CORPORATE

IT'S A DATA-DRIVEN WORLD. PROTECT YOURSELF.

The world is awash in data, and the tide will only keep rising. Regardless of how data originates—financial transactions, social media, smartphones, the Internet of Things, industrial-strength analytics, and much more—organizations must understand how it affects them and have sound legal strategies in place to minimize potential liabilities.

Quantifying the sheer amount of data helps put this in perspective. Market intelligence firm IDC forecasts that the global volume of data will rise 900 percent, from 4.4 zettabytes in 2013 to 44 ZB—the equivalent of 4 trillion gigabytes—in 2020. In visual terms, 4.4 ZB would stretch two-thirds of the distance from the earth to the moon, and 44 ZB would equal 6.6 times that.

"The explosion of data, combined with technological breakthroughs in how to analyze it on a huge scale and put it to commercial use, means that data has become a new form of currency among businesses," says Bryan Brewer, a Crowell & Moring partner and chair of the firm's Corporate Group. "Like any currency, it poses risks that have to be managed. Companies that are attuned to data risks will anticipate possible scenarios and find new ways to protect themselves."

U.S. DATA REGULATION: A PATCHWORK WITH HOLES

Regulatory oversight of data in the United States is diffuse, varying according to the type of data being regulated. There is no single governing regime.

The most prominent federal laws are the Health Insurance Portability and Accountability Act (for medical data and better known as HIPAA); the Financial Services Modernization Act of 1999 (for financial data and better known as the Gramm-Leach-Bliley Act); various consumer data protection statutes overseen by the Federal Trade Commission; and the Electronic Privacy Communications Act, which restricts surveillance of data transmission and access to stored data. The California Online Privacy Protection Act is generally considered the top state-level statute.

The patchwork nature of the regulatory environment is exacerbated by the fact that the law is constantly having to catch up to both advances in technology and newly emerging privacy concerns. According to Brewer, this means that data issues often are legal topics of first impression—which makes their resolution more challenging for in-house law departments and their outside counsel.

Companies doing business on the world stage must also be cognizant of non-U.S. laws. The most prominent—and furthest-reaching—such law governing data and privacy is the European Union's General Data Protection Regulation (better known as GDPR), which went into effect in May 2018.

DATA GOES TO MARKET

For many companies, data has become a core driver of their go-to-market strategy. Perhaps the biggest battleground for corporate data issues is the universe of commercial agreements between companies. These cover everything from mergers, acquisitions, and dispositions to licensing deals, vendor/supplier and service contracts, marketing arrangements, and more.

Regardless of whether regulators compel them, best practices and general risk mitigation require that companies address many important questions in negotiating agreements. Notably:

- How can we use data to create new products?
- What are the known and potential risks involved?
- Where should we draw the lines around data ownership?
- What are appropriate restrictions around data mining?
- What should we do with the results of our analyses?
- How should our data be stored? By whom?

"Like any currency, [data] poses risks that have to be managed. Companies that are attuned to data risks will anticipate possible scenarios and find new ways to protect themselves."

—*Bryan Brewer*

"The losses that can result from data breaches or mishandling may be suffered by a variety of affected parties beyond a company and its service provider, which means more potential claims of liability."

—*Jeffrey Selman*

- What are the risks associated with advanced technologies such as artificial intelligence and machine learning, and how can we mitigate them?

So critical are such questions, Brewer notes, that "the smartest and most innovative minds are grappling with them, and the answers they come up with could directly affect a company's competitiveness and long-term viability."

RISK ALLOCATION IS CRITICAL

Which brings us to the toughest question of them all: how to properly allocate data-related risk—particularly through hacks and other data breaches—among parties to an agreement. "We're asked about this every day," says Jeffrey Selman, a partner in Crowell & Moring's Corporate Group. "It's top of mind for companies across industries and geographies."

The most common clauses for allocating data risk are indemnification and limitation of liabilities. Given the stakes involved, they contain among the most fiercely negotiated language in commercial agreements these days.

An additional source of pressure on risk allocation clauses is that in most states, legal liability for data breaches attaches to the owner of the data and not a service provider whose actions cause the breach. Typically, the service provider is obligated only to notify the data owner that a breach occurred.

Clearly, parties that don't fully address the risks related to data and that fail to limit their own potential liability do so at their peril. Selman adds, "The losses that can result from data breaches or mishandling may be suffered by a variety of affected parties beyond a company and its service provider, which means more potential claims of liability. All sides to an agreement need to protect themselves upfront as much as possible."

WHAT TO LOOK FOR

Brewer expects the debate to coalesce around two key issues:

Commercialization of data. Data has become so plentiful, finely categorized, and malleable—and the technology for organizing and analyzing it so powerful and efficient—that companies will seek to commercialize data by using it to create new products. This raises a host of questions that must be resolved, notably, Do companies have the legal authority to commercialize their data? The answer isn't as obvious as one might think.

Regulation of data as currency. As data gains de facto currency status in the business world, regulation must evolve to recognize this status and govern data's use accordingly.

As for new regulatory action, the legislative pipeline doesn't include proposals for updating data oversight. Brewer is hopeful, however, that rising corporate demand for greater clarity could compel agencies to issue guidance documents. The agencies most likely to do so, he says, are the Department of Health and Human Services, which is responsible for HIPAA compliance and enforcement; the FTC, in its roles as consumer watchdog and M&A gatekeeper; and the SEC, which could set new rules on data-related disclosures for publicly traded companies.

Meanwhile, because data is one area where regulation will continue to lag innovation, companies should do their part to stay ahead of the regulators by thinking about and addressing risk in their agreements.

DATA AND M&A: A LOT TO THINK ABOUT

Data and privacy issues are becoming crucial points to be addressed in mergers and acquisitions, especially when deals cross multiple jurisdictions.

Says Crowell & Moring's Jeffrey Selman, "Both sides should understand that multijurisdictional transactions create additional data and privacy considerations that must be negotiated. This is true even if the parties aren't located in the jurisdictions involved. They need to know the relevant regulations, anticipate concerns that regulators could raise, and position themselves to be compliant."

The point about location is due to the long legal reach of two laws in particular: the EU's General Data Protection Regulation (GDPR) and the California Online Privacy Protection Act (CalOPPA). Both apply to entities that do business in the EU and California, respectively, regardless of where the entities are actually located. Global politics also plays a key role in cross-border combinations between data-heavy technology companies.

Both Selman and Crowell & Moring's Bryan Brewer recommend that deal legal teams expand to include specialists in privacy and cybersecurity. For multinational transactions, teams should include experts in GDPR, UK law, and CalOPPA, as well.