Navigating the protection of big data

In the first of a two-part series, **David A Prange** examines whether to use patent protection or trade secrets when protecting big data analytics

The continued miniaturisation of computing power, wireless interconnectivity, and the expansion of the internet has led to the production of large-scale quantities of data. Considered on a macro level, the data may reflect consumer preference trends or event probabilities that, if identified, may be useful for guiding business decisions. Ongoing advancements in parallel processing allow businesses to analyse this "big data" to gain greater understanding of customers, business processes, and risks. Companies thus may now tune business decisions based on data analytics.

While data analysis strategies continue to change business practices, big data analytics and results should motivate companies to define or revisit strategies for protecting these proprietary investments. Specifically, challenges to software patent protections, the more stringent application of subject matter patentability requirements, and a developing shortage of qualified data scientists mean that companies should consider or revise policies to protect big data analytics as trade secrets. The first part of this two-part series will frame the dilemma of protecting proprietary big data intellectual property in view of the current state of patent law for software and algorithm-based inventions, as well as trade secret law after the passage of the federal Defend Trade Secrets Act. Part two of the series will consider available strategies for protecting big data trade secrets in the US.

Big data basics

A concept originating in the late 1990s, the term "big data" describes both large volumes of data and resulting data processing employed to understand this data. Big data is generally characterised as:

- A large volume of generated data;
- Generated for analysis at a rapid velocity; and
- Consisting of a variety of formats in which the data is available.

The data may be generated by the numerous computing devices that now permeate our society – including personal handheld devices, personal computers, machine or environmental sensors designed to record and provide specific types of information. The data may also originate from government or other institutional sources that record statistical information – eg, census or survey information. Regardless of source, data comprising big data consists of a large accumulation of individual events or facts. At a macro level, these individual events or facts may reveal consumer trends, machine failure probabilities, or other population preferences that may provide actionable insight for company decisions. The analysis for finding these trends means developing and employing software and algorithms consisting of step-by-step processing instructions that may categorise, manipulate, and analyse the available data set. These software processes may be tuned to the specific industry and data set to which the software is applied. In turn, the software analytics required for big data analysis has resulted in engineering specialisation for software engineers. As can be presumed, extracting actionable information from these big data sets requires time and financial investment to develop appropriate expertise and usable information.

The software patent problem

Historically, significant attention for protecting software innovations had been focused on patents including, for example, innovations that may relate to big data analytics. Although underlying mathematical algorithms have been recognised as unpatentable for some time,[1] patent applicants have tried numerous different claiming techniques to claim software originating from algorithmic instructions. In 2014, the Supreme Court of the US (SCOTUS) considered the patentability of software in *Alice Corp v CLS Bank Itnl.*[2] Although the court did not establish a *per se* rule that software inventions are unpatentable, SCOTUS held that patentability analysis for software patents must consider whether the claims (1) only encompass abstract ideas and (2) if encompassing an abstract idea, whether the claims include some additional inventive step showing an application of the abstract idea. Applying this test, the Supreme Court in *Alice* invalidated the patent at issue because it consisted of computer-implemented business processes for mitigating settlement risk for trades between financial institutions. According to the court, the process could be done without the assistance of a computer.

A result of the *Alice* decision has been increased scrutiny on software patents and more aggressive challenges by patent infringement defendants. Both Federal Circuit and district court decisions following

the two-part *Alice* test for patent subject matter eligibility demonstrate a stiffening inquiry to the patent eligibility requirement. Cases addressing patents directed to the manipulation of information using a computer that may otherwise be done by hand, albeit more slowly, have found such types of patents invalid. For example, in *CG Technology Development, LLC v Big Fish Games, Inc*,[3] the court considered a patent addressed to collecting user gaming information and then generating and displaying statistical information based on the collected gaming information. The court held the collection and generation of statistical information as an abstract idea. The court went on to find that the claim did not demonstrate any inventive concept by demonstrating a specific application of that abstract idea. Other cases have found the general manipulation and processing of data likewise unpatentable.[4]

The *Alice* decision and its progeny have made patent protection more uncertain when it comes to software patents. Older patents prosecuted without the benefit of the *Alice*-line of cases now have a greater risk of being invalidated as defendants and courts can apply the more rigorous test for subject matter eligibility than was considered at the time of prosecution. Current prosecution itself has become more difficult with the patent office placing greater scrutiny on the eligibility requirement through application of specific guidelines promulgated to patent examiners.[5]

This recent development in patent law suggests that protecting big data analytical software with patent protection should be reconsidered. As big data analytics focuses on source code and algorithmic manipulation of data sets, it suggests that patent protection may be more difficult to obtain. Even if a patent is issued and then asserted, defendants and courts now routinely address patent subject matter eligibility issues early in litigation. Doing so reduces potential leverage of the patent owner. It is not to say that patent protection is unobtainable for big data software analytical tools. At least one recent Federal Circuit case addressing software patenting has cooled what had been a rapidly developing invalidation of software patents.[6]

While there may still be an opportunity to obtain patent protection relating to big data analytics (as it will depend on the proposed claim language), other patenting requirements also should be considered. For example, the patent application should provide an adequate written description of the invention as well as the best mode known to the inventor at the time to practise the invention. To adequately support the claims this may require disclosing the algorithms and specific software code that are used to drive a company's big data analytics. This disclosure is generally made at the time of filing the patent application. Thus, a company seeking patent protection for its big data assets may arrive at the unenviable position of disclosing to the public an asset with significant underlying investment yet still not obtain patent protection for it.

Turning to trade secret law

In the aftermath of *Alice* and the increased scrutiny placed on software inventions, trade secret strategies may provide an alternative to protecting big data analytics. Up until the passage of the Defend Trade Secrets Act (DTSA), discussed below, state-by-state variations in trade secret law protections complicated the assertion of trade secrets cases. While many states have enacted versions of the Uniform Trade Secrets Act (UTSA), a degree of uncertainty stemmed from legislative action and state court interpretations of these laws. For example, state law exhibits some significant variation on the definition of a trade secret. Some states apply a common law definition derived from a six-factor test originating from the Restatement of Torts; other states implemented variations of the UTSA definition of a trade secret.

The DTSA, passed in 2016,[7] may remedy some of the existing uncertainty. The DTSA introduces a new federal civil cause of action for trade secret misappropriation. The federal law adopts with minimal amendment the existing definition of a trade secret as used for criminal claims based on the Economic Espionage Act. This definition expressly contemplates protecting computer source code as a trade secret. To that end, the DTSA-adopted definition of a trade secret expressly includes source code, algorithms, programs, and data sets as potential types of information that may be considered a trade secret.

A trade secret protection strategy would appear to be a natural fit for big data source code analytical tools. Unlike patent law, there is not the immediate, and now potentially substantial, hurdle of demonstrating that the source code one desires to protect is eligible subject matter. Nor is there a novelty requirement for protecting information as a trade secret in comparison to obtaining a patent based on that same information. Even so, the statutory definition of a trade secret requires the owner to take reasonable measures to keep the information secret. To assert a trade secret in a misappropriation case, the owner may need to demonstrate that the steps the owner took to protect the information were reasonable under the circumstances. Further, trade secret protection can be more limited than patent law. For example, a third party may legitimately reverse engineer a product to find a trade secret and not be liable for trade secret misappropriation. Thus, while trade secret protection afforded under the DTSA may more easily accommodate the subject matter for protection – source code and algorithms – the trade-off is that a company may be charged with continual vigilance to maintain that secrecy.

Summary

What to do with those big data assets? Businesses investing in big data analytics face increasing uncertainty following the erosion of patent protection. But state trade secret law and the passage of the DTSA offer an alternative avenue for protecting these assets. Trade secret law, however, provides no easy answer for how to approach or implement a protection strategy to adequately cover big data assets. These big data assets manifest themselves both as the software, algorithms, and data sets from which companies derive trends to inform on business decisions. But these big data assets also are the data software engineers who develop the algorithms used. Thus, companies should employ complementary measures to ensure that their big data assets do not walk out the door for a competitor's use. Suggestions on what to do is up next in part two.

Footnotes

1. *Gottschalk v Benson*, 409 US 63 (1972).
2. 134 S Ct 2347 (2014).
3. 2:16-cv-00857-RCJ-VCF (D Nev 29 Aug 2016).
4. See, eg, *OpenTV, Inc v Apple Inc,* No 14-cv-01622, 2015 US Dist LEXIS 44856 (ND Cal 6 Apr 2015).
5. See www.uspto.gov/patent/laws-and-regulations/examination-policy/2014-interim-guidance-subject-matter-eligibility-0 (last accessed 5 Oct 2016).
6. *Enfish, LLC v Microsoft Corp*, 822 F3d 1327 (Fed Cir 2016).
7. Pub L No 114-153, 130 Stat 384 (2016).

Author

David A Prange is a trial lawyer and registered patent attorney at Robins Kaplan. He focuses on complex business litigation with an emphasis on intellectual property, including patents, trade secrets, trademarks, and licensing disputes.