/Autonomous
/Sensing
/Communication
/Battery
/Navigation
/Mirrorless
/Ecology
100m
48
mph

CHOMBOSAN/GETTY IMAGES

COVER STORY

DATA, DATA EVERYWHERE

POSITIONING YOUR COMPANY TO SURVIVE AND THRIVE IN THE DATA REVOLUTION

If you've spent much time driving in San Francisco, Detroit, or Pittsburgh, you may well have shared the road with an autonomous vehicle guiding itself down the highway. The same is true in a variety of other locations, as dozens of companies conduct trials of their self-driving cars and trucks.

While the development of fully autonomous vehicles has a ways to go, the technology is moving fast. Many predict this is just the beginning of the biggest change in transportation in 100 years—all made possible by the pervasive and expanding use of digital technology, which is used for everything from tracking the movements of triathletes to powering robots working in dangerous environments.

The range of possibilities seems endless. Artificial intelligence can help factory machines "learn" to perform better over time. Analytics can be used to predict everything from customer needs to when industrial equipment will require maintenance. Bots can be used to handle basic compliance questions. Networks of sensors connected through the Internet of Things (IoT) can enable automation, agility, and safety in production plants. And the list goes on.

These varied developments rely on one common foundation—data. Today, data is not just financial transactions and customer lists. It also includes information coming from smartphones, cars, cameras, and a wealth of connected sensors embedded in homes, businesses, equipment, and devices. This flood of data is powering innovation in new ways and making data more of a business asset than ever. As *The Economist* recently noted, "Data are to this century what oil was to the last one: a driver of growth and change." Even traditional brick-and-mortar businesses are increasingly data-driven.

But as data becomes more valuable, companies also face more, and sometimes new, legal risks. "Businesses know how important data is to innovation, but you also have to think about the unprecedented implications it poses for things like regulatory enforcement, product liability, cybersecurity, and IP," says Cheryl Falvey, a partner at Crowell & Moring, co-chair of the firm's Advertising & Product Risk Management Group, and former general counsel of the Consumer Product Safety Commission. If those kinds of factors are not addressed, she says, “data can become less of an asset and more of a liability.”

IOT FOR THE LEGAL DEPARTMENT

The opportunities and challenges presented by today’s growing flood of data can be seen in a wide range of products and systems, from the emergence of blockchain technology to digital health—and especially today’s high-profile autonomous vehicle initiatives. Experts say that a typical autonomous vehicle will generate about 4,000 gigabytes of data per day—roughly the same daily amount generated by 3,000 people using their computers. Companies expect this data about the car, the road, and the passengers will open the door to new revenue-generating offerings and business models.

However, significant legal questions surround these developments. “Autonomous vehicles are going to be a game-changer for our economy and entire transportation system, but companies will first have to navigate real regulatory issues like physical safety, cybersecurity, and privacy,” says Paul Rosen, the former chief of staff at the Department of Homeland Security who is now a Crowell & Moring partner. “What happens to the consumer data these connected cars collect and transmit? How detailed is that information? Where and how is it stored? And who is legally at fault if a self-driving car crashes?” Such questions are being sorted out, and, Rosen says, “litigation and the courts will likely weigh in on the answers to many of them.”

One challenge is managing the sheer volume of data that companies hold. “Today, e-discovery in a case is going to seek not just traditional things like email,” says Falvey. “It’s going to ask for information such as location data from phones, activity data from wearable technologies, and operational and testing data from drones and autonomous vehicles.”

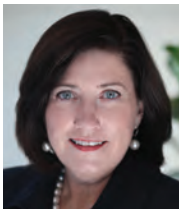
The challenges go far beyond data volume, however. Today, general counsel need to develop a deeper understanding of the data the company owns. “Do you know what the data could be telling you about the performance of the company’s medical device, for example, or the electrical grid or factory operations?” asks Falvey. “If there is an issue that ends up causing harm to someone, the question will be what did the data show in advance and were reasonable steps taken to understand that data and address any potential risks it revealed?”

That question is key, Falvey continues, “because at a high level, the laws concerning corporate liability come down to whether your actions were reasonable. Did you know or should you have known about the issue?” With the wealth of data that is now under corporate control, the answer to that question is likely to be yes. As Big Data tools become more powerful and more mainstream, courts increasingly may find that companies should have such insight into potential safety and security issues with new products and new technologies. “When it comes to data collection, the lawyer for the business should probe what data is available and what it means in order to mitigate the legal risks of having data and not acting on it,” she says.

WHAT YOU SHOULD HAVE KNOWN

Government agencies also have an evolving perspective about what companies “should know” from their data. “There is a growing expectation that companies are going to be using Big Data to monitor and protect their supply chains,” says Cari Stinebower, a Crowell & Moring partner and former counsel for the U.S. Department of the Treasury’s Office of Foreign Assets Control. Increasingly, she explains, agencies believe that a corporation should be able to track its goods from the extraction of natural resources at the mine through production to finished product—including the activities of suppliers and subcontractors. “So if your product is a piece of electronic equipment containing gold mined in Zimbabwe or cobalt coming from the Congo, they think that you should know about it,” she says.

Regulators today expect companies to have the same kind of data-driven insight into their customers, as well. For example, a company could be held responsible for selling items to individuals and other companies on a blacklist under a Bush-era counterterrorism executive order or the 2008 Foreign Narcotics Kingpin Designation Act. “Increasingly, enforcement agencies expect companies to screen not only their customers but their ‘ship-to’ information, as well.



“Businesses know how important data is to innovation, but you also have to think about the unprecedented implications it poses ...” *—Cheryl Falvey*

"Companies will first have to navigate real regulatory issues like physical safety, cybersecurity, and privacy." *—Paul Rosen*

In the retail space, that's an incredible volume of data," says Stinebower.

Here again, the ability to collect and analyze large amounts of data is something of a double-edged sword. It can open the door to increased collaboration across the supply chain for faster innovation and increased efficiency. But, says Stinebower, "along with that also comes the liability of having to track that data to manage the risk of litigation."

MORE RISK ON MORE FRONTS

Because data is used throughout the business, companies need to monitor litigation risk across a growing range of activities—and problems can now arise in unexpected areas. In some instances, data-related issues can expand into criminal investigations from regulators. For example, if a company analysis shows that someone in the supply chain is diverting products from one jurisdiction to another, that could indicate a corruption issue involving financial transactions and payoffs to government officials or others to move goods across borders. "That can get the attention of regulators," says Stinebower. "And if there is a tie to the U.K., it may fall under the U.K. Bribery Act, which prohibits private bribery as well as bribes to government officials."

Data is likely to play a growing role in the antitrust world, as well. "Some officials have suggested that ownership of large amounts of data could be an attribute of market power, like a dominant manufacturer owning more production capacity than anyone else," says Ryan Tisch, a partner in Crowell & Moring's Antitrust Group. "With the growing importance of data in business, we may see cases where the regulators look closely at the data troves being held by companies trying to merge. They might see that one has 70 percent of the available data of a specific type and the other has 20 percent. They could then decide that this would be a merger to monopoly from a data standpoint, based on the idea that the merged company would be able to raise prices when they monetize that data, or use that data to erect barriers to upstart competitors." It is also possible that regulators or private litigants could allege theories of monopolization or attempted monopolization based on companies' efforts to build or maintain supremacy in a given data ecosystem.

Big Data can also be a concern in the IP arena. With the ease of storing and sharing electronic content, lax compliance with key license agreements creates exposure to claims for trademark and copyright infringement. This problem may arise when a company continues to post content after the license period is over, shares it with subsidiaries not covered by the license, or moves it across platforms—for example, taking content licensed only for a company website and using it on a mobile app. "So, without realizing it, a company could be infringing on trademarks and copyrights licensed in a commercial agreement," says Kent Goss, a partner in Crowell & Moring's Litigation Group. He adds that this infringement, even if unintentional, could potentially expose a company to a claim for damages in the six to seven figures, depending on the number of images, videos, or other works involved.

In these situations, whether a company is infringing may depend on where a suit is filed. "There is inconsistency in the Circuit Courts about just what constitutes infringement for online content," says Goss. "Some say that if users view and

"Increasingly, enforcement agencies expect companies to screen not only their customers but their 'ship-to' information, as well." *—Cari Stinebower* click on the unauthorized content, that's infringement. Others say that simply making the content available is enough, regardless of whether users are viewing it—a very low bar for a plaintiff to reach." The Copyright Office has recently adopted the latter view.

WHEN MACHINES MAKE BUSINESS DECISIONS

A more immediate antitrust concern lies in the growing use of analytics and computer algorithms to automate pricing, particularly on e-commerce platforms. These tools can monitor prices and buyer behavior to constantly reset prices to keep up with demand and the competition, without human intervention.

There is nothing wrong with employing such algorithms per se. But the speed and efficiency that some algorithms bring to pricing means that these tools can be misused—or appear to be misused—by parties wanting to fix prices. "One company might have an agreement with another company to use the same algorithm to get to the same price output. Or, competitors might agree on the output they want and build similar algorithms to get to that," says Tisch. "Companies investing in pricing algorithms will need to account for the inevitable efforts of regulators and the plaintiffs' bar to portray them as tools of anticompetitive collusion."

The DOJ is increasingly looking at how competitors use their data to collaborate with one another, particularly with the use of algorithms in pricing strategies. "The DOJ is concerned that consumers are at a disadvantage online, and that algorithms could make it easier for businesses to raise prices," says Tisch. "But companies must use technology to optimize their strategy to reach customers at prices that make sales. It's time to consider practical, realistic compliance measures to make sure pricing algorithms don't raise undue risk."

The use of pricing algorithms is likely to grow. As that happens, companies should recognize that this is an area where appearances can matter. That is, when competitors' prices are following each other closely, it could look like price-fixing to regulators and plaintiffs. Even if it is not, says Tisch, "the sheer unfamiliarity with technology will often drive risk in a way that's unfortunate. People who don't understand it might have doubts about how those prices change—and plaintiffs' lawyers could exploit that."

DATA PROTECTION: STILL KEY

Ensuring the privacy and security of data has been a key challenge for years, and the digital revolution is making it more important and more complicated than ever. Data flows through a universe of connected devices and systems, creating more points of vulnerability. And the stakes of security breaches can be high. "What if the autonomous car is hacked and crashes? What about the impact of hacking into connected homes or medical devices?" asks Falvey.

Today, data is shared widely. It often moves across political boundaries, and in a cloud-enabled world, a company's data might be spread across servers in the U.S. and around the globe, creating significant challenges in terms of litigation, data privacy, and even export controls.

In the U.S., for example, there is no federal data-breach notification law, but many states have them, leaving companies to deal with varying statutes and regulations. European law has been fairly strict in terms of protecting data privacy. "There is a sort of battle of wills between the Europeans, who value data privacy over financial transparency, and the U.S., which wants financial transparency in order to fight things like money laundering and terrorist financing," says Stinebower. As a result, American companies often have trouble accessing their overseas data for U.S. compliance efforts. Nevertheless, she says, "U.S. regulators expect enterprise-wide knowledge from the U.S. component of the business. It kind of sets companies up for conflicting legal obligations."

In 2016, the Second Circuit said that the U.S. government could not compel Microsoft to produce data stored on a server in Ireland. Then, in 2017, the Northern District of California ordered Google to comply with a U.S. warrant requiring it to hand over information related to a specific Google account holder—data that was kept overseas. The Supreme Court may resolve the issue this term.

"These rulings create uncertainty for businesses moving and storing data around the world," says Rosen. This reality, according to Rosen, is driving a growing call for Congress to update the 30-year-old Stored Communications Act that drives many of these cases. The European Union's General Data Protection Regulation will take full effect in May 2018, requiring breach notification and stiff fines for privacy violations.

Overall, says Rosen, varying laws and regulations in the

"Some officials have suggested that ownership of large amounts of data could be an attribute of market power, like a dominant manufacturer owning more production capacity than anyone else." *—Ryan Tisch*

"Without realizing it, a company could be infringing on trademarks and copyrights licensed in a commercial agreement." —Kent Goss

United States and elsewhere are creating "a uniquely challenging environment for companies trying to figure out how to build products and provide services while complying with a patchwork of data security and privacy regulations and laws."

NAVIGATING THE CHANGING LANDSCAPE

To reduce litigation risk in a data-driven world, companies need to continue to focus on the basics—having sound governance and strong compliance programs in place. In addition, GCs need to develop a better understanding of what the company "should know" from its data and, where appropriate, use analytics to proactively identify risks lurking in the data.

With the pervasiveness of data in business, legal departments should also consider a layer of central control over the groups focusing on specific risks. "Compliance specialists have become very specialized," says Stinebower. "There is a need to pull back and have a bird's-eye view of all the different compliance functions so you can cross-check your data privacy program, your fraud program, your anti-corruption program, your export controls, your customer complaints. You need someone in place to coordinate and cross-pollinate that work."

It's also good for legal departments to ensure compliance programs are in step with technological change. "One of the novel qualities of a digital product is that it may not be the same thing two years from now," says Falvey. "If you sell a digital system today, you might upgrade functionality, change how the software works over time, and wake up responsible for a product entirely different than the product designed today. So the GC needs to recognize that the legal risks mapped out at the product launch could be different just a few months later, and the compliance program must allow for that evolution to catch future risks that may be unknown to you at the product launch."

This highlights a key point: with fast-changing technology becoming the foundation of business, corporate law departments operate in a world where "what I do this year won't be good enough next year," says Falvey. "The technology is evolving, cybercriminals are becoming more sophisticated, and the law is creating higher and higher levels of responsibility. You have to keep up with those moving targets."

In the coming year and beyond, adds Rosen, "companies will need to stay nimble and adjust to an evolving legal and regulatory landscape around technology, Big Data, and litigation."

HOW MUCH IS ENOUGH?

The use of Big Data is still fairly new, and just what regulators expect companies to know from their data is still evolving. "Their thought is, if you're collecting it, you should have compliance programs around it," says Crowell & Moring's Cari Stinebower. "Then the question is, how much should you be using Big Data and artificial intelligence to do things like make sure your products are not going to prohibited parties? How far do you need to go?"

With no formal standard in place, it's a good idea for companies to keep an eye on what competitors and peers are doing with these tools in terms of compliance—and monitor what regulators seem to expect from industry.

Meanwhile, the financial services industry has been doing a lot to raise those expectations. Following a flurry of compliance problems and fines a decade or so ago, "institutions have invested heavily in building out their compliance functions," says Stinebower. "Groups of financial institutions have been putting together tests and pilot projects to use Big Data to detect, for example, patterns in human trafficking or problems in the customer due-diligence space." Eventually, she says, "the rest of the world is going to have to follow their lead, because regulators are watching this and saying, 'If the banks can do it, everybody else can do it, as well.'"

At the same time, Stinebower continues, the financial industry has been essentially pushing compliance responsibilities out to their clients. Using the "know your customer's customer concept, they are requiring their customers to maintain robust compliance programs that protect the financial institutions from exposure to money laundering, corruption, or export controls violations. This is just putting more pressure on the average retailer and average manufacturer to use sophisticated compliance tools."