM Directive – Press Publications and OCSSPs.

- **Press Publications:** Article 15 of the EU’s Digital Single Market DSM Directive⁷⁴ (**‘DSM Directive’**) gives new rights to publishers of press publications when their publications are used by information society service providers: for a period of 2 years from the date of publication, press publishers can license online use of their publications to information service providers. The new right is intended to permit press publishers to recoup investment in the content they make available, which has historically been shared by aggregators and media monitoring services for profit without any payment to the original press publisher. There is no impact on existing defences and exceptions to copyright infringement and the new right does not apply to “acts of hyperlinking” (although what constitutes an act of hyperlinking is not defined).⁷⁵

⁷² *GS Media BV v Sanoma Media Netherlands BV* (C-160/15) EU:C:2016:644.

⁷³ *GS Media*, paragraph 51.

⁷⁴ [European Directive on Copyright in the Digital Single Market](#) (Directive (EU) 2019/790 of the European Parliament and of the Council Of 17 April 2019).

⁷⁵ Article 15, DSM Directive.



- **Content providers & upload filters:** The DSM Directive adds further complexity for a limited group of content providers – online content sharing services providers⁷⁶ (**OCSSPs**) will be liable for the publication of protected works unless the rightsholder has granted has license to the OCSSP to do so. OCSSPs will no longer be able to rely on the safe harbour for hosting providers set out in the E-Commerce Directive in a potentially far reaching change to existing law and established practice: if no licence/authorization is granted by the rightsholder, an OCSSP will be liable unless they can show that (a) they made best efforts to obtain an authorization, and (b) made best efforts to remove infringing content after notification from the rightsholder and (c) acted expeditiously, upon receiving a sufficiently substantiated notice from a rightsholder to disable access to, or to remove from, their websites the protected works, and made best efforts to prevent their future uploads.

71. **Conclusion.** Whereas in earlier years rightsholders concentrated on taking down providers of peer-to-peer networks designed to make protected content illegally available online, other users of protected material are now at risk of copyright infringement simply by hyperlinking to third party content. It's therefore key for any business that shares third party content to assess the potential risk of copyright infringement under the hyperlinking cases and the new DSM Directive and to consider what steps it can take to reduce/remove liability. It's also important that businesses that conduct activities falling within the hyperlinking cases and the DSM Directive continue to monitor ongoing discussion and cases before the CJEU – this is a complex and nuanced area of law that requires detailed analysis and scrutiny to form a view of whether particular activities amount to an illegal communication to the public of a protected work.

I. CLOUD IP: THE PATENT TROLL THREAT

72. **Growth of the cloud.** Digital transformation is propelling business cloud-wards at prodigious rates: research company Gartner⁷⁷ forecasts (pre-COVID-19) that public cloud market will grow 17% in 2020, up from \$228bn in 2019 to \$266bn. At the same time scale economies are extending the cloud's reach out from the data centre, connecting billions of intelligent IoT (Internet of Things) devices at the edge: by 2021, one million new IoT devices will be coming online every hour.⁷⁸
73. **The cloud and NPEs.** The concentration of computing resources into the expanding cloud is becoming increasingly attractive as a target for patent litigation to **NPEs**, non-practising entities that buy patents to sue others for infringement as their only revenue source. At a time when data security and privacy risks are

⁷⁶ The aim is to “target only online services that play an important role on the online content market by competing with other online content services, such as online audio and video streaming services, for the same audiences”, i.e., YouTube, Instagram. Services that have a main purpose other than that of enabling users to upload and share a large amount of copyright-protected content with the purpose of obtaining profit from that activity, such as providers of business-to-business cloud services and cloud services, which allow users to upload content for their own use, such as cyber-lockers, are excluded. Smaller operations are subject to lighter obligations but the criteria are cumulative: “platforms which have less than 3 years of existence in the European Union AND which have a turnover of less than €10 million AND have less than 5 million monthly users”. Exceeding any of these 3 triggers the full regime.

⁷⁷ ‘Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020’, 15 November 2019, <https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020>.

⁷⁸ “In 2021, 1 million new IoT devices will be purchased every hour of every day”, (Gartner Digital Business, October 2015) – <https://www.gartner.com/smarterwithgartner/gartner-predicts-our-digital-future/>.



front of mind for cloud service providers ('CSPs') and their customer, the intellectual property risks to cloud service availability posed by NPE patent claims are attracting increasing attention.

74. **The NPE perspective.** NPEs are well placed to monetise their patents at each stage of the litigation cycle. They have access to capital and all necessary forensic and legal resources; and an NPE doesn't practise its patents so is immune to a defendant's competitive counterclaim or cross-licence offer. Patent stats show consistently increasing NPE activity. Overall, NPE patent litigation increased 4% in 2019 over 2018, accounting for 58% of new cases in the US District Court.⁷⁹ In the cloud sector, NPEs appear to have doubled down over the last five years, acquiring more cloud patents for their armoury as well as filing more patent cases. As the cloud extends out to embrace IoT devices at the edge, early trends in the IoT patent space show a similar picture, with NPEs acquiring more patents and launching more claims year on year.

NPE activities may attract opprobrium as arbitraging the patent system, but that is to miss the point: the defendant in a patent claim brought by a NPE generally has an unattractive real-world choice between the cost and distraction of litigation and the cost of settlement which, whilst low in relation to likely litigation costs, is high relative to the perceived merits of the claim.

From the NPE's standpoint this makes sense. Claiming that software in the CSP's PaaS (Platform as a Service) or IaaS (Infrastructure as a Service) infringes the NPE's patents can be an efficient way to threaten alternative objectives: the CSP risks an injunction stopping it from using the software that embodies the patented technology; and the CSP's customers using that software also face disruption as they may be liable both for their own workloads and for their CSP's infringing code that they use.

75. **The perspective of the CSP and its customers.** From the standpoint of the CSP and its customers all this is bad enough, but software patent risks are further exacerbated by ubiquitous use of OSS, which now generally powers the cloud. OSS developments are created by communities of individual developers. With no single holder of software rights, patent infringement issues are unlikely to be top of mind; and if they are, developers will generally lack the resources to help them navigate the risks. Compare this with a corporate developer of proprietary software who holds all the rights to its technology and has both the incentive to address patent infringement risks and the legal and technical resources to do so. The rub is that, simply because they are open, OSS developments and communities are easier targets for NPEs than proprietary software as they don't need to go to the same lengths to discover potential infringement. The softness of the target increases risk for CSPs using OSS and their users.

76. **Muted regulatory response to cloud IP issues.** Cloud software patent risk is evident and growing, so it is perhaps surprising that the regulatory response has been muted, especially when data protection, privacy and information security figure so large. Yet an unsettled cloud software patent claim runs risks to cloud service availability that are arguably of the same order as information security risks. In cloud guidance, regulators like the UK's Financial Conduct Authority ('FCA') and the European Banking Authority ('EBA') do not expressly address IP risks but implicitly consider them in terms of business continuity, customer duties and reputational risk. So, the FCA says that firms should:

"identify and manage any risks introduced by their [cloud] arrangements. Accordingly firms should carry out a risk assessment to identify relevant risks and identify steps to mitigate them, document this

⁷⁹ '2019 Patent Dispute Report', 1 January 2020, Unified Patents – <https://www.unifiedpatents.com/insights/2019/12/30/q4-2019-patent-dispute-report>.



assessment, identify current industry good practice ... assess the overall operational risks, monitor concentration risk and consider what action it would take if the provider failed”⁸⁰

The EBA states that institutions outsourcing to the cloud should:

“should ... take into account all of the following: (a) ... activities that are critical to the business continuity/viability of the institution and its obligations to customers, (b) the direct operational impact of outages, and related legal and reputational risks, (c) the impact any disruption of the activity might have on their revenue prospects ...”⁸¹

IP risks are not called out expressly, but this is clear guidance that firms must identify, assess and plan for all relevant risks including service availability failure, which could of course crystallise due to IP risks.

77. **Contractual protection to counter the NPE threat.** CSPs have been quick to respond to growing cloud IP risks as a means of competitive differentiation and offering innovation protections to their cloud customers. For example, Microsoft took an early lead in designing measures to counter NPE cloud patent litigation with its Azure IP Advantage program. Launched in February 2017,⁸² the program provides without further charge to eligible customers for their applications on Microsoft’s Azure platform (i) uncapped indemnification coverage against IP infringement claims, (ii) patent pick giving access to 10,000 patents to choose from and use in defence of a claim and (iii) a springing licence, sprung for the customer if Microsoft transfers patents to an NPE.⁸³ In October 2017, the program was extended to China⁸⁴ and in October 2018 Microsoft joined the LOT (License On Transfer) Network⁸⁵ to increase the strength of the springing licence component for the broader LOT community. To help customers meet the developing NPE IoT patent threat at the cloud’s edge and in a first for the cloud/IoT industry, Microsoft announced on 28 March 2019 a further expansion by offering cloud to edge, end to end coverage to address patent risk. The program will extend the protections available through Azure IP Advantage to Azure Sphere and Windows 10 IoT for eligible customers.⁸⁶

⁸⁰ See ‘FG 16/5 – Guidance for firms outsourcing to the ‘cloud’ and other third-party IT Services’, pages 6 and 7, FCA, July 2016 – <https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf>. Emphasis added.

⁸¹ ‘Recommendations on outsourcing to cloud service providers’, Final Report, EBA, 20 December 2017, paragraph 4.1, page 12 – [https://eba.europa.eu/sites/default/documents/files/documents/10180/2170121/5fa5cdde-3219-4e95-946d-0c0d05494362/Final%20draft%20Recommendations%20on%20Cloud%20Outsourcing%20\(EBA-Rec-2017-03\).pdf](https://eba.europa.eu/sites/default/documents/files/documents/10180/2170121/5fa5cdde-3219-4e95-946d-0c0d05494362/Final%20draft%20Recommendations%20on%20Cloud%20Outsourcing%20(EBA-Rec-2017-03).pdf).

⁸² ‘Protecting Innovation in the cloud’ (Brad Smith, President, Microsoft, 8 February 2017) – <https://blogs.microsoft.com/blog/2017/02/08/protecting-innovation-cloud/#sm.00001bvwb1hrrdm3txe1lqyf04oww>

⁸³ Azure IP Advantage – <https://azure.microsoft.com/en-us/overview/azure-ip-advantage/>.

⁸⁴ ‘Extending Microsoft Azure IP Advantage to China’ (Erich Andersen, Corporate Vice President, Deputy General Counsel, Microsoft, 19 September 2017) – <https://azure.microsoft.com/en-gb/blog/extending-microsoft-azure-ip-advantage-to-china/>.

⁸⁵ ‘Microsoft joins LOT Network, helping protect developers against patent assertions’ (Erich Andersen, Corporate Vice President, Deputy General Counsel, Microsoft, 4 October 2018) – <https://azure.microsoft.com/en-gb/blog/microsoft-joins-lot-network-helping-protect-developers-against-patent-assertions/>.

⁸⁶ ‘Microsoft expands Azure IP Advantage Program with new IP benefits for Azure IoT innovators and startups’ (Erich Andersen, Corporate Vice President, Deputy General Counsel, Microsoft, 28 March 2019) – <https://blogs.microsoft.com/on-the-issues/2019/03/28/microsoft-expands-azure-ip-advantage-program-with-new-ip-benefits-for-azure-iot-innovators-and-startups/>.



J. BREXIT: CODE IP POST-BREXIT TRANSITION

78. **Introduction.** Brexit is pervasive and will impact all aspects of life and society in the UK, including our intellectual property rights. In this section, we look at what we know about Brexit's effects on software and algos and how it may affect rightsholders and users based in the UK and elsewhere in the EU.
79. **The Withdrawal Agreement.** UK law applicable to software and algos is currently an amalgamation of:
- UK legislation,
 - directly effective EU legislation,
 - UK legislation implementing non directly effective EU law,
 - UK legislation implementing international treaty obligations,
 - the common law, and
 - judge-made case law from courts and tribunals (including the UK courts, the CJEU and various patent and trade-mark tribunals).
80. **Sources of EU copyright-related laws.** From a copyright perspective, EU derived laws have their origins in the following 11 directives and 2 regulations:
- Directive on the harmonisation of certain aspects of copyright and related rights in the information society (**'InfoSoc Directive'**), 22 May 2001,
 - Directive on rental right and lending right and on certain rights related to copyright in the field of intellectual property (**'Rental and Lending Directive'**), 12 December 2006,
 - Directive on the resale right for the benefit of the author of an original work of art (**'Resale Right Directive'**), 27 September 2001,
 - Directive on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission (**'Satellite and Cable Directive'**), 27 September 1993,
 - Directive on the legal protection of computer programs (**'Software Directive'**), 23 April 1992,
 - Directive on the enforcement of intellectual property right (**'IPRED'**), 29 April 2004,
 - Directive on the legal protection of databases (**'Database Directive'**), 11 March 1996,
 - Directive on the term of protection of copyright and certain related rights amending the previous 2006 Directive (**'Term Directive'**), 27 September 2011,
 - Directive on certain permitted uses of orphan works (**'Orphan Works Directive'**), 25 October 2012,
 - Directive on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market (**'CRM Directive'**), 26 February 2014,
 - Directive on certain permitted uses of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print-disabled (**'Directive implementing the Marrakech Treaty in the EU'**), 13 September 2017,
 - Regulation on the cross-border exchange between the Union and third countries of accessible format copies of certain works and other subject matter protected by copyright and related rights for the



benefit of persons who are blind, visually impaired or otherwise print-disabled (**‘Regulation implementing the Marrakech Treaty in the EU’**), 13 September 2017,

- Regulation on cross-border portability of online content services in the internal market (**‘Portability Regulation’**), 14 June 2017, and
- Three additional instruments (**Directive 87/54/EC**, **Council Decision 94/824/EC** and **Council Decision 96/644/EC**) which harmonise the legal protection of topographies of semiconductor products.

In addition, the **E-commerce Directive** and the **Conditional Access Directive** also contain provisions which are relevant to the exercise and the enforcement of copyright.

81. **Implementation into UK law.** Many aspects of these directives have been tested in the European Union courts over the years and harmonization has predominantly occurred piecemeal as a result of the judicial interpretation of these directives by the CJEU rather than by virtue of the text of the directives themselves.

These directives have, to a greater or lesser extent, been implemented into UK law and the decisions of the CJEU on the interpretation of these directives are currently binding on the UK.

Nothing changes until 31 December 2020. Under the terms of the Withdrawal Agreement, the UK intellectual property rights system continues as normal to the end of this year: afterwards, however, there are a number of points to be aware of when considering the status of existing or new IP rights: (a) what happens to existing law/existing rights, (b) what happens to rights created on and from 1 January 2021 and (c) how the UK government proposes to address new EU law.

82. **‘Retained EU Law’.** At a high-level, the general position with respect to EU law in the UK post-Brexit is as follows. For present purposes, we’ve simplified this by concentrating on those aspects most relevant to IP rights rather than describe all nuances related to the Withdrawal Agreement terms.

The starting point on 1 January 2021 is that existing EU law is incorporated into UK law: the European Union (Withdrawal Agreement) Act 2020 (and amendments it made to the European Union (Withdrawal) Act 2018), operates to convert the body of EU law (directives, decisions, case law, general principles of EU law) in effect at the end of the transition period into UK law (**‘retained EU law’**).

Then, from 1 January 2021 onwards and unless otherwise agreed as part of any new trade relationship: (1) the UK courts will no longer be subject to new decisions of the CJEU (except in a limited number of areas related to the Withdrawal Agreement), (2) the UK Supreme Court may, from that point onwards, choose to depart from retained EU law provided that any decision to do so is decided on the same basis as if the Supreme Court is deciding the same question in relation to its own case law, and (3) the UK government has the right to set out in regulations the circumstances in which retained EU law will no longer apply in the UK.

At the time of writing (21 April 2020), there’s no indication that the UK government will make changes to retained EU law applicable to IP rights, however it remains to be seen if UK law will continue to follow the same path or whether the UK will start to diverge from EU law.

83. **IP rights created on or after 1 January 2021.** On 1 January 2021 and in the absence of any trade deal, new rules will apply to certain copyrights, the *sui generis* database right, and the principle of exhaustion. There are also changes to how the other directives and regulations listed above will work post-Brexit – these are



outside the scope of this specific section, however advice and guidance is available from the UK's Intellectual Property Office⁸⁷.

- **copyright:** generally speaking, the rules applicable to most copyrighted works will remain the same because the rights originate in international copyright treaties such as the Berne Convention and TRIPS. It's unlikely therefore that core copyright law will change in the UK and EU and UK works will continue to be eligible for copyright protection in the other jurisdiction(s) on the basis of the reciprocity rules set out in the Berne Convention.
- **sui generis database right** (introduced by the Database Directive): for new databases created after 1 January 2021, UK citizens, residents and businesses will not be eligible to receive or hold database rights in the European Economic Area ('EEA') and only UK citizens, residents and businesses will be eligible for database rights in the UK. This means that existing rightsholders may need to acquire licensees or take steps to protect databases contractually. Database copyright is unaffected by these changes.
- **online content sharing services** will no longer be obligated to provide content ordinarily available in the UK to UK individuals located temporarily in another EU country. Similarly, EU based individuals may be restricted from viewing local EU content when in the UK.
- **exhaustion of rights:** exhaustion of rights is a key aspect of parallel trade rules in the EU. It means that where a product that is protected by IP rights has been placed on the market in any EU member state with the permission of the rightsholder, the rightsholder's rights to restrict resale or distribution in another territory are "exhausted" and local IP rights owned by the rightsholder in the second country cannot be used to prevent that resale or distribution. In a post-Brexit world, products placed on the UK market that are then parallel imported into the EU may no longer be considered exhausted in the EU and permission to do so may be required from the rightsholder (the position is not the same for items placed on the market in the EEA and then imported into the UK - per The Intellectual Property (Exhaustion of Rights) (EU Exit) Regulations 2019, products placed on the market in the EEA will be considered exhausted for the purposes of resale into the UK). This could have significant consequences for businesses and supply chains and businesses should review and assess the likely impact of this change on their supply and distribution models.

84. **New EU legislation.** The UK government has already stated that it does not currently plan to replicate the terms of the recently approved Directive on Copyright in the Digital Single Market into UK law (see section G above). This Directive introduces controversial rules on "upload filters" and new rules on text and data mining. The UK government in January 2020 stated that:

"the Government has no plans to [implement the Directive into UK law]. Any future changes to the UK copyright framework will be considered as part of the usual domestic policy process"⁸⁸.

Given the broad discretion and scope for different interpretations of various aspects of the Directive and the fact that most businesses who operate internationally are obliged to comply with the Directive's terms in any event, it's currently difficult to assess the impact of the UK government's approach on business and industry.

⁸⁷ See <https://www.gov.uk/guidance/changes-to-copyright-law-after-the-transition-period> for more information.

⁸⁸ <https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2020-01-16/4371>.



K. CONCLUSION

85. **Conclusion.** This white paper has built on a collection of blogs exploring the IP treatment of AI algorithms and data and focusing on recent cases (*Google v Oracle*, *SAP v Diageo*), legislative developments in IP law (text and data mining, the communication to the public right and Brexit) and IP treatment of particular IT sectors including of AI (ownership of AI algorithms and data), open source (the Affero GPL) and the cloud (the patent troll threat). We're conscious in a breakfast webinar that we can only scratch the surface, but hope that this paper provides further insight and tools to explore these perennially interesting areas. Please do get in touch if you have any comments or questions.

Kemp IT Law, Solicitors
Draft date: 23 April 2020
Ref: RHK/DAM/CTHK

KEMP IT LAW

IT Law at the Apex



Richard Kemp
Partner

T: 020 3011 1670
M: 07932 695 615
richard.kemp@kempitlaw.com



Deirdre Moynihan
Partner

T: 020 3011 1627
M: 07710 395 460
deirdre.moynihan@kempitlaw.com



Chris Kemp
Associate

T: 020 3011 1678
M: 07710 396 071
chris.kemp@kempitlaw.com