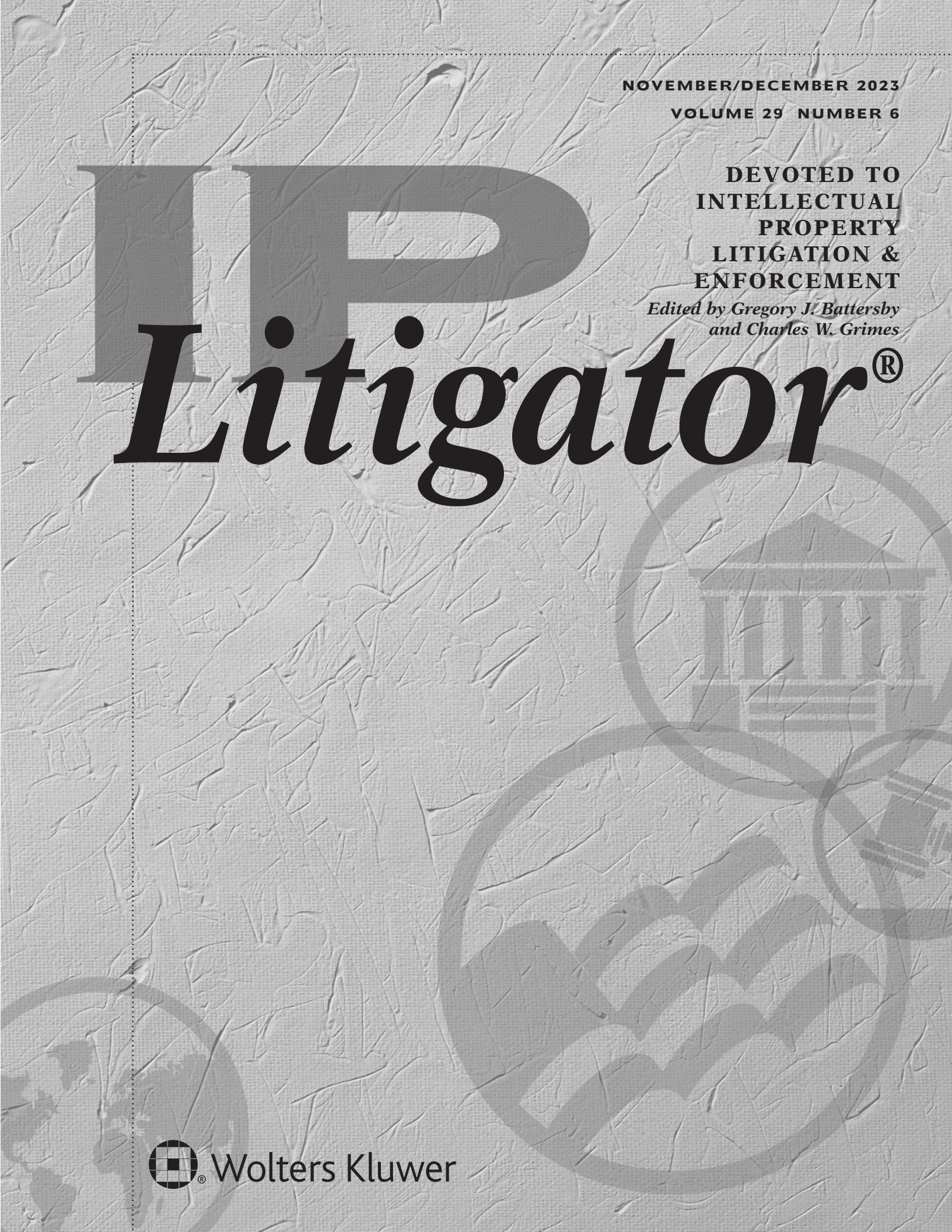
NOVEMBER/DECEMBER 2023
VOLUME 29 NUMBER 6

IP Litigator®

DEVOTED TO INTELLECTUAL PROPERTY LITIGATION & ENFORCEMENT

Edited by Gregory J. Battersby and Charles W. Grimes



Wolters Kluwer

Why Privacy And Trade Secret Law Are On A Collision Course

Jenny Colgate

Jenny Colgate, a partner at Rothwell Figg in Washington, D.C., is an experienced litigator whose experience extends into all facets of intellectual property and technology-related matters, including patents, data protection, trade secret, unfair competition, trademark, copyright, breach of contract, and fraud claims. In addition to litigation, Jenny consults with clients regularly on privacy law compliance and best practices, IP strategy, and contracts and licensing negotiations.

Can privacy law and trade secret law coexist, or is compliance with both impossible?

We are experiencing the fourth industrial revolution, driven by the rise in data and connectivity, analytics and artificial intelligence.

In the past industrial revolutions, the driving technologies were protectable by patents — things such as mechanization, steam power, water power, mass production, electricity and information technology systems.

Unfortunately, patent coverage does not extend to many of the driving technologies of the so-called Industry 4.0. To protect large data sets, algorithms for processing data, and the resulting takeaways from that data processing, companies typically have to turn to trade secret law.

Trade secrets are intellectual property rights on confidential information that may be sold or licensed.

To qualify as a trade secret, the information must be commercially valuable because it is secret, known only to a limited group of persons, and subject to reasonable steps taken by the rightful holder of the information to keep it secret, including the use of confidentiality agreements for business partners and employees.

But how can companies ensure confidentiality and limit knowledge of trade secrets when privacy statutes, ever-growing in breadth, subject the very same information to transparency and disclosure requirements? There is a conflict between data privacy and trade secret law.

What is more is that the conflict between privacy law and trade secret law keeps growing. Data privacy laws are expanding in scope, encompassing more potential trade secrets without providing a trade secret exception.

Some privacy laws are also being passed with private rights of action and the prospect of hefty damages, heightening the risk for companies forced to choose between protecting their trade secrets and strictly complying with privacy laws.

Meanwhile, trade secret law is also growing in scope. Companies are increasingly relying on trade secret law to protect valuable corporate assets, and as companies' reliance on trade secret law grows, so do the damages verdicts in trade secret misappropriation cases.

In 2022, several juries in trade secret cases awarded extraordinary verdicts to plaintiffs — including a $2 billion award to Appian in Appian Corp. v. Pegasystems Inc. this May in the Circuit Court of Fairfax County, Virginia.

How should companies deal with the conundrum of trying to comply with these two conflicting legal regimes?

Industry 4.0

For exploring these questions, we turn to three major industries, including food, retail and medical devices, and we look at some of the data sets and artificial intelligence that are driving technological development competition.

In the food industry, analysis of data from food manufacturers' sales history and the sales of similar product lines has also helped with supply chain optimization, enabling product sales figures to be estimated before goods have even been transported to the shop.[1]

In the retail industry, AI-powered product recommendation engines are changing the way that customers shop. A product recommendation engine filters and sorts a retailer's product offers based on a set of rules using data reflecting the customers' view history, purchase history and product reviews.

Also, using data about customer purchase histories, clothing styles and demographics, AI algorithms are being used to optimize supply chain networks.[2]

In the medical technology industry, AI-powered applications are everywhere. For example, mental health is one area that is being treated with medtech.

A recent study found that over 15% of those over 60 suffer from some form of mental disorder, such as dementia or Alzheimer's disease. Additionally, a number of young

people similarly suffer from mental and psychological issues, such as anxiety, depression and stress.[3]

Medtech devices are being used to treat these disorders by, for example, passively collecting data from one's smartphone, analyzing it and alerting one's loved ones if the technology thinks something is amiss.[4]

Trade Secret Laws

While it is generally known that businesses within these industries are using customer data in combination with algorithms to make key discoveries that drive their success, exactly what types of data they collect, the data sets themselves, how they analyze it and what takeaways they have garnered is typically regarded as trade secret.

For example, companies in the food and retail industry typically protect as trade secrets their data sets on customers' sales histories, as well as the takeaways — positive and negative — from analyzing this data.

In the medtech industry, mental health application providers similarly treat core elements of their business as trade secrets — such as the types of data they collect from users' connected devices, the data sets that result from those collections, and takeaways learned from analyzing that data.

This includes key combinations of activity that are generally likely to trigger a depressive episode, how triggers for stress differ based on socioeconomic factors, etc.

Thus, as our economy becomes more and more data-driven, it is also becoming more dependent on trade secrets. There are a number of issues with such a trade secret dependent economy.

For example, heavy reliance on trade secrets could shield important discoveries from the public. Take, for example, the discovery of specific combinations of activity that trigger depressive episodes in people.

While a fundamental goal of the patent system is to encourage the dissemination of discoveries and innovations in exchange for the right to exclude, there is no similar encouragement of discovery-sharing under trade secret law. Instead, companies' commercial success could hinge on keeping important discoveries secret.

And relatedly, if discoveries are being kept secret, then innovation will also be hindered. Instead of members of the public working to address or solve discoveries, the scope of innovators addressing discoveries will be limited to those in the know on the trade secret.

Among the problems that the trade secret dependent economy will face, one that the legal world continually seems to be overlooking is the conflict between trade secret law — which focuses on keeping data and its related discoveries confidential — and data privacy law, which focuses on disclosing the data companies are collecting and how they are using it.

The Conflict with Data Privacy Laws

Privacy law in the U.S. is a patchwork system with a lot of patches.

There is no federal general privacy law. However, there are an increasing number of state general privacy laws, as well as an even greater number of industry-specific privacy laws — both state and federal.

While the definition of protected information changes between the multitudes of statutes, all the laws generally lack a carveout for trade secret protected information. Further, arguments could be made that many of today's privacy laws expressly include trade secret protected information.

For example, the Health Insurance Portability and Accountability Act defines health information as "any information, including genetic information, whether oral or recorded in any form," that:

- Is created or received by a health care provider, health plan, public health authority employer, life insurer, school or university, or health care clearinghouse; and
- Relates to past, present, or future physical or mental health data or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual.

That HIPAA's definition of health information extends to "created information" relating to other health data and health care information arguably extends HIPAA coverage to AI-generated data.

Similarly, Illinois' Biometric Information Privacy Act defines biometric information as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."

The definition goes on to exclude information derived from items or procedures excluded under the definition of biometric identifiers — thereby presumably not excluding other derived information.

Washington's recently passed My Health My Data Act is perhaps the most clear of them all.

It defines consumer health data as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."

Further, the definition of "collect" expressly includes derived information — "'collect' means to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner."

The application of these privacy laws to derived and generated data is particularly problematic because of the user rights provided by the laws.

For example, MHMD provides consumers with the right to confirm whether a company is collecting, sharing or selling consumer health data concerning the consumer, and to access such data, including a list of all third parties and affiliates with whom the regulated entity or the small business has shared or sold the consumer health data.

In the context of the earlier-provided examples, all of which could arguably be considered consumer health data due to their relation to food, clothing sizes and mental health data, MHMD could require these entities to provide a requesting consumer with:

- Access to the collected trade secret protected data;
- Access to the trade secret protected takeaways generated by algorithms processing the trade secret protected data; and
- A list of all third parties and affiliates with whom the trade secrets have been shared or sold.

The disclosure of such information could equate to giving away a business's crown jewels. Another potentially catastrophic consumer request is the right to deletion.

MHMD provides that consumers may request that entities delete their consumer health data, including notifying third parties and others with whom information has been shared of the deletion request.

Again, how are entities to square the deletion requests provided by privacy law with their business interests, as acknowledged by trade secret law?

Possible Solutions

It is of critical importance that privacy statutes start acknowledging the conflict with trade secret law and clarifying how entities should resolve the conflict. For example, one solution could be eliminating derived or generated data from consumer access requests.

Why should end users have the benefit of seeing companies' work product, as opposed to just seeing the exact data that was collected? Deletion requests could also be limited to raw data — once a business has processed and made use of that data, it should not have to undo the fruits of it labor just because a consumer changed its mind.

While providing an exception for trade secret information would be the obvious step to solving the conflict, a downside of this would be that entities may feel drawn to over-claim trade secret protection to avoid privacy law compliance.

Moreover, a complete trade secret exception would give short shrift to the goals of data privacy law. Consumers should have rights to control data about them — but there must be limits.

Another possible solution that companies could implement themselves, without changes to any existing statutes, is having consumers sign nondisclosure agreements before disclosing trade secret protected information.

Of course, if a user refuses to sign an NDA then a company is a new conundrum: Should it reveal the information anyway, or refuse to reveal the requested information, possibly running afoul of data privacy laws?

Another consideration is businesses' identification of what constitutes trade secrets.

Traditionally there has been some reluctance from companies to prepare written documentation listing what their trade secrets are because, while the documentation may prove useful in a trade secret misappropriation case if the trade secret is among those listed, such a list could prove near-fatal if the trade secrets being litigated are not among those listed.

With the passage of an increasing number of data privacy laws, there is now a new reason for entities to create these lists: so that the data privacy team knows what the IP team regards as a trade secret.

This is a classic case of "the left-hand needs to know what the right hand is doing." An IP department certainly does not want to engage in the time and effort of protecting trade secrets only to find out that the data privacy department is revealing those trade secrets without hesitation to end-users in response to consumer requests.

It is important that the IP department and the data privacy department coordinate efforts to ensure that trade secret protected information is being regarded as confidential by all, and to the extent information has to be disclosed in response to consumer requests it is done so in as safe of a way as possible, in a manner determined by the company to be most-aligned with the corporate goals.

In some instances, this balance may tip slightly in favor of not fully disclosing information to consumers in the interest of trade secret protection, and in other instances this balance may tip the other way.

Ultimately, until the laws become clearer — and the conflict is resolved — businesses will need in some instances to just decide which legal regime reigns superior, and which set of risks they are willing to take.

1. *https://foodindustryexecutive.com/2022/07/the-impact-of-ai-and-big-data-within-the-food-industry/*.
2. *https://www.bloomreach.com/en/blog/2021/impact-artificial-intelligence-online-fashion-retail*.
3. *https://www.news-medical.net/health/What-are-the-Applications-of-Technology-Based-Mental-Health-Interventions.aspx*.
4. "Hudson, Florence D. Women Securing the Future with TIPPSS for Connected Healthcare, Chapter 7 (Colgate, Jenny and Jennifer Maisel, "The Right Not to Share: Weighing Personal Privacy Threat vs. Promises of Connected Health Devices").