KILPATRICK TOWNSEND

6 KEY TAKEAWAYS

IP Protection for Data

Data-driven businesses derive enormous value from data. That data, for example, is often collected from the businesses' website visitors. Data scrapers are automated scripts that collect data from websites. But, what if a data scraper is using data collected from a business's website to build competing products or services? What strategies can that data-driven business employ to protect collected data against misappropriation by data scrapers?

Kilpatrick Townsend's Sameer Vadera recently addressed these issues and more at the IPO Annual Meeting in Washington, D.C. His presentation, "IP Protection for Data," offered six key takeaways.

1

Can Copyright Law Protect Collected Data? *Yes, but copyright protection is thin*. A 1991 Supreme Court decision (*Feist Publications v. Rural Telephone Service Co.,* 499 U.S. 340 (1991)) held that the individual facts of a data set cannot be protected by copyright. The organizational structure of a data set, however, can be protected by copyright, if there is originality in the selection or arrangement of the data elements. In the context of big data, if there is originality in the inclusion of certain data fields of the data set, copyright protection can protect the data sets.

2

Can Trade Secret Law Protect Collected Data? *Yes, but businesses should take reasonable measures early to keep the data secret.* To be a protectable trade secret, the data set must derive independent economic value from not being generally known or readily ascertainable through proper means. Unlike copyright protection, trade secret protection does extend to the underlying facts in a data set.

3

Try Protecting a Data Set Under Contract Law. *If copyright law and trade secret law do not provide adequate protection, contract law is the first line of defense for many data collectors*. Effective legal obligations should be put into place upstream before users get access to the data set. Consider using a contract to restrict access to the data set unless the user agrees not to copy or commercially exploit the data. Common contract mechanisms include website terms-of-use agreement and contracts with vendors accessing the data.

4

What Other Avenues are Available For Protection?

- *Technical measures*: Technical measures can include, for example, password protecting the data set, encrypting data, configuring website designs to increase the difficulty of scraping data on the website, and creating mandatory click-through agreements that create legal obligations that prevent misuse of the data.
- *Digital Millennium Copyright Act:* The DMCA prohibits users from circumventing technological protection measures. The DMCA, however, requires that the data set include copyrighted content owned by the party seeking protection.
- *Computer Fraud and Abuse Act:* The CFAA prohibits accessing a computer in an unauthorized manner. While businesses have asserted CFAA claims against data scrapers, courts have generally interpreted data scraping as falling outside of the prohibited "access without authorization" covered by the CFAA; especially in scenarios where the data was publicly accessible on a website. *See hiQ Labs v. LinkedIn,* No. 17-16783 (9th Cir. 2019).
- *State tort law claims:* Creative approaches to protecting data can include asserting state tort law claims, such as misappropriation, lost profits, unfair competition, electronic trespass to chattel, and others. Depending on the fact patter, however, state tort law claims can be preempted by copyright or trade secret law.

5

What About Open Data Licenses?

- Consider whether there is business value to protecting mission-critical data (e.g., using trade secrets) and openly providing the remainder of the collected data set(s) under an open data license. Open data licenses are similar to open source licenses, in that the licenses encourage the sharing of data. This approach has the advantage of placing the burdens of data quality and data curation on stakeholders. In the machine learning and artificial intelligence context, improving data quality of data sets before ingesting the data sets into models can be burdensome and costly to a business. Providing the data to stakeholders who take on the burden of improving data quality can cut costs.
- Examples of data sets provided under open data licenses:
  - The Guardian Open Data Platform, X-force Exchange, and the Waymo Open Data Set

6

Summary

- Legal protection of collected data sets is often insufficient; especially considering the enormous value that data can yield. Implementing technical measures (e.g., password protecting data) and legal obligations (e.g., website terms-of-use agreements) early before data scrapers can access the data bolsters a business's prospects of protecting data.
- Businesses often employ a "kitchen-sink" approach, in which claims asserted against data scrapers include copyright, trade secret, contract law, and various statutes, such as the CFAA. *See hiQ v. LinkedIn*.
- Consider protecting core business data under trade secret law and making the remaining collected data available under open data licenses. This approach can increase the certainty of protection and reduce costs, for example, by avoiding the need to improve data quality or manage data curation of the collected data.

For more information, please contact:
Sameer Vadera, svadera@kilpatricktownsend.com