Big data and trade secrets: part 2

Concluding a two-part series, **David A Prange** discusses how to protect big data IP and the coming shortage of data scientists

The digital age and its enormous quantities of data – big data – have created new opportunities for recognising and capitalising on data-driven insights. In recent years, companies have accelerated investments in big data to identify consumer demand trends, product and equipment life cycles, and economic changes. These investments include the technology and processes for big data analytics, as well as personnel for performing those analytics. These investments result in developed intellectual property that may provide forthcoming competitive advantages.

Part I[1] of this two-part series considered some legal strategies for protecting big data assets. Big data analytics present protection challenges based on their character – software, algorithms, and data consisting of generated raw data and the resulting analytic data results. Patent protection is more difficult to obtain as increased scrutiny is placed on "software" patents that otherwise simply automate mathematical calculations or sorting that could be done, in theory, without a computer. Trade secrets law offers an alternative for protecting big data assets. Passage of the US Defend Trade Secrets Act ("DTSA") in 2015 may eliminate some of the state-to-state variations that often created uncertainty when using trade secret law to protect intellectual property. As a result, trade secrets law may become more attractive for protecting a company's cultivated big data proprietary advantage.

Protecting big data should also include consideration of the role played by data scientists. The DTSA includes an expansive definition of a trade secret, allowing for potential broad coverage of almost all aspects of a business. But trade secrets law is still dependent on the character of what is protected – information. When it comes to big data, the definition of a trade secret encompassed by the DTSA may be inadequate. It may not address the unique value the data scientists themselves develop as a result of their immersion in the data. A coming data scientist shortage means companies should refine their protection framework now to better position themselves should a dispute arise regarding its intellectual property with big data. Part II of this big data article series highlights some considerations for better protection.

Data scientist shortage and the increased risk to big data assets

Data science is an interdisciplinary field focused on processes and systems to extract information and insights from large structured and unstructured data sets. Data science professionals rely on mathematics, statistics, operations research, information science, and computer science to interpret, manage, and visualise information trends. Numerous universities now offer undergraduate and graduate programmes to prepare individuals for careers in the field. The current demand for data scientists significantly outpaces demand; some industry analysts predict a 50% shortfall of available data scientists for available jobs by 2018.[2]

This projected industry shortage of skilled individuals places greater risk on company big data intellectual property. As companies across industries cultivate strategic advantages with big data, pressure builds within and across industries for all market participants to use big data. The result is increased competition for available data scientists. Competition will make data scientists a highly sought-after kind of employee – and one that could leave with a business' proprietary information unless properly managed.

Protecting big data assets: reasonable efforts paired with employment contracts

Complicating the challenges of potential data scientist mobility is the nature of big data software and data assets, which can be easily moved from computer to computer. This easy transportability suggests that companies should rely on a combination of physical measures and additional contract provisions to protect their big data investments. For information to be a trade secret, a company should take reasonable efforts to protect that information.[3] If a company asserts a trade secret, the company may have to explain how it has kept the information confidential. Company sophistication matters. Larger, more sophisticated companies may be held to a higher standard than smaller or less sophisticated companies.[4] Thus, precautionary measures that any business should take to implement network security, such as network password protection, access limitations, and computer port limitations (for example, preventing flash drive use), may not be sufficient under the circumstances for protecting big data. Other physical protections may be necessary, including limited networks and avoiding cloud storage of information (unless the cloud itself is proprietarily protected). Actively cataloging the types of information protected as a trade secret in order to evaluate the existence of redundant protective measures serves as another good practice. The exercise, if documented, may be used at trial as an exhibit to help explain to a jury the different processes that are used to protect a company's trade secret information. But doing such a study also has risks if the conclusions are not followed; a party challenging a trade secret may point to the lack of diligence as proof that reasonable measures were not taken to protect asserted trade secret information.

Protecting people assets – the data scientists – can be more difficult because they cannot be locked away like the software and data on which they work. Placing restrictions on data scientist employment opportunities potentially conflicts with the public policy goal of promoting worker mobility. Some US states recognise an "inevitable disclosure" doctrine,[5] providing that an employee with knowledge of a trade secret can be prevented from working for a competitor on the theory that the individual's work at the competitor will result in the "inevitable disclosure" of the trade secrets learned at the former employer. Other states have not endorsed this doctrine,[6] or taken a middle position in which application of the doctrine depends on the type of individual or if there is a separate employment agreement.[7] The DTSA takes an intermediate position in allowing for an injunction award against an individual. To enjoin an individual based on statutory trade secret misappropriation, there must be actual or threatened misappropriation as opposed to the individual possessing general knowledge.[8] It can be more difficult to prevent a data scientist from leaving for a competitor if there is no specific misappropriation identified.

Adding limitations to an employment agreement that restrict future employment opportunities also may be difficult to enforce. Relying on a covenant not to compete to try and restrict data scientist mobility after termination means applying state law, which differs significantly across the US. There is no uniform statutory provision that reduces enforcement uncertainty. At the state level, many states will enforce a covenant not to compete provided the defined restriction is reasonable in purpose and scope. Other states, including California, consider such covenants void and unenforceable in many circumstances. This general prohibition, however, does not necessarily reach a limited restriction that focuses on the trade secrets of the former employer. In such a case, the trade secrets should be defined with sufficient specificity to put the employee on notice of what the employee cannot use once that employment terminates. The specificity should motivate companies to take steps to evaluate what information could be a trade secret and then provide education to employees on what this information is and how to use it. These types of provisions will also support a conclusion that certain information is a trade secret and the contractual provision is another reasonable effort taken to keep the information secret. Thus, while companies with big data assets may not be able to simply prohibit employees from moving to competitors, companies can limit former employee activities related to the company big data trade secret assets to which the employee was exposed.

Covenants not to compete tailored narrowly to address trade secrets should do several things beyond identifying the trade secrets with as much specificity as may be practicable at the time of contracting. The agreement should further include an employee acknowledgment addressing ownership, secrecy, and the fact that the employer has taken reasonable efforts to keep the information secret. The agreement should further include an obligation on the part of the employee to return all company property upon termination of employment. The agreement should also provide for continuing obligations on the part of the employee after termination to keep trade secret information secret. These types of provisions can and should likewise appear in company-to-company nondisclosure agreements that companies may use to further business collaboration.

Summary

Protecting big data assets has no easy solution – patent protection is more difficult to obtain and trade secret protection has been characterised as requiring "eternal vigilance"[9] to police secrecy and company trust in its employees. In many respects, trade secret protection steps for big data assets are similar to protecting other types of trade secrets, such as chemical formulas or manufacturing processes. But software analytics and the data on which it works (and the data produced by the analytics) may be more easily portable by the nature of being software. There also may be a greater risk of loss because software practices that favour open source sharing may influence data scientist understanding about the scope of what is proprietary company information and what is not. The challenge to protect big data assets suggests using complementary protection strategies, focusing as much on the data scientists as the software and analytics themselves, to help keep secrets secret and competitive advantages arising from those secrets preserved.

Footnotes

[1] Navigating the protection of big data, *Intellectual Property Magazine's* Dec/Jan 2017 issue, p.54.

[2] See Deloitte *Analytics Trends 2016: The Next Evolution,* p7 (2016) available at www2.deloitte.com/content/dam/html/us/analytics-trends/2016-analytics-trends/pdf/analytics-trends.pdf

[3] 18 USC § 1839(3).

[4] See, eg, *Fail-Safe, LLC v AO Smith Corp*, 674 F3d 889 (7th Cir 2012).

[5] See, eg, *WL Gore & Assoc, Inc v Wu*, 2006 WL 2692584 (Del Ch 2006).

[6] See, eg, *Whyte v Schlage Lock Co*, 125 Cal Rptr 2d 277 (4th Dist 2002).

[7] See, eg, *H&R Block Eastern Tax Servs, Inc v Enchura*, 122 F Supp 2d 1067 (WD Mo 2000).

[8] 18 USC § 1836(3)(A)(i)(I).

[9] *RTE Corp v Coatings, Inc,* 84 Wis2d 105, 118 (Wis. 1978).

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.