Big Data, Social Media, and IP: How to Make "Likes," "Tweets," and "+1's" Your Trade Secrets

How to protect proprietary intellectual property (IP) trade secrets rights for insights and algorithms derived from social media big data.

April 25, 2014

Publication

Leading players from different business sectors have spent the past few years learning how to use social media insights and analytics to drive consumer behavior. But outside partners usually provide the algorithms that drive those insights—and probably own any proprietary IP rights associated with them.

As data sources and sets continue to grow, many businesses see an advantage in bringing some "big data" capabilities in house. Taking such a step can give a business a leg up on their competitors by allowing them to turn the information big data creates into a company asset. And, in certain instances, it can also provide some opportunities for businesses to protect key data-derived insights under trade secret law, even if data from outside social media sources is a part of the underlying data set.

What is "Big Data"?

Big data has no single, accepted definition. Many use a three-fold definition based on data volume, velocity, and variety—or the "three Vs." Occasionally, those that use this approach include a fourth "V" to cover the data's value, veracity, or viability. When used this way, big data includes traditional structured data, which resides in a fixed field within a record or file, and unstructured data from sources like videos, social media, and RSS from sources within and outside an organization.

But another definition of big data exists. Under this alternative approach, "big data" is the term used to define the process of applying new computing tools and capabilities—like machine learning and artificial intelligence—to the ever-expanding universe of massive, complex information. Under this approach, big data is a term that helps describe the storage and analysis of large data sets using new, sophisticated, and evolving computing techniques and tools.

Regardless of the definition, members from a variety of industries are now leveraging big data to gain insights, predict consumer behavior, and make critical business decisions.

Big Data at Work

Large companies that interact directly with consumers or that have consumer brands have begun to use big data social media analytics tools to expand on consumer empathy capabilities, make real-time adjustments to marketing programs, and help bring the voice of the consumer to the decision-

making table. For example, Proctor & Gamble has built "Business Spheres" meeting spaces in more than 50 locations that allow 360° view of big data analytics visuals. Additionally, a host of third-party providers offer numerous ways for a variety of businesses to generate, capture, and act on data generated by consumers, particularly in social media.

Trade Secret Laws and Big Data

While trade secret laws differ from state to state, generally any innovative formula, practice, process, design, instrument, pattern, or compilation of information receives protection from unauthorized use if, in fact, efforts have been taken to keep secret the information or innovation in question. Under this definition, the tweets, texts, and Facebook status updates of customers and consumers obviously don't qualify for trade secret status. But, once social media data gets brought in-house, big data capabilities may allow use of trade secret law to protect at least some of the data contained within it.

Specifically, trade secret law may extend its protection to the analytic data sets and inferences that big data analysis generates because of the advanced properties and extended uses that exist within that derived data. As a result, when companies start thinking about big data, they should also think about trade secrets because, done right, big data could lead to proprietary insights.

Trade secret protection usually attaches when the information is not generally known in the industry, a company has taken reasonable measures to keep it secret, and the secrecy has some economic value. Measures that can help protect social media big data secrets are the same as those used to protect other trade secrets: confidentiality agreements, specific contracts terms, secrecy policies, training, and infrastructure.

BUT: Protect Your Data First

Bringing outside social media data is not without risk. Outside data could:

- Come in with corruptions or malware (destructive software) that bypasses the data security measures your organization has in place
- Contain personably identifiable information (PII) or other information subject to privacy laws that requires special handling
- Be rights-encumbered or give rise to antitrust concerns, especially if it contains pricing information
- Impact existing data preservation obligations that arise from ongoing or contemplated litigation—the dreaded E-discovery

These risks mean that any company contemplating taking advantage social media big data opportunities need to play both offense and defense to maximize the asset value of the information while mitigating the threats the data can create.

The Time for Big Data Is Now

Whatever definition gets used, big data is here to stay and—for better or worse—so is social media. The time is ripe is for companies to take control of the wealth of opportunities that big data can generate from consumer social media, including potential proprietary, protectable trade secrets. To make the most of these opportunities, businesses must now start creating a plan to protect those secrets while also addressing the risks that's always a part of social media big data.

Thomas Mahlum is a partner at Robins Kaplan LLP. He represents Food and Beverage companies in complex business disputes involving contracts, intellectual property, unfair competition, trade secrets and fraud actions.

Related Attorneys

Thomas C. Mahlum

Services

Intellectual Property and Technology Litigation

Trade Secret Litigation