18

Software, Data and the Cloud

SUMMARY CONTENTS

Software and data licensing are tied to a significant amount of global commerce. While many aspects of the licensing agreements in these industries are similar to those in other industries, there are a number of unique features that characterize licenses of software and data.

18.1 DATA AND DATABASES

Analysts estimate that the global market for data will grow from $139 billion in 2020 to $229 billion by 2025.[1] Data fuels financial markets, consumer sales, advertising, healthcare, political campaigning, natural resources extraction and thousands of other industries, small and large. Yet surprisingly little is known or written about the licensing of data and database products.[2] This section offers an introduction to this increasingly important field.

18.1.1 *Protecting the Unprotectable*

Despite the expansive reach of US copyright law, no copyright exists in facts, information or data. This principle was established by the Supreme Court more than a century ago in the seminal case *International News Service v. Associated Press*, 248 U.S. 215 (1918), in which the Court held that the news of the day, independent of its expression in a particular news story, is not subject to copyright. The Court reaffirmed this principle three decades ago in *Feist Publications v. Rural Telephone*, 499 U.S. 340 (1991), explaining "That there can be no valid copyright in facts is universally understood. The most fundamental axiom of copyright law is that no author may copyright his ideas or the facts he narrates." In *Feist*, the compiler of a telephone directory

[1] Markets and Markets, Big Data Market by Component, Deployment Mode, Organization Size, Business Function (Operations, Finance, and Marketing and Sales), Industry Vertical (BFSI, Manufacturing, and Healthcare and Life Sciences), and Region – Global Forecast to 2025, www.marketsandmarkets.com/Market-Reports/big-data-market-1068.html.

[2] The term database has several meanings. First, a database is a type of computer program that can store and provide access to large quantities of data. In another sense, a database is the collection of data elements contained in a software database program. For the purposes of this chapter, we will use the latter meaning.

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

argued that copyright should be recognized in its compilation of names and telephone numbers – the product of significant labor and effort. Nevertheless, the Court flatly rejected this "sweat of the brow" theory of protection. It notes that "The same is true of all facts – scientific, historical, biographical, and news of the day. They may not be copyrighted and are part of the public domain available to every person." Under the principles set forth in *Feist*, the compiler of a collection of data may obtain a "thin" copyright in any creative arrangement and selection of entries in a database, but no copyright in the data elements themselves, singly or in the aggregate.

The situation is different in Europe. In 1996, the EU adopted Directive 96/9 on the Legal Protection of Databases (the EU Database Directive), granting fifteen years of legal protection to any collection of data, information or other material that is arranged in a systematic or methodological way, provided that it is accessible by electronic or other means and its producer has made a "substantial investment" in its compilation. Around the same time, a significant debate occurred in the United States regarding the advisability of enacting similar database protection legislation. Despite the introduction of several different proposals in Congress, no such legislation was enacted, leaving databases without formal legal protection in the United States.[3] More recently, the EU enacted the General Data Protection Regulation (GDPR), a sweeping set of legislation intended to protect individual data, which is discussed in greater detail in Section 18.1.4.

This being said, there are numerous legal tools at the disposal of a US database owner to prevent the unauthorized use of data that it has compiled. For example, Section 1201 of the Digital Millennium Copyright Act of 1998 (DMCA) prohibits the circumvention of technological devices that are intended to control access to copyrighted works. In other words, hacking the protections that a database owner implements to protect its data could be a violation of the DMCA, even if the use of the protected data is not a copyright infringement.[4] Claims for unauthorized use of data are also available under theories of trade secret misappropriation, unfair competition and trespass (sometimes referred to as "cybertrespass").[5]

In addition, there are ongoing efforts to "propertize" data in the United States, thus overcoming the precedent established in *INS v. AP* and other cases, as discussed in the following article relating to individual health information.

THE FALSE PROMISE OF HEALTH DATA OWNERSHIP
JORGE L. CONTRERAS, 94 *N.Y.U. L. REV.* 624, 626–33 (2019)

Debates regarding data ownership and privacy have been brewing in academic circles since the emergence of computers and digital records in the 1960s, but it was the growth of the Internet in the late 1990s and early 2000s that sparked widespread debate among cyberlaw and intellectual property scholars. In recent years, increasing wealth inequality and the rise of digital platforms have fueled a renewed conversation about the ownership of personal information.

[3] J. H. Reichman & Paul F. Uhlir, A *Contractually Reconstructed Research Commons for Scientific Data in a Highly Protectionist Intellectual Property Environment*, 66 L. & Contemp. Probs. 315, 374–76, 388–95 (2003).

[4] See Raymond T. Nimmer, *Issues in Modern Licensing of Factual Information and Databases* in Research Handbook on Intellectual Property Licensing 99, 112–15 (Jacques de Werra, ed., Edward Elgar, 2013).

[5] See id. at 105–12, 115–16.

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

Joining this debate, some health law scholars have raised concerns regarding individual autonomy, privacy and distributive justice in arguing for the propertization of genetic and other health information. In his bestselling book *The Patient Will See You Now*, cardiologist and patient advocate Eric Topol asserts that "[t]he ownership of property is essential to emancipation. It's unquestionably appropriate, a self-evident truth, that each individual is entitled to own all of his or her medical data." Popular awareness of these issues has been fueled, among other things, by the story of Henrietta Lacks, an indigent African-American cancer patient whose excised tumor cells formed the basis of a multi-billion industry while her descendants continued to live in poverty. At least six U.S. states have enacted legislation purporting to grant individuals ownership of their genetic information (though one has since repealed that legislation). And even former President Barack Obama once opined that "if somebody does a test on me or my genes … that's mine."

But the push toward individual data ownership has gained the most momentum thanks to a new crop of technology-focused startups. In a global health data market worth an estimated $67 to $100 billion per year, these aspiring data intermediaries seek to use Blockchain and mobile apps to enable consumers to control, and get paid for, the use of their Individual Health Information (IHI), and in the process retain a healthy portion of the proceeds. These firms include Nebula Genomics (co-founded by Harvard Medical School professor and genomics pioneer George Church), Genos (a spinout from Chinese sequencing giant BGI-Shenzhen), DNASimple (a recent contestant on the ABC television show Shark Tank), Invitae (seeking to sell "genome management" services) and LunaDNA (backed by equipment manufacturer Illumina). The motivations of these firms may be summed up by the Chairman of Genos, who has publicly stated that "our business is to make money enabling researchers and individuals to connect and transact with each other."

In a less commercial vein, Unpatient.org, a short-lived not-for-profit effort by Topol and Leonard Kish, sought to empower patients through data ownership. Unpatient.org released its own "Data Ownership Manifesto" which proclaimed that "[d]ata that reflects you should belong to you," rather than to healthcare providers and pharmaceutical companies.

But perhaps the most intriguing addition to the propertization camp is Hu-manity.org, which approaches the issue of data propertization from the perspective of international human rights, arguing that a "31st human right" in personal data ownership should be recognized under the Universal Declaration of Human Rights, following from which individuals should be able to sell, and profit from, access to their data.

In each of these business models, the aspiring data intermediary acts as the consumer's authorized agent in selling or licensing her IHI to healthcare providers, pharmaceutical manufacturers, and anyone else interested in it, remitting a share of the revenue back to the consumer and, of course, retaining a portion for itself. While the idea that consumers, as a matter of equity and distributive fairness, should share in the profits earned from the use of their data is not a new one, it is only today, with the advent of technologies such as Blockchain and pervasive mobile connectivity, that markets in IHI have become feasible.

Though there are differences among these proposed offerings, an individual who signed up with one of these data intermediaries would be given the ability to opt-in to one or more research studies and contribute all or a portion of her stored data to the study. In some cases, an individual may not wish to share certain types of information, such as a family

history of schizophrenia or an HIV-positive diagnosis. In that case, the intermediary could screen the studies offered to the individual or exclude IHI relating to the sensitive subject area. DNAsimple advertises that it will pay donors for saliva samples to help genetic disease research. Genos estimates that IHI payments to consumers would be in the range of $50 to $250; while LunaDNA offers participants a mere $3.50 for the use of their genetic marker data and $21 for a full genomic sequence.

The linchpin of this new business model is the recognition of an individual's ownership of IHI. Without it, companies, hospitals, insurers, and data intermediaries can (and today do) aggregate and sell individual health information without consulting, or paying, the individual. But if consumers owned their data, anyone who tried to use or sell it without permission would be stealing (or at least converting) that data. Ownership of IHI would potentially invest individuals with powerful and legally enforceable mechanisms to prevent intrusion, appropriation, and exploitation of information that they do not wish to share—authority that seems particularly desirable in today's world of untrammeled data exploitation.

Recognizing a property right in IHI, of course, would represent a significant departure from current U.S. law, which has held for more than a century that data—objective information and facts—cannot be owned as property. As Justice Louis Brandeis wrote, facts are "free as the air to common use." This longstanding rule has been applied consistently to information ranging from the news of the day, stock recommendations, and sports scores to the sequence of naturally occurring human DNA. The federal court in *Greenberg v. Miami Children's Hospital Research Institute, Inc*. expressly rejected property-based claims under which the plaintiffs sought a share of the profits made using discoveries based on their children's genetic data. Thus, under current law, facts—raw information about the world—once generally known, cannot be owned.

Numerous scholars have argued against the creation of a new form of personal property covering individual data. Their objections range from moral and dignitary concerns over commodification of the individual, to utilitarian concerns about barriers that individual ownership of health information could impose on biomedical research and its potential impact on patient safety and public health, to a sense that the propertization of IHI is unnecessary in view of existing common law and regulatory protections of individual privacy and safety.

But, as noted above, the current movement toward ownership of IHI is driven, to an increasing degree, by concerns over privacy, autonomy, and distributive justice. These core ethical considerations are difficult to balance against a "communitarian" instrumental analysis. Thus, even if granting individuals ownership over IHI is likely to impede scientific research and public health monitoring, this cost may be acceptable to those who value personal privacy and autonomy above aggregate net benefits to society.

Notes and Questions

1. *No protection for data*. Why doesn't US law recognize copyright in data? Should the United States move toward a database protection regime similar to that in the EU?
2. *Health data*. What do advocates for recognizing property interests in personal health data hope to gain? Do you think, as the author suggests, that "granting individuals ownership over IHI is likely to impede scientific research and public health monitoring"? Is this cost worth the benefit of such ownership?

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

18.1.2 *Licensing Data*

If a data licensing agreement will cover the EU, then the licensor may rely on the *sui generis* protection afforded by the EU Database Directive as a licensable intellectual property (IP) right. To do so, the definition of IP in the agreement should include "data and database rights" or language to the same effect. This small modification allows data to be licensed on terms similar to those used for patents and copyrights.

In the United States, database licensors have largely compensated for this lack of *per se* legal protection by relying on a combination of trade secret law, restrictive contractual terms and technological access and control mechanisms. These are discussed in greater detail below.

18.1.2.1 Trade Secrets

Trade secret protection for databases is a tricky subject. At one extreme, a database may contain information that is entirely proprietary to the database creator, such as a company's internal sales and production figures, or the results of an internal safety testing program. In these instances, assuming that the information in the database otherwise meets the statutory requirements for trade secret protection, the data within the database can be considered to be protected by trade secret law. At the other extreme, a database may contain public information that is readily accessible to others, such as stock prices or sports scores. In these cases, trade secret protection is probably not available for the data (though, as we will see below, such databases can be protected quite effectively through contractual terms of use).

In the middle lies a gray area. A database may contain information that is technically public, but the collection and combination of which is not straightforward. As explained by the Ninth Circuit in the context of the Economic Espionage Act, 18 U.S.C. § 1839(3),

> A trade secret may consist of a compilation of data, public sources or a combination of proprietary and public sources. It is well recognized that it is the secrecy of the claimed trade secret as a whole that is determinative. The fact that some or all of the components of the trade secret are well-known does not preclude protection for a secret combination, compilation, or integration of the individual elements. The theoretical possibility of reconstructing the secret from published materials containing scattered references to portions of the information or of extracting it from public materials unlikely to come to the attention of the appropriator will not preclude relief against the wrongful conduct. Expressed differently, a compilation that affords a competitive advantage and is not readily ascertainable falls within the definition of a trade secret.[6]

Thus, many data and database licensing agreements refer to trade secrets as the IP being licensed, though doing so may involve some risk that portions of the license grant may be invalidated if the data is no longer viewed as having trade secret status.[7]

18.1.2.2 Data Licensing as a Contractual Matter

When there is no trade secret or other underlying IP right to support a license of data under US law (e.g., a database of stock prices or sports scores), licensing agreements often elide the

[6] *United States v. Nosal*, 844 F.3d 1024, 1042 (9th Cir. 2016).

[7] See the famous "Listerine" case, *Warner-Lambert Pharm. Co. v. John J. Reynolds, Inc.*, discussed in Section 12.2 (holding that the loss of trade secret status did not override the parties' intent that royalties be paid in perpetuity).

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

question of what rights, specifically, are being "licensed." Rather, they often state that the data in question is being licensed without reference to a particular set of IP rights.

EXAMPLE: DATABASE LICENSE

a. Licensor hereby grants Licensee a worldwide, nonexclusive license during the term of this Agreement to incorporate the Database into the Licensee Product in the manner described in Appendix A, and to license the Licensee Product to users (directly or indirectly through one or more sublicensees) for the users' internal purposes only and for a period as long as the Agreement is in effect.
b. The Parties agree and acknowledge that any use of the Database not expressly authorized by the foregoing clause (a) is strictly prohibited. Without limiting the generality of the foregoing, Licensee and the users are expressly prohibited from (i) sublicensing or reselling the Database or any data elements included therein on a standalone basis separate from the Licensee Products; (ii) using or allowing third parties to use the Database for the purpose of compiling, enhancing, verifying, supplementing, adding to or deleting from any mailing list, geographic or trade directories, business directories, classified directories, classified advertising, or other compilation of information which is sold, rented, published, furnished or in any manner provided to a third party; (iii) using the Database in any service or product not specifically authorized in this Agreement or offering it through any third party other than the sublicensees; or (iv) disassembling, decompiling, reverse engineering, modifying or otherwise altering the Database, other than as required to provide the products and services permitted under this Agreement, or any part thereof without Licensor's prior written consent, which consent may be withheld in Licensor's sole discretion.

The absence of an underlying IP right results in several challenges for the data licensor. First, it means that if the licensee violates the licensing agreement, the licensor cannot bring an infringement suit. Rather, it is left with only its contractual remedies. Second, because the licensor lacks contractual privity with third parties who obtain and use the data that the licensee impermissibly disclosed or disseminated, it cannot bring contractual claims against them. And without an IP claim, the licensor has little recourse against such third parties.

The lack of an underlying IP right also makes it particularly important for the licensor to construct a contractual framework that emulates the existence of an IP right, as shown in clause (b) of the above example. This text makes it clear that the "license" granted in clause (a) is the only use that the licensee is permitted to make of the licensed data, even if there is no underlying IP right that would prevent other uses. It is also beneficial, in these cases, to specify the types of uses that are *not* permitted, as shown above.

It has been said that "data is the new oil," and data has, for decades, fueled the oil and gas industry itself. Vast quantities of geophysical data are generated in the search for new fossil fuel reservoirs, and the petroleum exploration and production (E&P) industry was one of the pioneers of the use of "big data" in its operations. The following case involves a license of E&P data that went awry.

M.D. Mark, Inc. v. Kerr-McGee Corp.

565 F.3d 753 (10th Cir. 2009)

BRISCOE, CIRCUIT JUDGE

Plaintiff M.D. Mark, Inc. (Mark) filed this action alleging that defendants Kerr-McGee Corporation (Kerr-McGee) and Oryx Energy Company breached the terms of seismic data license agreements and also misappropriated seismic data owned by Mark. Mark prevailed on its claims at trial and was awarded $25,266,381 in compensatory damages. Kerr-McGee now appeals, attacking each aspect of the jury's liability findings, as well as the amount of the damage award. [W]e affirm the district court's judgment in all respects.

I

PGI, Mark and the Seismic Data

In the 1970's and 1980's, a Texas-based company called Professional Geophysics, Inc. (PGI) developed, at substantial expense, a collection of geophysical information called seismic data. PGI in turn licensed that data, for a fee, to members of the oil and gas industry for exploration purposes. In 1991, PGI declared bankruptcy and Mark, a Texas-based company, purchased PGI's database for $1.4 million, or approximately $53 per mile for approximately 26,000 miles of data. Mark then began, and continues to this day, to license that data.

Sun/Oryx

In the early 1980's, the Sun Exploration & Production Company (Sun), a Delaware corporation headquartered in Houston, Texas, entered into a series of license agreements with PGI covering approximately 16,000 miles of seismic data. In December 1985, Sun created a subsidiary called Sun Operating Limited Partnership (SOLP) and transferred to it a group of assets, including the seismic data licensed from PGI. In doing so, however, Sun apparently did not transfer to SOLP any of the underlying license agreements. In May 1989, Sun changed its name to Oryx Energy Company (Oryx).

Kerr-McGee

Between 1984 and 1994, Kerr-McGee, an Oklahoma-based corporation, entered into a series of license agreements in its own name with PGI and Mark covering approximately 775 miles of seismic data. Kerr-McGee itself, however, did not engage in any oil or gas exploration. Instead, all such exploration was conducted by its subsidiaries, including Kerr-McGee Oil and Gas Corporation (KMOG).

Merger Between Kerr-McGee and Oryx and Subsequent Changes

On October 14, 1998, Kerr-McGee and Oryx entered into a written agreement pursuant to which Oryx would merge into Kerr-McGee. That merger was approved by the companies' shareholders on February 26, 1999.

Communications Between Oryx/Kerr-McGee and Mark re Merger

On October 16, 1998, Mark, aware of the pending merger between Kerr-McGee and Oryx, sent a letter to Oryx reminding it that Oryx had licensed "certain PGI … seismic data" and

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

that "[t]hose licenses [we]re not transferable, as stated in the agreements." The letter went on to state:

> However, M.D. Mark will allow the data to be transferred and licensed to Kerr-McGee upon the payment of a transfer fee and the execution of a current M.D. Mark license agreement. This offer to transfer the data is valid for thirty (30) days from the date of this letter. If, however, Kerr-McGee does not wish to transfer the data, then M.D. Mark is requesting the immediate return of its data within thirty (30) days.

Oryx apparently responded to the letter by telephoning Mark and asking additional questions about the proposed transfer fee.

On November 11, 1998, Marilyn Davies, the president of Mark, sent another letter to Oryx stating, in pertinent part:

> As we discussed, M.D. Mark would authorize Kerr McGee to have access to this seismic data for about $200 per mile if all of the data was retained. The fee would go higher if Kerr McGee chose to retain only certain data sets instead of the entire volume …
>
> Since the actual consummation of the [merger] deal won't take place until 1st Quarter 1999, M.D. Mark will extend its offer to transfer the data until thirty (30) days after the merger/consolidation/control change date.

No further response was received from Oryx until February 11, 1999, when Patricia Horsfall, Oryx's manager of exploration, sent a letter … to Mark stating, in pertinent part:

> Contingent upon approval of the merger by the companies' shareholders, your records will need to be changed to reflect the name change of the Licensee, under the referenced Seismic Data License Agreement(s), from Oryx Energy Company to Kerr-McGee Oil & Gas Corporation, a subsidiary of Kerr-McGee, located in Houston.

On February 17, 1999, Davies sent a letter to Horsfall stating that "the PGI seismic [data] is not transferable, assignable, etc. and cannot be made available to Kerr-McGee without prior written approval from M.D. Mark and the payment of an authorization or transfer fee." Davies' letter further stated that, in the absence of such authorization or transfer fee, "the licenses of all PGI seismic data in Oryx's possession w[ould] be automatically terminated" upon the closing of the merger, and all "data must be returned."

On March 26, 1999, Salazar, Kerr-McGee's in-house counsel, sent a letter to Mark stating:

> Please be advised that Kerr-McGee Corporation will not pay a transfer fee for any data subject to a license from PGI to Oryx Energy Company or any of its predecessors. We are in the process of packaging all data identified on our records as being subject to any such license and will be shipping it to you as soon as packaging is complete.

On March 31, 1999, Davies acknowledged Salazar's March 26, 1999 letter and requested that all data be "returned to [Mark's] storage facilities" in Houston, Texas. Davies' letter outlined all of the types of material that needed to be returned to Mark, and stated, in conclusion, "that any and all licenses to PGI seismic data re [*sic*] now terminated."

On August 16, 2000, Davies sent a letter to Salazar stating that "[t]he option of returning the data ha[d] been withdrawn," and enclosed an invoice in the amount of $3,000,000 "reflecting the charges based on the discount given to a volume license purchase." On

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

August 29, 2000, Salazar sent a letter to Davies stating that it "remain[ed] [Kerr-McGee's] intention to retain the data … and to not pay a transfer fee."

This Lawsuit

On February 16, 2001, Mark filed suit against Kerr-McGee and Oryx in Colorado state court asserting claims for misappropriation of trade secrets, breach of contract, tortious interference with contract, and unjust enrichment. On March 7, 2001, Kerr-McGee removed the action to federal district court in Colorado, premised on diversity jurisdiction.

During discovery, it was determined that Kerr-McGee was in possession of 3,175 miles of Mark's seismic data that was not covered by any of the existing license agreements between PGI or Mark and Kerr-McGee, Sun, or Oryx. This discovery gave rise to an additional claim of misappropriation by Mark against Kerr-McGee.

The case proceeded to trial on September 17, 2007. During trial, the parties and the district court focused on three categories of seismic data underlying Mark's claims 2:

Category 1 Data – this category encompassed approximately 15,745 miles of seismic data licensed by Sun/Oryx from PGI/Mark prior to Oryx's merger into Kerr-McGee;

Category 2 Data – this category encompassed the 775 miles of seismic data licensed directly by Kerr-McGee from PGI/Mark prior to the merger; and

Category 3 Data – this category encompassed approximately 3,175 miles of seismic data found during discovery to be in Kerr-McGee's possession but not covered by any pre-existing license agreements (this is sometimes referred to as the "bootleg data").

At the conclusion of all the evidence, the jury found that:

> Oryx breached one or more of the license agreements it entered into with PGI/Mark, covering Category 1 data, by "transferr[ing] the license agreement[s] to Kerr McGee Corp, without prior approval," and that Mark suffered $15,745,000 in damages as a result of the breach;
>
> Kerr-McGee breached one or more of its own pre-merger license agreements with PGI/Mark, covering Category 2 data, by "transfer[ring] license[s] to Kerr McGee Oil & Gas [Corporation]" without "prior consent," by failing to return all data to Mark, and by failing to safeguard Mark's trade secrets, and that Mark suffered $968,750 in damages as result of this conduct; and
>
> Kerr-McGee "gained access to and possessed PGI data [i.e., Category 3 data] through improper means" beginning in at least 1996, Kerr-McGee also, after the merger with Oryx, wrongfully transferred control of the Category 1 data to a Kerr-McGee subsidiary, id., and that Mark suffered $25,266,381 in damages as a result of Kerr-McGee's misconduct regarding the Category 1 and Category 3 data.

On September 28, 2007, the district court entered judgment in favor of Mark and against Kerr-McGee in the amount of $25,266,381.

[The parties appealed].

II

1. Challenges to the Jury's Liability Findings Regarding Category 1 Data

Kerr-McGee … attacks the jury's findings that Oryx and Kerr-McGee misappropriated Category 1 seismic data. More specifically, Kerr-McGee contends that there was no

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

evidence of any "wrongful transfer" of the Category 1 data from Oryx or Kerr-McGee to a Kerr-McGee subsidiary, as was necessary to a finding of misappropriation under the district court's instructions.

It is true that Kerr-McGee presented evidence in its defense suggesting that the Category 1 data was not transferred to KMOG, and instead "was left in the former Oryx subsidiary SOLP … " However … the evidence presented at trial … suggested that the employees of Kerr-McGee and its subsidiaries generally paid little heed to corporate formalities, instead viewed Kerr-McGee and its subsidiaries as a "family," and readily shared seismic data without regard to any limitations imposed by the underlying license agreements. In light of this evidence, we cannot say that the jury's misappropriation findings were "clearly, decidedly, or overwhelmingly against the weight of the evidence."

2. Challenges to the Jury's Liability Findings Regarding Category **2** Data

The jury found, with regard to the Category 2 data, that Kerr-McGee breached one or more of its own pre-merger license agreements with PGI/Mark by "transfer[ring] license[s] [covering Category 2 data] to Kerr McGee Oil & Gas," i.e., KMOG, without "prior consent," by failing to return all data to Mark, and by failing to safeguard Mark's trade secrets.

As previously noted, Mark presented, during its case-in-chief, the testimony of Kerr-McGee's in-house attorney Carlos Salazar. Salazar testified, in pertinent part, that Kerr-McGee itself did not engage in any oil and gas exploration. Instead, Salazar testified, such exploration was handled by Kerr-McGee's subsidiaries. Further, Salazar testified that he and other Kerr-McGee employees "considered [Kerr-McGee] to be a family of companies," and "didn't … see anything wrong with affiliates and subsidiaries exchanging [seismic data] information." … Marilyn Young, a Kerr-McGee-employed attorney who oversaw Kerr-McGee's family of subsidiaries, testified … that "Kerr-McGee wanted all [of] its oil and gas exploration and development and production to go through" KMOG, and that, in 2002, the subsidiaries were reorganized in a fashion such that KMOG oversaw Onshore LP.

In addition to this testimony, the jury was presented with a copy of the 1994 Agreement between Kerr-McGee and Mark. That agreement required Kerr-McGee, absent "written permission" from Mark, to "maintain the Data on its premises at all times" and prohibited Kerr-McGee from "provid[ing] copies [of the data] to third parties for removal from [Kerr-McGee]'s premises for any purpose." Notably, the agreement provided that these requirements "appl[ied] even in the event of a corporate reorganization … or a merger," and that "no disclosure" could "be made to any parties involved in such actions, even if such parties [we]re the surviving entities after such corporate reorganization … or merger." Lastly, the agreement provided that in the event of a breach by Kerr-McGee, Mark could terminate the agreement and require the return of "all physical evidence of the Data including any reprocessing of the Data."

In light of this evidence, we are unable to conclude that the jury's findings regarding the Category 2 data were "clearly, decidedly, or overwhelmingly against the weight of the evidence." Thus, in turn, we conclude that the district court did not abuse its discretion in denying Kerr-McGee's motion for new trial as to the Category 2 data issues.

3. Challenges to the Jury's Liability Findings Regarding Category **3** Data

The jury found that Kerr-McGee gained access to and possessed through improper means the Category 3 data.

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

Turning now to the evidence presented at trial, it is true, as asserted by Kerr-McGee, that Mark did not produce any direct evidence that Kerr-McGee acquired the Category 3 data by means of theft, bribery, misrepresentation, or breach or inducement of a breach of a duty to maintain secrecy or not to disclose a trade secret. Importantly, however, Mark's evidence established that:

> Mark regularly maintained records of the data sets it licensed to third parties, and those records showed no license or delivery of the Category 3 data to Kerr-McGee, Oryx/Sun or any Kerr-McGee subsidiary;
>
> [A]lthough Kerr-McGee was in possession of the Category 3 data, it could not produce a single employee, former or present, who could explain how Kerr-McGee obtained the data, when the data was obtained, or how or when it may have been utilized by Kerr-McGee or any of its subsidiaries;
>
> Kerr-McGee could produce no license agreements or other records validating its possession of the Category 3 data; and
>
> [T]he Category 3 data films possessed by Kerr-McGee were of arguably poor quality, thereby allowing the jury to reasonably infer they were not originals provided directly by Mark to Kerr-McGee.

In our view, this circumstantial evidence was more than sufficient to have allowed the jury to reasonably infer that Kerr-McGee utilized one of the improper means listed in the district court's instructions to obtain access to the Category 3 data. Thus, we conclude the district court did not abuse its discretion in denying Kerr-McGee's Rule 59 motion for new trial with respect to the jury's findings regarding the Category 3 data.

The judgment of the district court is AFFIRMED.

Notes and Questions

1. *Intercompany sharing. M.D. Mark* relates in large part to a licensee's sharing of licensed data among a group of affiliated companies. Both the jury and the court found that such sharing violated the terms of the relevant data licensing agreements. Why do you think that such data sharing among affiliated companies was prohibited? What harm did M.D. Mark suffer from Kerr-McGee's internal sharing of the data? Do you think that M.D. Mark was reasonable in its request for a transfer fee for the licensed data?
2. *Good lawyering*. What would you have done to avoid, or reduce, liability if you had represented Kerr-McGee before and during the events described in this case, at least with respect to the Category 1 and 2 data?
3. *Bootleg data*. How do you think Kerr-McGee came into possession of the Category 3 data? Do you think the jury's inferences were fair, given the lack of direct evidence of misappropriation?
4. *Return of data*. What does it mean to "return" data that can be copied an infinite number of times?

18.1.3 *Noncircumvention and Noncompetition in Data Licensing*

In some cases, parties licensing data may seek additional contractual protections to prevent the misuse of their licensed data. The following case describes one such contractual mechanism.

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

Eden Hannon & Co. v. Sumitomo Trust & Banking Co.

914 F.2d 556 (4th Cir. 1990)

RUSSELL, CIRCUIT JUDGE

Eden Hannon & Co. ("EHC") is an investment company located in Alexandria, Virginia, and Sumitomo Trust & Banking Co. is a New York subsidiary of a Japanese bank. This appeal involves the competition between EHC and Sumitomo to purchase an investment portfolio from Xerox Corporation. In the past, EHC has produced extensive economic models for the purpose of valuing Xerox lease portfolios, bidding on these portfolios, and selling the income rights to the portfolios to institutional investors. In the late summer of 1988, Sumitomo indicated interest in purchasing a portfolio through EHC. To that end, Sumitomo signed a "Nondisclosure and Noncircumvention" agreement with EHC, in order to protect the confidential information that EHC later shared with Sumitomo. In violation of that agreement, and after taking possession of EHC's confidential analyses, Sumitomo bid on the December 1988 Xerox portfolio, won the bid, and made a direct purchase of the portfolio. EHC had bid also on that portfolio, and its bid was ranked third by Xerox officials.

EHC subsequently filed this suit, stating four counts: misappropriation of trade secrets, breach of contract, breach of fiduciary duty, and breach of the duty of good faith and fair dealing. Sumitomo denied these allegations. [The district court] found that Sumitomo's actions constituted a breach of contract, and found that a misappropriation of trade secrets had not been proven. As a remedy, the district judge enjoined Sumitomo from repeating its violation of the Nondisclosure and Noncircumvention Agreement. Both parties have appealed the rulings adverse to their positions, and we affirm in part, reverse in part, and remand.

I

The "portfolio" that Xerox sells is composed of the right to receive the stream of income from a group of copiers leased by Xerox, and to receive the residual value of the copiers when the leases expire or are terminated. This is known as the Xerox Partnership Asset Strategy ("PAS") Program. Four times a year, Xerox invites a limited number of investors to bid for a portfolio, which typically contains several hundred copiers leased by Xerox to various customers for terms usually ranging from one to three years. EHC has been a regular bidder and frequent winner in the past, winning ten quarterly bids in the first three-and-a-half years of the program. The bids submitted to Xerox are not just dollar figures; instead, a bid consists of several components, and each component addresses how an element of the projected revenue stream would be divided between Xerox and the successful bidder.

EHC does not bid with its own money in these sales. Instead, it arranges in advance for a bank or insurance company to provide the monetary investment, and in return that investor receives all of the revenue generated by the leases.

Given that EHC's value is in its knowledge, it must guard that knowledge jealously. On the other hand, it must also disclose a great amount of its confidential analysis regarding a proposed bid on a portfolio in order to convince an institution to bid from $25 million to more than $60 million on a single portfolio. To that end, EHC requires any interested investor to sign a "Nondisclosure and Noncircumvention Agreement" (an "Agreement")

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

before it can receive any of EHC's confidential information. This Agreement requires that the investor not disclose the information it receives from EHC to other parties. Most importantly, it also requires that the potential investor "not independently pursue lease transactions" with Xerox's PAS Program "for a period equal to the term of the Purchase Agreement." Since the copiers are usually leased for one to three years, we presume that this term would prevent an investor from independently pursuing a portfolio for approximately three years.

Sumitomo was a potential investor interested in the PAS portfolio. Immediately after EHC won the June 1988 portfolio bid, a Sumitomo officer, Ragheed Shanti, based in the United States, telephoned EHC to express interest. In order to evaluate the PAS program, Shanti attempted to obtain EHC's economic data on their winning June bid. EHC insisted that it could not disclose that information without an Agreement signed by a Sumitomo representative. Shanti tried to avoid signing an Agreement, and then attempted to water down the provision that would require Sumitomo not to "independently pursue" portfolio purchases … EHC refused this substitution, and Shanti eventually signed the original Agreement on the part of Sumitomo. During these negotiations over the language of the Agreement, Sumitomo admitted to EHC that it was also considering financing a portfolio bid by a competitor of EHC, DPF Leasing Services, Inc. ("DPF"). EHC indicated that the Agreement would not prevent Sumitomo from financing a competitor's bid. However, EHC did not want to create a new competitor that would use EHC's information to bid directly against it. Thus, the understanding between EHC and Sumitomo was that Sumitomo could finance a competitor's bid, but it could not directly bid (i.e., "independently pursue") on a portfolio during the "term of the Purchase Agreement."

Once the Agreement was signed, EHC disclosed a great amount of confidential bidding information to Sumitomo. However, Sumitomo and EHC could not reach a deal on a bid for the next portfolio to be offered in December, 1988.

This did not prevent Sumitomo from participating in the bidding for the December portfolio, however. In fact, Sumitomo bid directly on the portfolio, in clear violation of the Agreement with EHC. In submitting its bid, Sumitomo worked through Gerry Sherman, who was a former employee of DPF, a competitor of EHC. Sherman had formed his own one-man company, Oasis, which would work on bids for Xerox PAS portfolios. Sherman had experience from his days at DPF in the economic modelling and bidding process for such portfolios. Sumitomo argues that Oasis won the December bid by carrying out the same functions as EHC would have carried out.

This is not true. To us, and to the district court, it is clear that Oasis was merely a stalking horse for Sumitomo, and that Sumitomo was the direct bidder for the December portfolio. Unfortunately, it is unclear whether Sherman also provided the financial advice to Sumitomo that enabled it to make its bid. Sherman did work on the Xerox PAS Program when he was employed by EHC's competitor, DPF. Sumitomo has claimed that it gained all of its knowledge on how to value and bid for a Xerox portfolio from Sherman. While Sumitomo admits that it had possession of the confidential materials it got from EHC, it claims that it did not use these materials at all. It states that after negotiations fell through with EHC on August 25, 1988, Shanti put these materials in a box and never looked at them again. In a close call, the district judge found that Sumitomo had not misappropriated EHC's trade secrets, and thus, the district judge must have found Sumitomo's story more credible on this point.

FIGURE 18.1 In the 1980s, Xerox sold investment portfolios comprising revenue streams from hundreds of leased photocopier machines.

Since our disposition of this case does not depend on knowing whether Sumitomo actually used this information, we will not dwell on the point. However, we have our doubts about the correctness of this finding.

II

The Supreme Court of Virginia has decided several cases involving agreements not to compete in the employment law arena, and those cases are substantially similar to the case at bar. In many employment contracts, there is language stating that upon termination of the employment relationship, the employee is restricted from competing with the employer within a certain amount of time and within a certain geographical area (for the purposes of this opinion, these are called "employment agreements"). The Virginia courts have held repeatedly that employment agreements are enforceable if they pass a three-part reasonableness test:

(1) Is the restraint, from the standpoint of the employer, reasonable in the sense that it is no greater than is necessary to protect the employer in some legitimate business interest?
(2) From the standpoint of the employee, is the restraint reasonable in the sense that it is not unduly harsh and oppressive in curtailing his legitimate efforts to earn a livelihood?
(3) Is the restraint reasonable from the standpoint of sound public policy?

Paramount Termite Control Co. v. Rector, 380 S.E.2d 922, 924 (Va. 1989). The agreements that pass this test may be enforced in equity.

The Noncircumvention and Nondisclosure Agreement … is nearly identical in purpose to an employment agreement. Most importantly, an employment agreement enables an employer to expose his employees to the firm's trade secrets. Similarly, a noncircumvention agreement enables potential joint venturers to share confidential information regarding a possible deal. In both instances, the idea is to share trade secrets so that business can be conducted without losing control over the secrets. Often, the value of a firm is its special knowledge, and this knowledge may not be an idea protectible by patent or copyright. If

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

that firm cannot protect that knowledge from immediate dissemination to competitors, it may not be able to reap the benefits from the time and money invested in building that knowledge. If firms are not permitted to construct a reasonable legal mechanism to protect that knowledge, then the incentive to engage in the building of such knowledge will be greatly reduced. Free riders will capture this information at little or no cost and produce a product cheaper than the firm which created the knowledge, because it will not have to carry the costs of creating that knowledge in its pricing. Faced with this free rider problem, this information may not be created, and thus everybody loses. To counteract that problem, an employer can demand that employees sign an employment agreement as a condition of their contract, and thus protect the confidential information. This means that if an employer takes in an employee and exposes that employee to trade secrets, the employer does not have to allow the employee to go across the street and set up shop once that employee has mastered the information. Although it was not explained in this detail, Virginia has recognized this interest in protecting confidential information.

These employment agreements (or in the present case, a noncircumvention agreement) are often necessary because it can be very difficult to prove the theft of a trade secret by a former employee. Often, the purpose of an employment agreement can be to prevent the dissemination of trade secrets, yet a mere ban on using trade secrets after the termination of employment would be difficult to enforce. Judge Lord explained the problem well in *Greenberg v. Croydon Plastics Co.*, 378 F.Supp. 806, 814 (E.D.Pa.1974):

> Plaintiffs in trade secret cases, who must prove by a fair preponderance of the evidence disclosure to third parties and use of the trade secret by the third parties, are confronted with an extraordinarily difficult task. Misappropriation and misuse can rarely be proved by convincing direct evidence. In most cases plaintiffs must construct a web of perhaps ambiguous circumstantial evidence from which the trier of fact may draw inferences which convince him that it is more probable than not that what the plaintiffs allege happened did in fact take place. Against this often delicate construct of circumstantial evidence there frequently must be balanced defendants' witnesses who directly deny everything.

Actually, Judge Lord's description of the problem covers just the tip of the iceberg. There are several problems with trying to prevent former employees from illegally using the former employer's trade secrets, and these problems are caused by the status of the law regarding the misappropriation of trade secrets. First, as Judge Lord depicted so well, it is difficult to prove that the trade secret was actually used. Second, the former employee tends to get "one free bite" at the trade secret. Most courts will refuse to enjoin the disclosure or use of a trade secret until its illegal use is imminent or until it has already occurred. By that time, much of the damage may be done. Third, even if a clearly illegal use of the trade secret by a former employee can be shown, most courts will not enjoin that person from working for the competition on that basis. Instead, they will merely enjoin future disclosure of the trade secret. Yet, policing the former employee's compliance with that injunction will be difficult. Finally, even if the employee does not maliciously attempt to use his former employer's trade secrets in the new employer's workplace, avoiding this use can be difficult. It would be difficult for the employee to guard the trade secret of the former employer and be effective for the new employer.

In order to avoid these problems, many employers ask their employees to sign noncompetition agreements. These agreements prevent an employee from working with the competition within a limited geographical range of the former employer and for a limited

time. As seen above, Virginia courts will only enforce these agreements if they are reasonable. Yet, when they are valid, they make the guarding of a trade secret easier since they remove the opportunity for the former employee to pass on the trade secret to the competition, either malevolently or benevolently. This does not supplant the need for law protecting trade secrets. Non-competition agreements cannot prevent disclosure anywhere in the world and until the end of time, for they would be held unreasonable. Instead, a non-competition agreement will merely prevent the illegal use of a trade secret next door in the near future, where the use might do the most damage.

EHC's position regarding potential investors was the same as an employer–employee relationship in regard to the use of trade secrets. The thing that made EHC valuable was its expertise in valuing lease portfolios. EHC would "sell" its knowledge of the value of a particular PAS portfolio to investors for a percentage of the profit. It was necessary for EHC to share its confidential economic models and projections on the particular bid in order to attract investors. Yet, if it gave this information to an investor without restriction, that investor would merely make the bid directly and cut EHC out of the deal, after EHC's investment in expertise and research made the bid possible.

EHC could have merely prohibited its potential customers from using its information if that customer became a rival bidder. Indeed, this was the essence of Shanti's counterproposal regarding the language of the agreement, which was rejected by EHC. Such an arrangement would have become an unenforceable honor system. In the present case, Sumitomo has denied that it used the materials it received from EHC, and claimed that it gained its expertise primarily from Gerry Sherman. The trial judge ultimately ruled that there had not been a misappropriation of trade secrets, but his ruling was based on Sumitomo's denials and the citing of Sherman's experience in the area. The trial court did not definitively discover whether Sumitomo actually used these materials, and there was no way that it could have found out. For that reason, EHC chose to include in its agreement with potential investors the noncircumvention clause. Armed with that agreement, EHC could protect its information by merely showing that an investor was competing contrary to the agreement, without having to prove that it was actually using EHC's confidential information.

One reason why [EHC] had a noncircumvention clause was to prevent its disclosures from creating new competitors. The competition for the PAS portfolios was already keen. Xerox invited a limited number of businesses to bid for the portfolios, and there were many other businesses who wanted a chance to bid that were seeking invitations. EHC had a legitimate fear that it would let a new bidder through the door if it educated that investor and gave it contacts to Xerox. Thus a reasonable noncircumvention clause was constructed to place a reasonable limit on competition from a temporary ally.

Thus, EHC's noncircumvention agreement is merely a twist on employment noncompetition agreements that have been recognized by the Virginia courts. That being so, we will briefly discuss the application of Virginia's three-factor test for reasonableness to the case at bar. We have reworked the terms of the test so that it will address noncircumvention agreements.

1. *Is the restraint on circumvention no broader than is necessary, from the standpoint of the trade secret holder, to protect the holder from the disclosure of its confidential information*? Yes. The limitation provided by the noncircumvention clause did not prevent Sumitomo from doing many things. Sumitomo could still invest in a bid won by a

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

competitor of EHC; it could use this information internally in order to put together its own bid for lease portfolios offered by companies other than Xerox; and Sumitomo could bid directly for PAS portfolios in approximately three or four years after the Agreement was signed. This was a narrowly drawn limitation.

2. *From the standpoint of the party that received the confidential information, is the restraint reasonable in the sense that it is not unduly harsh and oppressive in curtailing the legitimate efforts of that party to conduct its business*? Yes. Most importantly, Sumitomo could still invest immediately in any winning bids, including EHC's competitors. Also, Sumitomo could bid directly on any other lease program other than Xerox's, and it could directly invest in Xerox's PAS Program after several years. Furthermore, presumably Sumitomo can make (and has made) money in its other banking activities.
3. *Is the restraint reasonable from the standpoint of sound public policy*? Yes. This factor overlaps the area covered by the first two factors to a great extent. Presumably, public policy seeks to protect the development of trade secrets without ruining competition or driving the receiver of confidential information out of business. As discussed above, this noncircumvention agreement satisfies those concerns. EHC's economic modeling process receives some protection, the bidding for Xerox PAS portfolios remains highly competitive, and Sumitomo will certainly remain a profitable bank.

Notes and Questions

1. *Noncircumvention*. How does noncircumvention differ from nondisclosure (as discussed in Section 5.2)? Why do you think that EHC included both types of restrictions in its agreement? How did Sumitomo allegedly breach the noncircumvention provision of its agreement with EHC? Did Sumitomo also violate the nondisclosure provisions?
2. *Nonuse*. Sumitomo claimed that it did not use the data obtained from EHC, and the district court agreed. Why did the Fourth Circuit find this fact to be irrelevant?
3. *Suspicious behavior*. The Fourth Circuit in *Eden Hannon* seems to make much of the admittedly suspicious behavior exhibited by Sumitomo's employee Ragheed Shanti and its consultant Gerry Sherman. Why does this behavior matter in establishing the breach of contract claims made by EHC?
4. *Employee noncompetition agreements*. The court in *Eden Hannon* bases its analysis of the parties' Noncircumvention and Nondisclosure Agreement on the law of employee noncompetition agreements. How are these two types of agreement similar? Do you think that agreements between sophisticated business parties should be judged by the same standards as agreements between an employer and its employees?
5. *Free riders*. What is the "free rider" problem identified by the court as a justification for restrictive noncompetition and other agreements?
6. *State-level variation*? Note that employee noncompetition agreements are seemingly permitted in Virginia. Yet in some states, such as California, such agreements are far more difficult to enforce. Would a California court have viewed the agreement between EHC and Sumitomo differently as well?
7. *Data versus other types of licenses*. Are noncircumvention/noncompetition agreements more important in data licenses than in other types of licensing agreements like patents or copyrights? Why?

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

18.1.4 *Data Privacy*

As noted in Section 18.1.1, there is a plethora of recent legislation relating to the protection and privacy of individual data.[8] The most prominent recent legislative enactment in this area has been the EU's General Data Protection Regulation (GDPR), which has caused companies around the world to scramble to adjust their data-handling practices and online privacy policies.[9] Data privacy legislation also exists at the US federal level in certain industries, namely healthcare (with the Privacy Rule under the Health Insurance Portability and Accountability Act of 1996 [HIPAA][10]) and consumer financial information (with the Gramm-Leach-Bliley Act[11]).

At the state level, all fifty states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private and governmental entities to notify individuals of breaches of security involving personally identifiable information.[12] In addition, states such as California have also enacted broadly applicable data privacy laws that apply to all entities holding personal data in the state or affecting the state's residents.[13]

Beyond these legislative and regulatory mechanisms, governmental oversight exists to protect individual data and privacy. Since the early days of internet commerce, the US Federal Trade Commission (FTC), which is authorized to police unfair and deceptive business practices, has monitored the collection and use of consumer data by online vendors.[14] In recent years, the FTC has investigated and brought actions for deceptive data claims and practices against prominent companies including Uber, Vizio, BLU and AshleyMadison.com.[15] The FTC has also been active in policing the data security practices of healthcare providers and personal genomics testing companies. In 2014 it filed charges against two companies, Genelink, Inc. and foru International, among other things, for failing to maintain adequate and reasonable data security for their customers' personal information.[16] These claims were settled with the companies agreeing to "establish and maintain comprehensive data security programs and submit to security audits by independent auditors every other year for 20 years."[17] Two years later, the FTC found medical testing company LabMD liable for data security practices "lacking even basic precautions to protect the sensitive consumer information maintained on its computer system."[18]

[8] Individual data refers to data identifying an individual human subject's identity, address, financial, health or other personal information. This being said, vast quantities of data, such as the Xerox lease information and seismological data discussed in the cases in Sections 18.1.2 and 18.1.3, would not be subject to data privacy regulation.

[9] For an overview, see Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 Denver L. Rev. 1 (2020).

[10] 45 C.F.R. Parts 160 & 164 (2003) (hereinafter HIPAA Privacy Rule) (pertaining to the use and handling of protected health information by healthcare providers and related entities).

[11] Requires that financial institutions include privacy notices and limit the sharing of nonpublic personal information (NPI) – "personally identifiable financial information (i) provided by a consumer to a financial institution, (ii) resulting from a transaction or service performed for the consumer, or (iii) otherwise obtained by the financial institution" (15 U.S.C. § 6809(4)).

[12] See Natl. Conf. of State Legislators, Security Breach Notification Laws, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[13] California Consumer Privacy Act of 2018, AB 375 (codified at Cal. Civ. Code Div. 3, Part 4, Title 1.81.5 [commencing with Section 1798.100]).

[14] See Fed. Trade Comm'n, Privacy Online: Fair Information Practices in the Electronic Marketplace (2000); Fed. Trade Comm'n, Privacy & Data Security Update: 2016 at 1 (2017).

[15] See Fed. Trade Comm'n, Privacy and Security Enforcement – Press Releases, www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

[16] Id.

[17] Id.

[18] *In re. LabMD, Inc.*, Docket No. 9357, Opinion of the Commission 1 (F.T.C. 2016).

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

This panoply of regulation – state, federal and international – coupled with monitoring and enforcement by governmental agencies has sweeping consequences for transactions involving data and databases. These include:

- the structuring of internal systems and processes to secure personal data;
- the creation and updating of compliant data privacy policies and notifications;
- the development of mechanisms to obtain and record individual consent to data practices and to take necessary measures to address information by nonconsenting individuals; and
- implementing response and remediation plans to address consumer complaints and data breaches.

But while these measures will undoubtedly require substantial resources, both financial and personnel, they need not lead to an excess of additional contractual verbiage in data licensing agreements. The following example illustrates language that may be used to supplement a data licensee's obligations with respect to data privacy and security regulations.

EXAMPLE: DATA SECURITY AND PRIVACY

a. Licensee shall, at its sole expense, comply with all applicable Laws regarding the storage and handling of personally identifiable information ("PII"), obtaining consent from individuals for the collection, storage and use of PII, and the notification of individuals and relevant governmental agencies in the event of a breach of security pertaining to PII, an unauthorized release, disclosure or exposure of PII or other unauthorized data or information disclosure [**1**].
b. Within 24 hours after discovering or being informed of any breach of Licensee's security measures pertaining to PII, any unauthorized access to or release of PII, or of any other event requiring notification under applicable Law (a "Data Breach"), Licensee shall notify Licensor of the Data Breach using the expedited Notification procedure specified in Section __ [**2**], and shall keep Licensor fully apprised of Licensee's investigation and response to such Data Breach. Licensee shall implement all additional security and privacy measures reasonably requested by Licensor in response to such Data Breach.
c. Licensee shall, at its sole expense [**3**], prepare and disseminate all notifications required by Law to all individuals affected by a Data Breach, as soon as possible, but in no event later than required by Law. Licensee shall consult with Licensor during the preparation of such notifications and shall incorporate Licensor's reasonable suggestions with regard thereto.
d. Licensee shall indemnify and defend Licensor against any losses arising out of claims related to any Data Breach in accordance with the provisions of Section __ [**4**].

DRAFTING NOTES

[1] *Compliance* – strictly speaking, it is not necessary to require specifically that the licensee comply with applicable data privacy and protection laws, as compliance is typically required under the general compliance with law clause found in most agreements (see

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

Section 13.5). However, if the licensing of PII forms an important component of an agreement, then it may be prudent to call out compliance with data privacy and security laws simply to raise awareness of this key issue.

[2] *Expedited notification* – some agreements provide special expedited email or telephonic notice instructions for events requiring immediate action (see Section 13.12).

[3] *Data subject notification* – many state statutes require that written notice of data breaches be provide to all affected individuals, which could number in the millions. As a result, this obligation can be costly, and it is important that responsibility for this cost be allocated between the licensor and licensee.

[4] *Indemnification* – assuming that an agreement contains a general indemnification provision (see Section 10.3), the data breach provision may simply reference the general indemnification provision of the agreement. Alternately, the general indemnification clause may be adjusted to specify that data breaches are subject to its requirements.

Notes and Questions

1. *Data privacy versus value*. Most data privacy regulation seeks to protect personally identifiable information obtained from individuals. How valuable is this information? What are the consequences of its unauthorized disclosure or use? Why is this type of data protected so much more stringently than valuable commercial data such as the seismological geophysical data in *Kerr-McGee* or the Xerox portfolio data in *Eden Hannon*?
2. *Data privacy vs. trade secrecy*. Does an individual have trade secret protection over his or her personally identifiable data? What about when a corporation collects that data and includes it in a customer or patient database? Why would trade secrecy status vary depending on who holds the data?
3. *Data privacy proliferation*. How can enterprises simultaneously manage compliance with data protection, security and breach regulations in all fifty states, the federal government, the EU and elsewhere? Is the protection afforded by this legislation worth the significant burden of compliance?

18.2 PROPRIETARY SOFTWARE LICENSING

The software industry today is almost too large to size accurately. Almost every electronic product – from medical devices to automobiles to kitchen appliances – contains software, and in many cases cannot operate without it. This section provides a brief background concerning the legal protection of computer software, as well as considerations for software licensing. The subject of "open source software" (OSS) licensing, an important phenomenon, is addressed in Section 19.2.

18.2.1 *Source Code and Object Code*

The classic legal model of computer software contemplates two basic forms of code: *source code* – programming language instructions written (usually) by a human author; and *object code* – the machine-readable executable version of a source code program.[19] Under this

[19] Today, there are many variants on the classic model, including pseudocode and interpreted programming languages such as HTML and JavaScript, which do not require compilation to execute.

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

classic model, a source code program is "compiled" by another program, called a compiler, to form the object code version of the program. Object code is what most people are familiar with when they download or install a computer program – it is the file often labeled with the suffix ".exe" or similar designation.

Anyone who has taken an introductory computer class will recognize some of the programming languages in the example below.

EXAMPLE: SOURCE CODE

C[20]

```
Int main(…)
{
…Printf("Hello World");
 …
}
```

HTML[21]

```
== History ={{Main|History of copyright}}[[File:European Output of
Books 500–1800.png|thumb|upright=2|European output of books before the
advent of copyright, 500s to 1700s. Blue shows printed books. [[Log-
lin plot]]; a straight line therefore shows an exponential increase.]]
```

Perl[22]

```
#!/usr/bin/perl -w
# 531-byte qrpff-fast, Keith Winstein and Marc Horowitz <sipb-iap-
dvd@mit.edu>
# MPEG 2 PS VOB file on stdin -> descrambled output on stdout
#  arguments:  title  key  bytes  in  least  to  most-significant
order$_='while(read+STDIN,$_,2048){$a=29;$b=73;$c=142;$t=255;@
t=map{$_%16or$t^=$c^=(
$m=(11,10,116,100,11,122,20,100)[$_/16%8])&110;$t^=(72,@
z=(64,72,$a^=12*($_%16
-2?0:$m&17)),$b^=$_%64?12:0,@z)[$_%8]}(16..271);if((@a=unx"C*",$_)
[20]&48){$h
=5;$_=unxb24,join"",@b=map{xB8,unxb8,chr($_^$a[-$h+84])}@ARGV;s/  …
$/1$&/;$
```

[20] This simple program, known as "Hello, World" was introduced in 1972 by Brian Kernignan, one of the developers of the C programming language.

[21] Hypertext markup language (HTML), now maintained by the Worldwide Web Consortium (see Chapter 20), is used to design web pages. This sample is from the Wikipedia page for the topic "Copyright." The source code for every web page is available through a browser option.

[22] "Perl" refers to a family of computer programming languages that emerged in 1987. This example "script," known as "Qrpff," allows the user to "break" the CSS encryption of a DVD. It was considered when it was written in 2001 by some to violate the Digital Millennium Copyright Act's prohibition on anti-circumvention measures.

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

```
d=unxV,xb25,$_;$e=256|(ord$b[4])≪9|ord$b[3];$d=$d≫8^($f=$t&)$d≫12
^$d≫4^
$d^$d/8))≪17,$e=$e≫8^($t&($g=($q=$e≫14&7^$e)^$q*8^$q≪6))≪9,$_
=$t[$_]^
(($h≫=8)+=$f+(~$g&$t))for@a[128..$#a]}print+x"C*",@a}`;s/x/
pack+/g;eval
```

These examples of source code are very different, just as different human languages differ in grammar, character sets and vocabulary. Yet each has the power to convert human instructions into commands that can be executed by a computer. As Professor Sonia Katyal has observed, "source code is much more than just lines of commands—it comprises the lifeblood of software, embodying both the potential of the creativity that produces the code and the functionality that the code achieves."[23]

Object code, on the other hand, is comprehensible only to the true computer savant. As one such savant has written, "All computer code is human readable. Some forms are simply more convenient to read than others."[24] Object code is also referred to as "binary" or "machine" code, as it is processed and executed directly by a computer.

EXAMPLE: OBJECT CODE[25]

```
10110100
11111111
01011100
10100101
```

18.2.2 *Legal Protection of Software*

Legal rules concerning software began to emerge in the 1970s when software first left government labs and corporate data processing centers and began to enter the mainstream marketplace. Among the most heated debates that occurred during that era concerned the most sensible mode of legal protection for software: patent, copyright, trade secret or something new? Eventually, copyright protection prevailed as the primary mode of protecting software in the United States.[26]

18.2.2.1 Copyright

Given the analogy between software created using written programming languages and other written works of authorship (books, articles, etc.), it was felt that computer software was best

[23] Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 Cornell L. Rev. 1183, 1194 (2020).

[24] David S. Touretzky, *Source vs. Object Code: A False Dichotomy*, July 12, 2000, www.cs.cmu.edu/~dst/DeCSS/object-code.txt.

[25] This code is a binary representation of the Hello World program written in the C programming language.

[26] See National Commission on New Technological Uses of Copyrighted Works (CONTU), *Final Report on the National Commission on New Technological Uses of Copyrighted Works*, July 31, 1978 (reproduced in 3 Computer L.J. 53 [1981]).

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

considered a "literary work" for the purposes of copyright protection.[27] This is the case even though lines of computer code are purely functional in nature, and copyright generally excludes the functional elements of a work.[28] By extension, the executable object code version of a computer program, even though it is incomprehensible to most people, is deemed to constitute a different representation of that same copyrightable work and, thus, is also subject to copyright, though this position was heavily contested at the outset.[29]

Beginning in the 1980s, courts began to distinguish between protectable forms of software expression and unprotectable ideas regarding software architecture and structure.[30] In *Whelan Associates, Inc. v. Jaslow Dental Laboratory, Inc.*, 797 F.2d 1222 (3d Cir. 1986), the court held that a software program's "structure, sequence, and organization" were eligible for copyright protection. And in *Google v. Oracle*, the Supreme Court confirmed that certain functional elements of computer code – particularly so-called application programmer interfaces (APIs) – can be protected by copyright.[31] As suggested by the dispute in *Google v. Oracle*, the lines separating protectable and unprotectable software content remain blurred today.

Finally, the screen displays and other images produced by computer software are protected by copyright, even though these images are not necessarily "fixed" in a tangible medium (i.e., they are intangible projections or manifestations of the illumination of different electronic elements in a computer screen).[32] Moreover, these images often change in a manner enabled by the programmer, but controlled by the user. Nevertheless, the different configurations and motions of an avatar in a video game would generally be owned by the designer of the game. However, there is a limit to this logic, and the text typed by the user of a word processing program or the music composed with a music synthesis program are owned by the user.

One consequence of treating computer software as a copyrightable work is that its reproduction is an exclusive right of the copyright owner. Yet "reproduction" in the copyright sense has two distinct connotations in the context of software: first is making copies of the software for distribution to others, but a second connotation involves the inevitable reproduction of every computer program in the memory of a computer when the program is executed. The Ninth Circuit confirmed that this "transient" copy is, indeed, a copy for the purposes of the Copyright Act in *MAI Systems Corp. v. Peak Computer Inc.*, 991 F.2d 511 (9th Cir. 1993). In *MAI*, the court held that even though a licensee was authorized to reproduce MAI's software as part of its use, a third-party maintenance provider, Peak, was not so authorized. Thus, when Peak performed maintenance services on the licensee's computers, thereby creating a transient copy of MAI's software, Peak was found to infringe.[33]

[27] US Copyright Office, Compendium of U.S. Copyright Office Practices § 721 (2017).

[28] 1 Nimmer on Copyright § 2A.10.

[29] US Copyright Office, supra note 27, § 721.5. See Pamela Samuelson, *CONTU Revisited: The Case against Copyright Protection for Computer Programs in Machine-Readable Form*, 33 Duke L.J. 663 (1984); Arthur R. Miller, *Copyright Protection for Computer Programs, Databases, and Computer-Generated Works: Is Anything New Since CONTU?* 106 Harv. L. Rev. 97 (1993).

[30] 4 Nimmer on Copyright § 13.03[F]; Miller, supra note 29.

[31] *Google LLC v. Oracle Am., Inc.*, 141 S.Ct. 1183 (2021).

[32] Some of the earliest software copyright cases involved the layout of pull-down menus used in business spreadsheets and similar software. See *Lotus Dev. Corp. v. Borland Int'l, Inc.*, 516 U.S. 233 (1996).

[33] Though the *MAI* decision has been roundly criticized (see Aaron Perzanowski, *Fixing RAM Copies*, 104 Nw. U. L. Rev. 1067 [2010]), it appears to remain the law, and software licensees that wish to engage third-party maintenance providers are well-advised to ensure that their licensing agreements permit usage and reproduction of licensed software by contractors working on their behalf.

18.2.2.2 Patents

The eligibility of computer software and algorithms for patent protection has fluctuated over time. It has long been the case that abstract ideas, such as mathematical formulas, are not eligible patent subject matter. In *Gottschalk v. Benson*, 403 U.S. 63 (1972), the Supreme Court rejected a patent claiming "a method for converting binary-coded-decimal … numerals into pure binary numerals" using a general-purpose digital computer. The Court reasoned that the "claim is so abstract and sweeping as to cover both known and unknown uses of the … conversion [method]." As a result, the claims were considered to be abstract ideas that were ineligible for patent protection. Six years later, in *Parker v. Flook*, 437 U.S. 584 (1978), the Supreme Court held that a patent claiming several conventional applications of a novel mathematical formula was similarly drawn to ineligible subject matter.

It was not until 1981, in *Diamond v. Diehr*, 450 U.S. 175 (1981), that the Supreme Court upheld a patent claiming computer software. The claimed method employed the well-known Arrhenius equation to calculate and control the temperature in a process for curing rubber. The Court held that, while the Arrhenius equation itself was not patentable, the claimed method for curing rubber was an industrial process of a type that has historically enjoyed patent protection. The use of the equation and a computer were incidental to the patentable inventive process.

Software patents differ substantially from copyrights covering computer software. Copyright protects the expression of a work – the lines of code written by a programmer, the executable version of that code and the screen displays and images generated by the code. Patents, on the other hand, protect software functionality at a higher level. Actual source code is seldom included in a patent application, and in many cases software patents simply describe, and claim, the functions accomplished by particular programs.[34]

AMAZON'S ONE-CLICK PURCHASING PATENT

U.S. Pat. No. 5,960,411 (September 28, 1999)

1. A method of placing an order for an item comprising:

under control of a client system, displaying information identifying the item; and
in response to only a single action being performed, sending a request to order the item along with an identifier of a purchaser of the item to a server system;
under control of a single-action ordering component of the server system, receiving the request;
retrieving additional information previously stored for the purchaser identified by the identifier in the received request; and
generating an order to purchase the requested item for the purchaser identified by the identifier in the received request using the retrieved additional information; and
fulfilling the generated order to complete purchase of the item whereby the item is ordered without using a shopping cart ordering model.

[34] Mark A. Lemley, *Software Patents and the Return of Functional Claiming*, 2013 Wisc. L. Rev. 905 (2013).

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

The vagueness, potential overbreadth and poor quality of many software patents led to significant criticism of software patenting in the 2000s. Notorious examples of questionable software patents emerged, including Amazon's "one-click shopping" patent, British Telecom's patent that allegedly covered "the Internet" and Apple's patents covering basic smartphone gestures such as "tap to zoom." Compounding these issues, the 2000s also saw the rise of significant patent litigation initiated by so-called patent assertion entities (colloquially known as "patent trolls") that took advantage of broad and vague patent claim language to seek monetary settlements from firms across the electronics and computing industry. The system came under heavy fire from the popular media, scholars and even the Obama Administration.

Perhaps in response to some of these issues, the Supreme Court again turned its attention to algorithmic patents in 2010. In *Bilski v. Kappos*, 561 U.S. 593 (2010), the Court held that an algorithm for calculating a fixed price for monthly utility bills was an unpatentable abstract idea. Then, in *Alice Corp. v. CLS Bank*, 573 U.S. 208 (2014), the Court rejected patent claims drawn to a computer-implemented electronic escrow service for facilitating financial transactions, holding that the invention was merely an abstract idea. The Court also observed that claiming a generic computer implementation of such an abstract idea cannot transform it into a patent-eligible invention. *Alice* overturned much existing wisdom and practice regarding software patenting and appears to be responsible, at least initially, for a sharp increase in the number of software patent applications that have been rejected on eligibility grounds, and patents that have been invalidated, either at the Patent Trial and Appeals Board (PTAB) or in the courts.[35]

18.2.2.3 Trade Secrets

Computer software may be treated as a trade secret, even when copyright and patent protection are also available. The principal source of software trade secrecy is its source code – the human-readable instructions that are generally invisible and inaccessible to a user of an executable (object code) program (see Section 18.3.3.3).[36]

Yet trade secrecy is also sought with respect to the object code versions of programs. Take, for example, software developed by an enterprise and used internally for key strategic purposes, such as economic forecasting, oil and gas exploration or programmed securities trading. The enterprise could be seriously injured if a competitor obtained an executable version of such a program, or even its readouts and displays.

The issue becomes murkier, however, when dealing with computer software that has been publicly distributed.[37] Despite the inconsistency that seems to arise when treating something distributed to the public as a secret, a combination of contractual confidentiality requirements and the inherent difficulty of extracting intelligible source code from executable object code has resulted in a general recognition of trade secret protection for the internal mechanics of publicly distributed executable software programs.[38]

[35] Jasper L. Tran, *Two Years after Alice v. CLS Bank*, 98 J. Pat. & Trademark Off. Soc'y 354 (2016). Colleen Chien & Jiun Ying Wu, *Decoding Patentable Subject Matter*, 2018 Patently-O Patent L.J. 1 (2018). For an overview of software patenting issues, see Gregory J. Kirsch & Charley F. Brown, *Software Patents* in Bioinformatics, Medical Informatics and the Law 80 (Jorge L. Contreras et al., eds., 2022).

[36] Needless to say, open source code software, in which source code is made freely available to the public, is not subject to trade secret protection (see Section 19.2).

[37] Jay Dratler, Jr., *Trade Secret Law: An Impediment to Trade in Computer Software*, 1 Santa Clara Computer & High-Tech. L.J. 27, 45–47 (1985).

[38] 1 Milgrim on Trade Secrets § 1.09[5][b].

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

18.2.3 *Software Licensing*

As noted above, computer software can be, and often is, covered by a range of IP rights including copyright, trade secret and patent. As discussed in Section 6.1.4, software licenses are generally *product* licenses rather than *rights* licenses. That is, a blanket license is granted under all IP covering a particular software program, rather than enumerating the specific IP rights being licensed. Below are some other special provisions that are encountered in software licensing agreements.[39]

18.2.3.1 Software Use Licenses

Object Code. Most software licenses authorize the licensee to use the licensed software in executable, object code form. Whether the licensed software is an enterprise inventory management system, a consumer photo-editing app or an algorithm embedded in a pacemaker, the user only requires an executable version of the software, and the licensor is only willing to share object code with the user. Generally, these licenses do not permit the licensee to modify the software or to distribute it to third parties (other than its own affiliates).

User Limits. Such licenses sometimes include limits on the number of individual users that may access or use the software. These limits may be stated in terms of a maximum number of registered users, or in terms of the number of concurrent "seats" that may use the software at any given time. Thus, an app intended for individual use may be authorized for use on a single smartphone or other device. An enterprise software system may be limited to use by fifteen individual user IDs in the licensee's finance department. And a university mathematical simulation program may be limited to use by no more than fifty concurrent users at any given time. Often, technical measures enforce these limitations, and avoidance or circumvention of such measures can constitute both a breach of the licensing agreement as well as a violation of the Digital Millennium Copyright Act. And, as the Federal Circuit held in *Bitmanagement Software GmbH v. United States*, 989 F.3d 938 (Fed. Cir. 2021), failing to track and exceeding seat limitations for a licensed software system may constitute a breach of a license condition giving rise to a claim for copyright infringement in addition to breach of contract.

Internal Use Only. Many software use licenses are limited to the licensee's "internal business purposes." This limitation ensures that the licensee cannot use the software for "service bureau" purposes – permitting others to access and use the software remotely. When software contains "internal use" restrictions, the licensee should ensure that its external consultants, contractors, collaborators and business partners are also entitled to access and use the software to the extent necessary to support the licensee's business or to perform services for the licensee.

18.2.3.2 Software Distribution Agreements

One common form of software licensing agreement authorizes the licensee to distribute the licensed software to others, rather than use the licensed software for its own internal purposes. These agreements have various labels, including "original equipment manufacturer" (OEM), "value-added reseller" (VAR) and distribution agreements.

[39] In addition to the materials covered in this chapter, see also Section 10.1.3 covering "performance" warranties for software products.

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

OEMs. OEM agreements typically authorize the licensee to incorporate the licensed software into another software program or a hardware device. For example, the vendor of an electronic French grammar checker might license this program to Microsoft for incorporation into Microsoft Word, or the developer of road-mapping software might license it to Toyota for incorporation into its vehicles. Often, the licensee (OEM) sells the combined product under its own name, and the licensor is recognized only briefly (e.g., on a "splash" screen when its software is launched, or in the product user manual).

VARs. VAR and distribution agreements, on the other hand, typically limit the licensee to distributing or reselling the software as a standalone product or combined with other software in a manner that does not require substantial integration (e.g., reselling a video game as part of a video game "ten pack"). Some of these licensees may provide value-added services, such as software installation, support and training, along with the licensed software. In these cases, the licensor's software is usually identified by name (requiring a trademark license if the licensee will advertise or promote it).

APIs. Incorporation of one program into another sometimes requires the licensee to access and modify the source code of the licensed software (see below). However, this is usually not required, as software often includes object code "application programmer interfaces" or APIs that enable the integration of software programs without the need to access or modify source code. It is important to recall, however, that APIs themselves may constitute copyrightable code, which was the subject of the dispute in *Oracle v. Google* (Oracle alleged that Google infringed the copyright in Oracle's APIs for the Java programming language by incorporating them into the Android operating system without Oracle's permission).

18.2.3.3 Proprietary Source Code Licenses

Unlike the developers of OSS (see Section 19.2), the licensors of proprietary software seldom make the source code of their programs available to licensees. As discussed above, most typical uses of software – whether for internal use or incorporation into other products – require only object code. In some cases, however, a licensee may require access to the source code of licensed software. Some situations in which this might occur include the following:

- The licensed software will be incorporated into a proprietary program or device in a manner that requires detailed knowledge of licensee's larger systems, which knowledge the licensor lacks.
- The licensee requires modifications or customizations to the licensed software to reflect its own proprietary algorithms, formulas or processes.
- The licensee wishes the flexibility to modify the licensed software as it desires, without relying on the licensor.
- The licensee plans to use the software in a mission-critical application and wishes to verify independently that it contains no bugs, defects or vulnerabilities, and that it operates in a manner that will not compromise other licensee systems.
- The licensor is a small company with a limited track record, and the licensee does not have confidence that the licensor will be available indefinitely to make required modifications, updates and upgrades to the software.

In these and other cases, the licensor may grant the licensee access to the source code of a proprietary software program, together with rights to reproduce, modify and create derivative

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

works of the source code and then to use or distribute modified versions of the object code program that is derived from that source code. Unless the software is OSS, it is highly unlikely that the licensee will be granted the right to distribute or disclose the source code itself, or modifications of that source code.

EXAMPLE: SOURCE CODE LICENSE GRANTS

Licensor hereby grants to Licensee, and Licensee accepts, a nonexclusive, nontransferable right and license:

a. to modify, reproduce and prepare Derivative Works of the Source Code, and to incorporate those Derivative Works into Licensee Programs to produce Modified Licensee Programs;
b. to reproduce and distribute Modified Licensee Programs in Object Code form to Licensee's end user customers in the Territory pursuant to End User Sublicense Agreements meeting the requirements of Section __ below.

Licenses of proprietary source code require the parties consider several issues that do not arise in the context of typical software licenses or OSS licenses.

Confidentiality. A software proprietor's source code is often a valuable trade secret. Thus, source code releases are often governed by strict confidentiality restrictions – sometimes more strict than even the ordinary confidentiality terms applied to information exchanged under an agreement. For example, the number and identity of individuals to whom source code may be released is often specified, there are requirements regarding heightened security measures that must be applied to the storage and transmission of source code (e.g., encryption, password-protected directories). Likewise, the duration of confidentiality provisions relating to source code are often indefinite, rather than limited to a period of years, and almost always survive the termination of the license agreement. Often, the licensee must produce evidence that it has destroyed or permanently deleted all copies of source code and modifications thereto once its license has terminated.

Ownership. If the licensee is granted the right to modify the licensor's source code, then the parties must agree who will own those modifications. If the modifications are to be owned by the licensee, then the parties must also agree whether the licensor will receive a grantback license of any kind. These issues are discussed at length in Section 9.1.2.

Disclaimer of Warranties. If a licensee has the right to modify the licensor's source code, then the licensor will usually seek to disclaim any warranty or liability for errors or disruptions in the operation of the software, whether or not they are directly traceable to the licensee's modifications. While this may seem harsh for the licensee, it is often impossible to determine with precision what, precisely, has caused a software fault, particularly in large and complex systems (see Section 10.1.3.3, discussing warranty exclusions).

Escrow. Often, source code is "licensed," but placed in a third-party escrow account and released to the licensee only if the licensor fails to meet its warranty or maintenance obligations, or if the licensor suffers a bankruptcy or similar event that makes it likely that it will be unable to perform in the future (see Section 21.6).

18.2.4 *Maintenance, Support, Updates and Upgrades*

As noted in Section 10.1.3.8, many enterprise and OEM software licensing agreements include paid maintenance, support and other services by the licensor. The charge for these services is often based on a percentage (15–25 percent) of the annual licensing fee for the software. While the types of services included in these relationships can vary, below is a rough summary of what each generally entails.

Maintenance. Software "maintenance" generally means the correction of software errors and issues, often in accordance with a timescale that depends on the severity of the issue (see Sections 10.1.3.7 and 10.1.3.8).[40] Most maintenance plans include the provision of regular updates of the software (see below). Upgrades, on the other hand, may be included, but may also be offered by the licensor as new products subject to additional charges.

Support. Support generally refers to training and helpdesk support for the licensee's personnel who are using the licensed software. If the licensee has its internal "Level 1" helpdesk (which interacts directly with users), then the licensor may provide only "Level 2" and "Level 3" support. Level 2 support personnel generally interact with Level 1 personnel and do not take queries directly from users. Level 2 personnel are generally understood to be senior or specialist personnel with a higher degree of skill and familiarity with the software. Note that neither Level 1 or Level 2 support personnel are responsible for correcting errors in the software itself, only for responding to the large number of user inquiries and problems that can be resolved through the normal operation of the software. Level 3 support is often referred to as "engineering" support, and becomes involved only if an error in the software is detected or there is a compatibility issue with other software or hardware. Level 3 support personnel typically deal only with Level 2 support, and not with the Level 1 helpdesk or users. Level 3 support may be available only if the licensor also provides maintenance services to the licensee.

Patch or Correction. A software "patch" or "correction" is usually modified code that can be installed to address a problem or error in a software program.

Workaround. A workaround is a temporary way to avoid the consequences of a software error without actually correcting the error. For example, if a system uses the wireless Bluetooth protocol to connect to an office printer but the Bluetooth module malfunctions, a workaround might be to connect the system to the printer using a physical USB cable. This is not a correction of the software error in the Bluetooth module, but can often be implemented quickly to ensure that users can continue to use the system while a more permanent correction is developed or installed.

Updates. Software updates are new releases of a software program that correct errors, close security holes, ensure compatibility with new versions of hardware or operating systems, add support for new devices and make cosmetic changes. Updates are often designated by incremental increases of the software version number to the right of the decimal point (e.g., version 3.2 to 3.3 or 5.4.4 to 5.4.5, also called "point updates").

Upgrades. Software upgrades, often designated by increments to the left of the decimal point (e.g., version 3.2 to 4.0), are major modifications to a program that introduce substantial new features, performance or functionality.

[40] Computer hardware also comes with "maintenance" plans, which include configuration, repair and tuning of equipment, as well as installation of available software updates and upgrades. Hardware maintenance is often offered by third parties. Licensees engaging third-party software providers for hardware and software maintenance should ensure that their licensing agreements permit such third parties to access and reproduce licensed software. See note 33, supra, and accompanying text.

18.2.5 *Reverse Engineering Restrictions*

The term "reverse engineering" has its roots in the hardware world. It refers to the process of taking apart and inspecting a device to determine how it works, usually with the goal of building one's own device or creating another device that interacts with it.[41] From a hardware standpoint there is little that can be done to prevent reverse engineering. While patents may prevent one from making or using a new and infringing device, they are not effective at preventing the disassembly of a validly acquired device (particularly given recent judicial interpretations invalidating "conditional sales" of patented articles – see Section 23.5).

In the software industry, however, prohibitions on reverse engineering are viewed as more enforceable, both under trade secret and copyright law. These prohibitions are intended to prevent the user of a software program from reverse engineering an executable object code version of the software to derive its source code (or at least a source code approximation of what it does). In addition to reverse engineering, this process is also called disassembly or decompilation. While each of these activities is, from a technical standpoint, slightly different, the goal of each is to take the long string of zeros and ones comprising an object code program and convert it into human-readable source code. This, in turn, reveals how a proprietary software program works and, in theory, allows the reverse engineer to replicate it or to create products that interface directly with it (i.e., if the vendor does not provide an API to enable interoperability).

Reverse engineering of software code has long been a subject of dispute. In *NEC Corp. v. Intel Corp.*, 1989 U.S. Dist. LEXIS 1409 (N.D. Cal. 1989), the court held that NEC's reverse engineering of copyrighted microcode contained in Intel chips did not constitute an infringement of Intel's copyright.[42] A series of other cases found that the disassembly of video game console software in order to create game cartridges compatible with those consoles was a fair use under copyright law.[43] A few years later, § 1201(f) of the Digital Millennium Copyright Act expressly permitted reverse engineering for the sole purpose of achieving interoperability.

These legal developments led to the proliferation of contractual prohibitions on reverse engineering. Such prohibitions have, in turn, been challenged as preempting copyright law (which seemingly permits reverse engineering), but the prohibitions have largely been upheld (*Bowers v. Baystate Technologies, Inc.*, 320 F.3d 1317 (Fed. Cir. 2003, discussed in Section 17.1, Note 4)). Thus, prohibitions on reverse engineering are now standard features of the software licensing landscape.

EXAMPLE: PROHIBITION ON REVERSE ENGINEERING

Licensee agrees that it shall not, through manual or automated means, reverse engineer, reverse compile, reverse assemble, decompile, disassemble or otherwise seek to derive a Source Code version of the Licensed Software or otherwise to discern its internal architecture, structure or design.

[41] For example, one might reverse engineer a competitor's laser printer and printer cartridges in order to produce third-party cartridge replacements.

[42] See Jorge L. Contreras, Laura Handley & Terrance Yang, NEC v. Intel: *Breaking New Ground in the Law of Copyright*, 3 Harv. J.L. & Tech. 209 (1990).

[43] See *Atari Games v. Nintendo*, 975 F.2d 832, (Fed. Cir. 1992), *Sega v. Accolade*, 977 F.2d 1510 (9th Cir. 1992).

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

Notes and Questions

1. *Is software special*? Think of five ways that software licenses differ from licenses for other copyrighted works such as literary works and musical compositions. Now think of five ways that software licenses differ from patent licenses. How important are these differences? What would happen if a software program were licensed under an agreement used to license a motion picture for theatrical display, or a patent covering a new method of sequencing DNA?
2. *Source code*. Why is software source code treated so carefully? Think about the special measures taken to protect software source code when you read Section 19.2 about OSS licensing.
3. *Reverse engineering*. Why is reverse engineering routinely prohibited by software licensing agreements? Why do courts uphold these prohibitions, given the ample precedent establishing that reverse engineering does not constitute copyright infringement?
4. *Noncircumvention*. Noncircumvention clauses such as that discussed in the *Eden Hannon* case are not common in the software industry. Why not? Could a software vendor achieve advantages from such clauses that it might not otherwise be able to achieve using the provisions discussed in this section?
5. *Maintenance*. At 15–25 percent of the licensing fee per year, software maintenance programs are not cheap. Why does a licensee need to obtain maintenance services from the licensor? If you represented a licensee, are there any services typically included in a maintenance program that you would recommend your client forego (in an effort to reduce the annual charge for the program)? Other than revenue generation, why do you think that software licensors often insist that licensees purchase maintenance programs from them?

Problem 18.1

Your client AirBrain has designed a robotic carrier pigeon. In order to keep on track while flying it requires geospatial navigation software. As there is no existing pigeon-based navigation software, your development team believes that the fastest way to market is to adapt the navigation software developed by Boeing for commercial aircraft. Draft the licensing terms that you would propose to Boeing, including fallback positions if Boeing rejects your initial offers.

18.3 LICENSING IN THE CLOUD

The Role of Patent Pledges in the Cloud

Liza Vertinsky, *Patent Pledges: Global Perspectives on Patent Law's Private Ordering Frontier* 260–62 (Jorge L. Contreras & Meredith Jacob, eds., Edward Elgar, 2017)

The U.S. National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Put more simply, cloud computing is a form of computing that utilizes shared computer resources accessed over the internet or through mobile devices to deliver on-demand computing services. The cloud is a metaphor for the large data centers that perform the computing tasks desired by the end users.

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

This idea of concentrating computing resources at the center of a network rather than in user terminals is not new, but rather marks a return to the mainframe models of the 1950s, 1960s and 1970s. The use of the term "cloud computing" to refer to a distinct model of computing is new, however, and the rapid growth in cloud computing applications and services has produced what is now considered to be a distinct cloud computing industry.

While there are many firms offering different kinds of cloud computing applications and services, the industry is dominated by a small number of large firms. Amazon, Google, Microsoft and IBM are among the leaders in terms of market share and market influence, with Amazon by far in the lead in terms of market share. Other companies important in the cloud computing space include Salesforce.com, which pioneered software as a service, VMware and its competitor Citrix, which offer software for clouds, and Rackspace, which is leading a large coalition for free cloud software and provides its own public cloud and related services. On top of cloud computing platforms sit an increasing number of successful cloud computing companies such as LinkedIn (offers cloud based recruiting software), NetSuite (offers cloud-based business software), WorkDay (offers cloud based HR and finance software) and AthenaHealth (offers cloud based services for electronic health records), to name a few, all of which offer software as a service in targeted areas.

While the market leaders operate in all major segments of cloud computing and provide platforms for both developers and consumers, their business models and the ways in which these companies compete and expect to make money vary. In its current form the cloud computing market has been roughly stratified into three different segments: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). IaaS involves raw computing resources, analogous to virtualized hardware, providing customers with computing infrastructure for data storage, management and manipulation. It allows companies to outsource computing equipment and resources while giving them flexibility in how to deploy the infrastructure for their own purposes. Amazon has by far the lion's share of this market with its Amazon Web Services (AWS) platform. PaaS provides a platform and environment for building applications and services over the internet, operating essentially as a cloud based operating system. Microsoft and Google are among the market leaders in this segment, although Amazon's AWS is increasingly encompassing services that resemble those offered by a PaaS platform. PaaS examples include Google AppEngine, Microsoft Azure, and AWS Elastic Beanstalk. SaaS involves preconfigured software applications offered as a web based service to end users, like Google Docs and Gmail. These market categories increasingly overlap, however, as firms compete with alternative cloud platforms and accommodate new and disruptive technologies.

The cloud computing market is also differentiated into private, public and hybrid clouds. Private clouds are computing platforms that are under the control of a single customer, operated within the customer's firewall and under its own control. Public clouds can be used by anyone anywhere, based on a model of pooled, shared computing resources accessed over the internet. Hybrid clouds involve a combination of public and private cloud computing, allowing companies to keep certain computing functions or databases in house and have others externally provided via a public cloud. Amazon and Google focus primarily on public clouds, IBM began with a focus on private clouds but has subsequently found the need to embrace hybrid and public cloud strategies as well, and Microsoft has taken the lead in offering hybrid clouds.

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

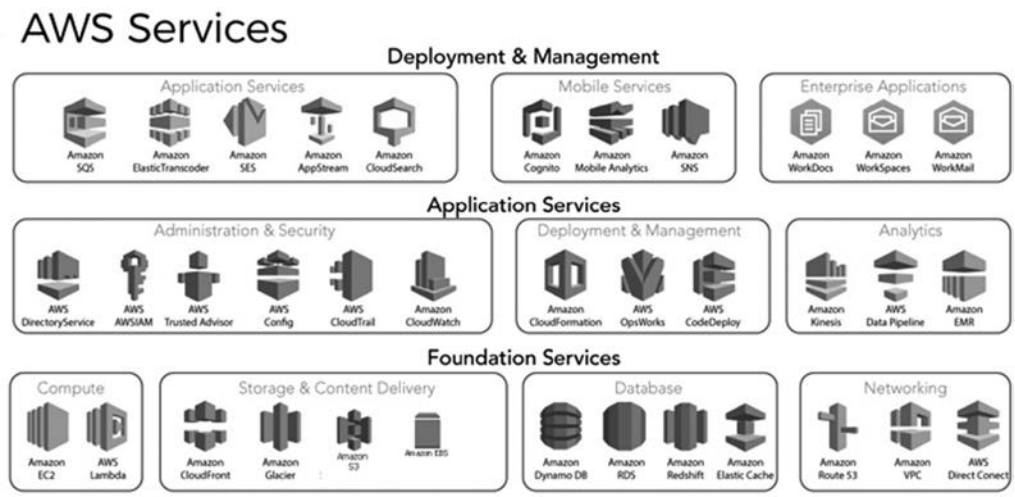


FIGURE 18.2 Amazon makes a range of applications available on a service-basis through Amazon Web Services (AWS).

Microsoft's cloud computing platform is called Azure. Below is an excerpt from a Microsoft document explaining the advantages of Azure to companies that are considering offering their own software and services to customers through the Azure platform.

Intellectual Property Protection: Azure Helps Protect your IP

Debra Shinder, Microsoft Corp. (n.d.), https://aka.ms/Azure-Trusted-IP

Business method and software patents provide a lucrative opportunity for non-practicing entities (NPEs), who stockpile large numbers of patents with no intention of developing products, but for the purpose of suing companies and individuals for infringement. This type of cloud-based patent litigation is increasing, and lawsuits and countersuits can cost your organization money and time and damage your reputation. The aggressive tactics of NPEs discourage innovation.

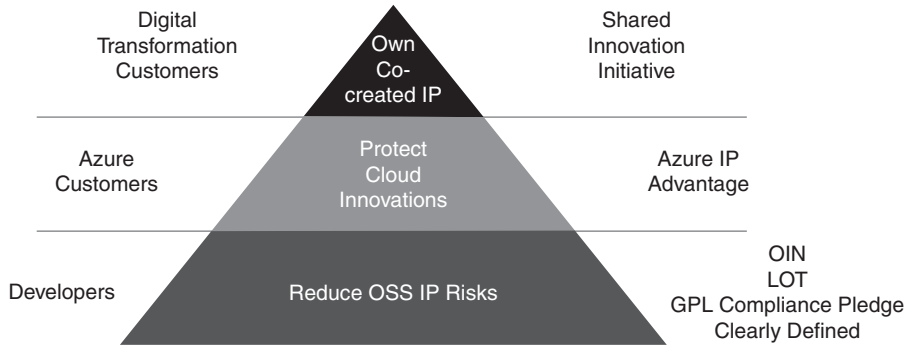
Trust in the cloud encompasses not only the assurance of security, privacy, compliance, and resiliency, but also clarity and confidence that your innovations will be protected against frivolous infringement claims, including when you co-develop innovative solutions working together with a cloud provider. Microsoft Azure IP Advantage and the Shared Innovation Initiative can help offer that assurance.

IP in the Cloud

As computing shifts to the cloud, new risks to innovation emerge. These include risks to developers, to Azure customer organizations working in the cloud, and to customers who co-create intellectual property with Microsoft as part of their digital transformation.

Microsoft trust and IP initiatives build on one another to provide protections to all three of these categories.

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press



Azure IP Advantage

Intellectual property is increasingly being created, stored, and shared in digital form. Digital transformation has brought a paradigm shift to the business environment as companies embrace new approaches to creating, communicating, and interacting with customers, partners, and the public.

NPEs see this as an opportunity; they collect and hoard patents and then assert patent infringement against innovators. This is a growing concern for cloud services customers, and the fear of a patent suit discourages innovation in the cloud. Cloud providers can help their customers reduce the risk to be able to innovate with confidence, and Microsoft Azure offers best-in-industry protection against IP risks. Azure IP Advantage includes:

- **Uncapped indemnification**. This covers claims for IP infringement and extends to open source software (OSS) incorporated by Microsoft in Azure services (for example, Apache Hadoop used for Azure HDInsight). It is provided by default for all Microsoft cloud customers.
- **Patent Pick**. Microsoft provides a portfolio of 10,000 patents that customers can pick from and use to deter and defend against patent lawsuits. It is available to consuming Azure customers with an Azure usage of $1 k/m over the last three months who have not filed a patent infringement lawsuit against another Azure customer for their Azure workloads in the last two years. This helps to discourage excessive litigation.
- **Springing license**. This provides peace of mind with future patent protection; if Microsoft sells any of its patents to an NPE in the future, its customers will receive a license, so the NPE won't have an infringement suit against the customer. This is available to all consuming Azure customers with an Azure usage of $1 k/m over the last three months. Unlike other cloud providers, Microsoft does not require a reciprocal commitment from the customer for its patents. In addition, Microsoft is a member of the LOT Network, a non-profit community of companies that was formed to preserve the traditional uses of patents while providing immunization against the patent troll problem.

These protections help free companies to concentrate more on building their businesses, leveraging open source software, and serving their customers, and less on dealing with patent litigation.

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

Shared Innovation Initiative

Every company today is becoming in part a software company. Companies are increasingly collaborating with their cloud providers to co-create intellectual property to transform their business operations. There is growing concern that without an approach that ensures customers own key patents to these new solutions, tech companies will use the knowledge to enter their customers' market and compete against them—perhaps even using the IP that customers helped create.

Microsoft developed its Shared Innovation Initiative in response to these concerns when customers collaborate with Microsoft to develop new products and services that run on the Azure platform. We've created contract terms that lay out these principles for engagements where the parties are co-creating new IP. Shared Innovation builds on our approach outlined in the AIPA, and is based on seven guiding principles:

1. **Respect for ownership of existing technology**. We each own the existing technology and IP that we bring to the table when we partner together. As we work with customers, we'll ensure that we similarly will each own the improvements made to our respective technologies that result from our collaboration.
2. **Assuring customer ownership of new patents and design rights**. As we work together to create new technology, our customers, rather than Microsoft, will own any patents that result from our shared innovation work.
3. **Support for open source**. If our shared innovation results in the creation of source code and our customers so choose, Microsoft will work with them to contribute to an open source project any code the customer is licensed to use.
4. **Licensing back to Microsoft**. Microsoft will receive a license back to any patents and design rights in the new technology that results from the shared innovation, but the license will be limited to improving our platform technologies.
5. **Portability**. We won't impose contractual restrictions that prevent customers from porting to other platforms the new, shared innovations they own.
6. **Transparency and clarity**. We will work with customers to ensure transparency and clarity on all IP issues as the shared innovation project moves forward.
7. **Learning and improvement**. We'll continue to learn from this work and use this learning to improve further our shared innovation work.

Notes and Questions

1. *The cloud*. What is the "cloud"? How many of your daily activities involve use of a service provided via the cloud? (There may be more than you think.) As Liza Vertinsky points out, cloud computing is not new – it goes back to the roots of the computing industry in the 1950s. Why do you think that, after a long dormancy from the 1990s through the 2010s, cloud computing has recently made a comeback?
2. *Service not software*. From a contracting standpoint, the principal difference between obtaining software through physical media (disc or download) and through a SaaS model via the cloud is that cloud-based software delivery services typically don't provide the user with a copy of the executable program itself. Rather, the software is accessed through a browser or "thin" app front-end, but the bulk of the program – its guts – are stored and executed

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press

remotely. Thus, a SaaS license is really a service contract. While some small software elements may be downloaded to the user's computer, the crux of the contractual relationship that is established is not one of licensor–licensee, but of service provider–customer. What advantages and disadvantages can you see to obtaining access to a program remotely through SaaS rather than obtaining a physical copy of the software to run on your own computer? SaaS applications are priced in various ways, but one common method is a monthly service fee – just like a cable or phone service contract – rather than a one-time "purchase price" for a software program. What advantages and disadvantages exist with these different "purchase" models?

3. *Public, private, hybrid*. What relative advantages and disadvantages do you think a software vendor would derive from offering its software through a public, private or hybrid cloud platform? What are the differences among these three cloud structures?
4. *IP risks in the cloud*. Microsoft offers its customers (companies that host their software on the Azure cloud platform) several novel IP-related incentives. What threat is Microsoft responding to? Why is this threat of concern to customers of cloud-based services? How does each of Microsoft's Azure IP initiatives (uncapped indemnity, patent pick and springing license) respond to this threat? Which of these initiatives do you think offers customers the greatest protection from IP threats?
5. *Shared Innovation Initiative*. Microsoft's Shared Innovation Initiative is aimed at companies that wish to develop new software offerings for the Azure platform. How do the IP allocation terms of the Shared Innovation Initiative differ from what one might expect in a collaboration between Microsoft (one of the world's largest corporations) and a developer of software for its platform (see Section 9.3, discussing allocation of IP in joint development projects)? Why do you think Microsoft took this approach? Which of the Shared Innovation Initiative program features do you think is most important to Microsoft? To its customers?

https://doi.org/10.1017/9781009049436.019 Published online by Cambridge University Press