Tara Norgard

Harpreet Mahal

The Intersection of Trade Secrets and Data Privacy in the Digital Age

The digital age has been turbo-boosted by remote work in the wake of Covid-19, accelerating the availability, mobility, and value of information in every type of business. It is no longer a question of whether your business has valuable information to protect. The question is how to maximize and preserve the value of that information in conjunction with various emerging—and sometimes unexpected—legal considerations. In this article, we discuss the intersection of trade secret and data privacy laws in the digital age.

Trade Secrets

Trade secrets are a vital part of a business's intellectual property portfolio. Until 2016, trade secrets were primarily creatures of state law. All states except for New York, which relies on common law, and North Carolina, which has its own statute, have adopted some form of the Uniform Trade Secrets Act ("UTSA"). In 2016, Congress enacted the Defend Trade Secrets Act ("DTSA"), which for the first time provided a federal civil statute protecting trade secret rights. The DTSA co-exists and is closely aligned with the UTSA, but has a handful of unique provisions, such as an ability to obtain an *ex parte* seizure order in certain circumstances and a grant of legal immunity to corporate whistleblowers. The DTSA extended the Economic Espionage Act of 1996, which criminalizes certain trade secret misappropriations.

Both the UTSA and the DTSA generally define trade secrets as (1) information, that (2) has independent economic value (3) resulting from not being generally known, where (4) the owner of the information makes reasonable efforts or measures to maintain the secrecy of that information. Trade secrets can take a variety of forms. Iconic examples include the formulation of Coca-Cola and the algorithm behind the *New York Times* bestseller lists. But the vast majority of trade secrets are the bread and butter of everyday business, such as manufacturing details, customer lists, and methods of combining and processing data. Whether iconic or not, a business's efforts to understand and protect the value of its trade secrets can prove to be a valuable investment of legal resources.

Data Privacy

Many companies had a crash course in data privacy with the General Data Protection Regulation ("GDPR"), which went into effect in the European Union ("EU") in May 2018. The goal of the GDPR is to enhance individuals' control and rights over their personal data and simplify the regulatory environment for international business. The GDPR protects nine fundamental rights of "data subjects," *i.e.*, people whose data is collected: (1) the right to be informed about the collection and use of personal data (GDPR Articles 12-14), (2) the right to access copies of personal data (GDPR Article 15), (3) the right to rectification of inaccurate or outdated personal information (GDPR Article 16), (4) the right to be forgotten

and have personal information deleted (GDPR Article 17), (5) the right to data portability, or transfer, of personal data to another controller or to the data subjects themselves (GDPR Article 20), (6) the right to restrict or suppress processing of personal data (GDPR Article 18), (7) the right to object to processing of personal data (GDPR Article 21), (8) the right to object to automatic processing of personal data (GDPR Article 22), and (9) the right to withdraw previously given consent to process personal data (GDPR Article 7).

GDPR recitals, much like contract recitals, provide context for its binding articles. Recital 63 addresses the intersection of trade secret rights and the rights of the data subject, and sets forth a balancing approach. Specifically, Recital 63 states:

> That right [of access] should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject.

Council Regulation 2016/679, On the Protection of Natural Persons with Regard to the Processing of Personal Data and the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1, 12.

In the United States, an evolving patchwork of federal and state laws and regulations governs data privacy. Some examples of sector or target-specific laws include the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act, and the Video Privacy Protection Act, along with their amendments and associated administrative rules. On a state level, many states have introduced comprehensive state privacy bills, though only California (January 2020), Virginia (January 2023), Colorado (July 2023), Connecticut (July 2023), and Utah (December 2023) have passed legislation. The Minnesota Consumer Data Privacy Act has been in the Commerce Finance and Policy Committee for over a year but does not appear poised for enactment in the near-term.

California, with its second-generation data privacy law, California Privacy Rights Act ("CPRA" or "Proposition 24"), coming into effect in January 2023, may foreshadow the way other states will handle the right to data access and protection of trade secrets as these laws continue to emerge. California's current data privacy law does not mention trade secrets. However, the Office of the Attorney General ("OAG") was tasked with "[e]stablishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights . . . with the intention that trade secrets should not be disclosed in response to a verifiable consumer request." Cal. Civ. Code §1798.185(a)(3). During the public comment period, the OAG rejected an outright carveout for trade secrets, but echoed a GDPR-like balancing test, noting that "the interests in favor of protecting trade secrets must be weighed against the need for disclosure." OAG CCPA Final Statement of Reasons, Appendix A, Response #323. Under the CPRA, rulemaking authority is given to a new administrative agency, the California Privacy Protection Agency. The agency completed its public comments period in late 2021 and is now holding informational hearings before commencing formal rulemaking.

Trade Secret and Data Privacy Considerations in Litigation

In the United States, the intersection of trade secret and data protection laws is an emerging—and critical—area to consider, both in litigation and investigations.

For example, in *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp LLC*, an employer suspected former employees of trade secret misappropriation in opening a competing military-style gym. 587 F. Supp. 2d 548 (S.D.N.Y. 2008). The former employee had sent emails detailing actions supporting misappropriation claims and the employer sued for trade secret misappropriation. Instead of filing a case and accessing information through discovery, the employer obtained access to emails in the former employee's personal email accounts and new work account using saved password information on the former employee's company device. The former employee countersued for violations of the Stored Communications Act ("SCA"). The Court ultimately disallowed the use of that evidence for any uses other than impeachment. *Id.* at 571.

A different set of facts—and outcome—was presented in *Sunbelt Rentals, Inc. v. Victor*, where a former employee had linked a personal Apple account with an employer-owned iPhone and iPad. 43 F. Supp. 3d 1026 (N.D. Cal. 2014). The employee returned the devices to his former employer without unlinking them and proceeded to link a new iPhone from his new employer to that same personal Apple account. As a result, the employee's communications with his new employer were delivered to the former employer's devices. When sued for trade secret misappropriation, the former employee alleged violation of the SCA. The Court found that the passive nature of receiving those messages did not violate the SCA and the evidence was allowed to be used in the case. *Id.* at 1032.

Trade secret protection can also be implicated when investigating data breaches. When data breaches occur, companies oftentimes hire forensics services, either directly or through a law firm, to produce forensic reports on the data breach and help inform the path forward. These reports can contain, and if disclosed, have the potential to reveal information related to a company's trade secrets.

For example, a 2013 cyberattack on Target led to the data breach of customer credit card information. In litigation that followed, there was a dispute over the production of documents created by the Data Breach Task Force, which was created under the direction of Target's lawyers, to understand risk and allow attorneys to provide legal advice in anticipation of litigation. The court upheld an assertion of privilege in the second track of Target's two-track approach to its data breach investigation: (1) an investigation for ordinary business purposes which has the potential to be produced in litigation and (2) an investigation to help lawyers provide legal advice in anticipation of litigation. *In re Target Corp. Customer Data Sec. Breach Litig.*, 2015 WL 6777384, at *3 (D. Minn. 2015). Many companies have relied on a two-track approach since *In re Target*, with the first track being subject to discovery in litigation, and the second track benefit from attorney-client and work product protections.

It is important to recognize that the two-track investigative approach may not be followed in all cases. One example of this is *Wengui v. Clark Hill*, a case where Guo Wengui, a billionaire property developer accused of corruption in China, sued Clark Hill, the firm representing him for his asylum application in the United States, over a data breach that led to the online publication of his confidential information. 338 F.R.D. 7 (D.D.C. 2021). Clark Hill hired a company through external counsel to generate a forensic report and asserted that its cybersecurity vendor had separately worked to investigate the attack and remediate for business purposes. In evaluating whether to grant a motion to compel production of documents, including the forensic report, the court noted that the legal advice track report included recommendations for technical security remediation, and that the report had been shared with firm leadership and IT (not just the attorneys), and found that neither work product doctrine nor attorney-client privilege applied to the report. *Id.* at 14.

These cases show that although it is still prudent to segregate the investigation of a data breach for purposes of business versus legal considerations, leaving trade secret information out of all forensic reports, if possible, may be wise.

Lessons from the EU

Several cases in the EU have applied the balancing approach set forth in the GDPR, providing potential insight as to how courts in the United States might balance data privacy and trade secret rights under emerging US law.

In an administrative action in Austria, a data subject sought access to how marketing scores determining the likelihood that a subject belonged to a demographic group, such as conservative, traditionalist, hedonist, and digital individualist were calculated. The company refused on trade secret grounds. DSB Austria 2020-0.436.002 DSB-D124.909. The data protection authority in Austria, Österreichische Datenschutzbehörde (DBS), applied a balancing approach, ruling that the company did not have to disclose the algorithm or source code, but did have to disclose which input variables were used and why, the effect of the variable on outcome, the list of possible outcomes, and an explanation of the result.

A similar result came out of Denmark in 2019, where a pension company refused disclosure of a consultant's health assessment of a data subject based on a claim that the information was a trade secret. Datatilsynet 2019-31-1424. The Danish data protection authority, Datatilsynet, recognized the interest of protecting internal decision making and articulated a standard requiring "imminent risk of harm" to the trade secret in question. The matter ultimately was resolved with the company's inability to establish that the information in question was a trade secret.

In Amsterdam, a Dutch court examined the risk to trade secrets when, in response to a data subject's request and alleged violations of the GDPR, Uber refused to disclose information about an automated process to detect fraud and terminated driver accounts. Rb. Amsterdam C/13/692003/HA RK 20-302. The company argued that providing the information would risk divulging trade secrets about its anti-fraud process. The court found that the ride share company was not required to provide the extensive disclosures required for automated decision-making, however it did order the company to provide data subjects access to the personal data used for the decision to deactivate the data subject's account in a way that would allow verification of the correctness and lawfulness of the data processing.

Conclusion

The juxtaposition of trade secrets, data privacy and data security considerations create both opportunities and risks for businesses. A recognition and understanding of this intersection will serve businesses well as data, and the laws that govern its value and protection, continue to emerge in the information age.

About the Authors

Tara Norgard focuses on intellectual property and high-stakes business litigation and counseling. She has secured victories in district and appellate courts and arbitrations across the country, and negotiated multimillion-dollar, client-favorable settlements in matters involving a wide spectrum of technologies, including medical devices, financial systems, radiation therapy systems, dental treatments, glass coatings, and consumer goods. Tara is a powerful advocate for each client she serves with a keen strategic view and relentless attention to details that matter.

tnorgard@carlsoncaspers.com | 612.436.9620

Harpreet Mahal practices intellectual property law concentrating on litigation, patents, trade secrets, data compliance, trademarks, and licensing for pharmaceutical and biomedical companies. He develops proactive legal strategies by understanding the client's business needs, risks, and goals, drawing from his experiences both in the research laboratory and the clinical setting. Leveraging his medical and legal training and experience, he is a powerful ally and a strong advocate for sophisticated clients in competitive markets.

hmahal@carlsoncaspers.com | 612.436.9663