All Analytics

ELECTRONICALLY REPRINTED FROM JULY 10, 2017

Data Agreements for Analytics Organizations: What You Need to Know

By Gary A. Kibel & Michael C. Lasky

Data is omnipresent. It is created constantly, during every interaction and on every device. It is used by every type of company, regardless of its size, business model, or industry sector. It also informs nearly every type of business decision, from supplying inventory and pricing goods to placing advertising, predicting trends, and interacting with customers.

As data has grown in importance, new industries have been created to support its use in today's information economy, and new products and services are flourishing. Amongst the most important and fastest growing of these industry sectors are data analytics. Originally limited to companies that provided research and reports, data analytics companies now take many different forms. Indeed, the diversification of the data analytics business has led to an explosion in profits, with industry-wide revenue expected to reach $210 billion by 2020, according to market research firm IDC. Along with the traditional market research companies, data analytics businesses now include a broad array of businesses from companies that create their own data segments for resale, to companies that clean and process data, to companies that provide matching and database services.

Perhaps unsurprisingly, the varied form of data analytics firms creates a complex set of legal and regulatory requirements. In fact, data analytics firms frequently find themselves between a proverbial rock and a hard place. On one hand, data analytics firms routinely take in data from third parties, and thus must worry about data collection and consumer protection laws. On the other hand, data analytics companies routinely provide data and analysis to third parties, and in doing so, they must be careful to protect their intellectual property and the security of their data. Increasingly, data analytics companies are coping with these complexities by entering into data agreements to set parameters around data usage and ensure legal compliance. But how should data analytics firms utilize these agreements? What rights and protections should they require? In this article, we offer advice for avoiding common pitfalls in data agreements to better protect and grow your businesses.

Understanding The Deal

The most common pitfall in any data agreement is the failure of both business and legal personnel to understand the deal. Given the immense variation and complexity of data agreements, it is therefore critical to at least ask the following questions. The answers will inform the structure of any eventual contract.

- **What data is involved?** Different levels of data require different types of controls. Specifically, if a data analytics firm is providing, receiving or processing personally identifiable information about individuals, be aware that certain regulatory requirements may apply. If the firm is dealing with sensitive personal information such as health records, credit reports or bank records, additional legal requirements come into play. Understanding the substance of the data involved will allow a firm to craft the appropriate rights, obligations and restrictions in its contracts.
- **With whom is the data being shared?** An important -- and often overlooked -- element of data agreements is the practical component regarding with whom the information will be shared. How is data being transferred and presented? Is one party providing a platform or an API? Is data being stored in the cloud? It is important for a firm to structure its data agreement around the information

technology requirements of any data use or transfer.

- **Are the parties performing any operations on the data?** It is also important to understand the flow of any data that will be the subject of the agreement. Is the data analytics firm simply routing data? Or is it manipulating the data, g., by anonymizing or aggregating it, or combining it with other information? What analytics does the firm plan to perform? Where is the data likely to end up? What are the project deliverables? Resolving these issues are critical to delineating each party's rights and protecting your intellectual property.
- **What are the authorized and prohibited uses?** Before entering into a data agreement, it is important to consider the permitted and excluded uses of that data. What types of data and access does the business relationship require? Do you want to make sure your clients do not receive certain types of information? Are certain third parties not allowed access to data? Are certain uses of the data impermissible? Remember to only provide those rights necessary for your specific business arrangement.

Key Provisions in Data Agreements

Ensuring Rights to Data

In recent years, there has been a spate of lawsuits alleging the improper and deceptive collection of information from consumers. For example, in several ongoing lawsuits that were filed within the last year, a number of "smart television" manufacturers and downstream data analytics companies have been named in putative class actions that allege that the manufacturers failed to disclose their collection of television viewing data for purchasers of their smart televisions and their sale of this data to third parties. Some of these lawsuits -- like many class actions -- have also gained the attention of the Federal Trade Commission and state attorneys general.

In order to avoid this sort of legal exposure -- which can potentially total in the millions of dollars, as well as significant legal fees -- every data agreement should probe into how the data was collected. For example, the Federal Trade Commission requires that consumer data collection practices not be unfair or deceptive, e.g., that data collection practices on websites be disclosed on that website's terms of use and privacy policies. Similarly, certain types of data collection, e.g., collection of financial information in states such as California, require either the opt-in of the consumer, or the option to opt-out. In addition, the Digital Advertising Alliance and the Network Advertising Initiative have self-regulatory codes. These codes govern the use of data in online behavioral advertising. In any contract with a data provider, a data analytics firm should require a representation that all data was collected in compliance with the providing party's and any relevant third parties' terms of use and privacy policies as well as any self-regulatory codes of conduct. Data analytics firms, if providing data to its clients, should perform the investigation referenced above so that they can make the same representation on their own behalf to downstream clients.

Ownership and Access

Data, like any other asset, is a form of property. Thus, there are sometimes intellectual property rights inherent in data and in the operations and analytics performed by data analytics companies. In addition, data and data operations should generally be protected as confidential information or as a trade secrets and should not be provided to third parties without a non-disclosure agreements or firm confidentiality provisions in client and vendor contracts.

Further, as data grows in importance, companies are increasingly considering whether to apply for intellectual property protection in data and data processes, and enforce those rights against others. For example, non-practicing entities or "patent trolls" routinely collect broad data-based patents for assertion against entities in the data ecosystem. In one notorious case, a company named E-data acquired a broad patent to cover an "information manufacturing machine" and sued a number of companies in the data collection and protection ecosystem. In order to protect against these types of suits, it is important for data analytics firms to ask vendors to warrant that the materials they are providing do not infringe the third party intellectual property rights. However, in their own client contracts, data firms should avoid making representations about intellectual property infringement unless they have actually performed the requisite due diligence.

In addition, data firms should consider whether ownership or other rights in intellectual property should be provided to others. With vendors, data analytics firms should consider whether the work being paid for should belong to them. If so, there should be provisions in the agreement providing that it is a "work made for hire," or otherwise requiring its assignment to the company. Data analytics firms need to be clear with their clients concerning what work product or deliverables are the property of the client, and which are simply being licensed to the client for the purposes of this one transaction. The scope of any license is critical; study the exact types of data and the data flow, as well as any excluded uses before shaping the license.

Complying with Privacy Laws

In the United States, there is no one comprehensive federal law regulating the collection and use of data. Instead, there are a patchwork of federal and state laws concerning privacy, data security and consumer protection that may be relevant. Although a comprehensive survey of privacy laws is beyond the scope of this article, some of the most prominent federal laws concerning data are the Federal Trade Commission Act (unfair and deceptive data collection and use); the Gramm-Leach-Blilely Act (financial information); the Fair Credit Reporting Act (lending and credit information); the Health Insurance Portability and Accountability Act (medical and healthcare information); the Computer Fraud and Abuse Act and the Electronic Communica-

tions Privacy Act (interception of electronic communications); and the CAN-SPAM Act (email).

Given the range of possible privacy laws that may apply, it is important that all agreements contain a provision requiring compliance with applicable law. In vendor agreements, this means that the vendor should represent that all information was collected and used in compliance with applicable law, and that the data analytics companies' use as contemplated in the agreement will not violate applicable law. In client agreements, this means that the any data or deliverables cannot be used except permitted by applicable law. In addition, data analytics firms dealing with sensitive, financial, health, or other information should consider including specific representations required by subject-matter specific laws.

Data Security and Information Technology

Nearly all states have comprehensive data breach laws that require notification to data subjects in the event of unauthorized access to certain personally identifiable information. Moreover, data breaches suffered by major companies such as Target, JP Morgan Chase, and Sony have drawn the ire of the public and the attention of regulators. For this reason, data analytics firms should be concerned with data security. This is particularly true if data analytics companies use the cloud; though cloud computing offers nearly unlimited, cost-effective, and easy-to-access storage, it faces the threat of increased security issues, and we have found it to be particularly prone to attacks.

In their vendor agreements, data analytics companies should make sure that the vendor represents that it has complied with all data security laws and that its products and data do not contain any malicious code. Vendors should also represent that they implement industry-standard security measures to protect the integrity of any data. The vendor should also be required to not only immediately notify the data analytics firm of a breach but also take all necessary remediation and notification obligations at its own cost. In client contracts, these same representations are likely to be imposed upon data analytics companies, but it is important to narrow their scope. For example, data analytics companies should only take any remediation and notification obligations to the extent required by law.

Finally, if sensitive personal information is involved, it may be worth including a data security exhibit to the contract with additional protections. In that document, there may be further requirements concerning data encryption, security testing, and data breach remediation efforts. In addition, a data security exhibit may also include the requirement that the vendor have a written information security, backup, and disaster redundancy policy and further require security audits. In vendor agreements, it is important for data analytics firms to push for as many of these requirements as possible. However, data analytics firms should be sure to do research into their own security procedures as well before committing to security obligations in their client agreements.

Conclusion

As the data analytics sector continues to grow, data agreements have grown increasingly complex and varied. Such agreements need to be customized to the particular data and facts of a transaction. Whether working with a vendor or a client, it is therefore important to carefully understand the deal parameters and include relevant legal protections in the data agreement.

Authors Kibel and Lasky can be reached at gkibel@dglaw.com and mlasky@dglaw.com. Their colleagues, Marc Rachman (mrachman@dglaw.com) and Devin Kothari (dkothari@dglaw.com) assisted in the preparation of this article.

Gary A. Kibel is a partner in the Digital Media & Privacy department & Michael C. Lasky is a partner and co-chair of the litigation department at Davis & Gilbert LLP

Gary A. Kibel is a partner in the Digital Media, Technology & Privacy Practice Group of Davis & Gilbert. Mr. Kibel is a Certified Information Privacy Professional (CIPP) and advises clients in many industries regarding privacy and data security issues. He represents many clients in the ad tech and market research industries. He may be reached at 212.468.4918 or gkibel@dglaw.com.

Michael C. Lasky is a partner and co-chair of the litigation department at Davis & Gilbert LLP. He has many years of complex commercial and business law experience and has litigated a broad range of cases, He may be reached at 212.468.4849 or mlasky@dglaw.com