How to make sense of the kinetic past two years? Beyond the distracting headlines, barbed tweets, deregulatory initiatives, and a constant flurry of senior administration departures (and arrivals), there has been a deliberate and undeniable change in the federal government’s approach toward the regulation of businesses. As we note throughout this Forecast, reports of the death of the administrative/regulatory state may well be premature. While the pace of new regulations has slowed (for example, the Federal Register is now half the size it was two years ago), the business community would be wise to treat this trend as a pause, not a full stop.

Technological change, for example, continues to hurtle along, but the American economy needs to develop a regulatory framework that will facilitate that change, not impede it. Decades-old rules of international trade may well be due for reexamination, but they must be replaced with a legal framework in keeping with the times. Finally, with Congress’s continuing gridlock and the administrative state under siege, the judiciary will be called upon increasingly to determine the lines that neither Congress nor the executive branch can cross.

This is fertile ground for the business community to provide leadership in defining the future of regulation—both to monitor technological change and to ensure that the trade winds blow in a direction that benefits all. We hope that this year’s Regulatory Forecast will help our clients both understand and engage in this evolving new world.

—Dan Wolff and Richard Lehfeldt

FOCUS AREAS

12 INTERNATIONAL TRADE
New rules intended to protect American innovation could end up complicating foreign investment and collaboration.

14 REGULATORY
Is it time for the federal judiciary to reassert its role as the final arbiter of what a law means in litigation involving federal agencies?

16 ENERGY
Digital transformation is bringing extraordinary risks and opportunities to incumbent utilities, competitive suppliers, and consumers.

18 GOVERNMENT CONTRACTS
Doing business with the federal government is about to get tougher as requirements for cybersecurity become stricter.

20 CORPORATE
In a data-driven world, organizations need to put in place robust legal strategies to minimize liabilities related to data risk.

22 INTELLECTUAL PROPERTY
Although 3-D printing has the potential to revolutionize medical device manufacturing, liability concerns could stall progress.

24 GOVERNMENT AFFAIRS
Congressional input on rulemaking is increasing as the Trump administration pursues deregulation.

26 HEALTH CARE
The federal government is pushing the health care system to emphasize patient outcomes over patient volumes.

28 INSURANCE/REINSURANCE
Both insurers and regulators want InsurTech to succeed. There is a long road ahead.
Each year, Crowell & Moring’s team of lawyers and consultants examines the regulatory trends most likely to impact businesses for the creation of our annual Forecast. This year, one theme and one word consistently rose to the top: change. From trade agreements to data privacy, from how we regulate to who regulates to who gets regulated, winds of change are blowing through Washington and parts beyond.

Regulators worldwide are making momentous choices about how to confront change, including the transformative shift from analog to digital. As the U.S. navigates a season of deregulation and political stalemate, regulators elsewhere move forward with their agendas. In an increasingly connected world, action or inaction anywhere reverberates everywhere.

Industry faces similar choices: to stalemate or be heard, to fall backward or move forward. As with change generally, corporate decisions in swirling times like these will produce winners and losers.

In this year’s Forecast, we explore how the future of regulation will be influenced by change occurring both outside and inside of Washington. The winds of change will be powerful and come from unexpected directions. For businesses, staying nimble and understanding how best to participate in the discourse will be more important than ever.

We hope this Forecast is a resource to you for the year ahead.

—Scott L. Winkleman
Management Board Member and Regulatory Department Chair, Crowell & Moring
As we begin 2019, the global economy appears to be headed for uncharted waters, and many businesses are plotting a new course to avoid the storm clouds that could lie ahead. The global business climate is being challenged by mistrust and mercantilism. International agreements and organizations that have helped drive prosperity since World War II are fraying. The Trump administration is advancing an “America First” agenda that is causing major companies to rethink everything from their supply chains to where they elect to site headquarters offices and major manufacturing facilities. Other countries are making bold changes to tariffs, privacy laws, and other regulations that will impact international trade. What is certain is that nearly every major company will be affected over the coming year. Changes on the horizon include:

- New tariffs and trade barriers driving up costs and forcing companies to rearrange their supply chains and also potentially sparking retaliation against U.S. businesses overseas, especially in China.
- Some countries restricting the flow of data across borders, increasing costs and potentially impeding the growth of data-driven global businesses.
- The growing number and stronger enforcement of financial crimes regulations that are increasing the cost and regulatory burden of doing business in some regions.

But there are also bright spots of global cooperation in the trade of goods, services, and data, as well as intellectual property protection. Businesses that can adapt to and engage in the evolving policy landscape will have the edge.

“This is a time of tremendous uncertainty for global companies, as the U.S. makes aggressive
“Right now, you see more free trade agreements being negotiated by more countries, at a faster pace, than any time in history.”

—Robert Holleyman

A FRACTURED TRADE PICTURE

The world’s attention has been captured by the tough talk (and walk) of the world’s largest economy, as it revisits or revamps international trade deals, imposes tariffs on aluminum and steel and billions of dollars of Chinese imports, and reconsiders the proper role of the World Trade Organization in the America First era.

The Trump administration has also been granted greater authority by Congress to scrutinize or block foreign investments that might threaten U.S. control of key technologies. This move has enjoyed bipartisan support (see International Trade, page 12).

In North America, the new United States-Mexico-Canada Agreement (USMCA), which could replace NAFTA, holds the promise of bringing trade relations within the continent somewhat back to normal. But the trade war with China appears unlikely to fully resolve soon, Holleyman predicts. The U.S. has been pushing China for fundamental market-oriented reforms—such as reductions in subsidies to state-owned enterprises and openness to foreign investment in sensitive technological sectors—that China has been in no hurry to implement, he notes.

Yet even as the U.S. has escalated its tariff war with China, “the rest of the world is moving more aggressively to strike new agreements that can reduce tariffs and non-tariff barriers to trade,” Holleyman observes. He points to recent trade deals between the European Union and Japan and the EU and Canada; the Regional Comprehensive Economic Partnership, a 16-country inter-Asian negotiation; and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the agreement signed by 11 countries after the U.S. withdrew from its predecessor. The CPTPP went into effect in December 2018 and is now in force among seven nations.

As for the WTO, rumors of its imminent demise may be exaggerated, says Holleyman. The U.S. is unlikely to leave the WTO, and it (like the EU and Japan) continues to pursue WTO trade cases against China. The U.S. is also participating in planned WTO rule setting on digital trade and e-commerce.

With trade policy fracturing, the game of global commerce has grown in complexity—from checkers to chess. Companies must plan more intensively and think further ahead. “Every global company should be mapping out its supply chain—and its competitors’ as well—and analyzing them against various trade negotiations so that they can predict the impact of new agreements or tariffs,” Holleyman says. “You want to preserve your ability to do business but also find ways to expand your opportunities” (see sidebar, page 7).

STEERING THROUGH TRADE CONFLICTS

In the absence of stabilized trade regimes, countries and companies will continue to use trade policy as a competitive weapon, says David Stepp, an International Trade Group partner with
Crowell & Moring in Los Angeles. Stepp predicts a large increase in anti-dumping and countervailing duty cases as the Trump administration demonstrates its willingness to hear complaints by U.S. producers that they are victims of unfair competition. Even if these complaints are justified, a duty on a product meant to protect one group of U.S. manufacturers can send costs soaring for other domestic companies.

Stepp anticipates that the U.S. trade war with China will not be resolved quickly. The conflict has many companies weighing a variety of unpleasant options. “Moving all production outside of China can be an expensive and time-consuming process, especially for regulated industries where qualifying a new supplier can take a year or more. As a result, some companies will keep production in China and absorb as much of the added costs as possible,” Stepp predicts. This is especially likely in lower-margin industries like retail.

But some companies are finding ways to minimize the impact of tariffs. One strategy, known as tariff engineering, is to advocate with customs officials that an imported good is being listed under the wrong tariff classification and should be reclassified in a category not covered by a special duty. Conversely, other companies are arguing that a competitor’s imports are misclassified and should be covered by a special duty.

Other strategies include attempts by some companies to change the “country of origin” for their imported goods, for example by keeping some manufacturing in China but moving final production to a third country. If U.S. Customs rules that the product has been “substantially transformed” in this third country, then China might no longer qualify as the product’s country of origin and special tariffs would no longer apply.

Companies must tread carefully when attempting moves like these, Stepp says. “U.S. Customs is acting aggressively to enforce trade rules. Even when companies are not the importer of record, U.S. Customs is investigating whether companies are conspiring or colluding with importers to circumvent those rules,” he explains. General counsel should ensure that robust trade compliance programs are in place to handle the expected surge in enforcement actions.

As for the Chinese, they are retaliating against the new U.S. tariffs in multiple ways. Beyond increasing tariffs on U.S. exports, the government has the ability to make the business climate even more difficult for multinationals operating in China, by slow-walking licenses and permits, for example. “China is a highly regulated economy, so there are a lot of non-tariff ways to make life difficult for U.S. companies,” Stepp notes. For now, the Chinese government doesn’t want to discourage foreign investment, but it certainly can impose onerous measures if trade negotiations don’t go well with the United States.

WHAT’S IN YOUR SUPPLY CHAIN?

Trade conflicts could reduce opportunities for U.S. multinationals in countries other than China, Stepp says. “Other nations are retaliating against U.S. import tariffs with their own tariffs against U.S. exports. They’re also stepping up their own anti-dumping complaints and targeting U.S. exports such as agriculture that benefit from government subsidies,” he says.

As U.S. companies consider diversifying their sourcing to avoid current or potential tariffs, a good first step is to get a full understanding of tariff costs and of country-of-origin information from their major suppliers. Then they can look at opportunities to take advantage of reduced trade barriers under new trade deals that are signed or pending outside the United States.

Companies that have a better understanding of their supply chain are poised to reduce risks as well as costs. One example is in the area of consumer product safety. “All of this focus on tariffs is trickling into the consumer protection world because yet again companies are waking up to the fact they don’t always have complete visibility into their supply chain,” says Cheryl Falvey, a partner in Crowell & Moring’s Mass Tort, Product, and Consumer Litigation Group and the former general counsel of the Consumer Product Safety Commission.

Supply chain transparency is key to compliance with consumer protection regulations in areas such as country-of-origin labeling and “Made in the USA” claims, Falvey says. Tariff scrutiny shines a bright light on where the product is assembled and from what parts. Today’s products can be assembled from a variety of components sourced from different locations all around the globe. “Traceability is also crucial if and when a component within a consumer product fails,” Falvey notes. “Manufacturers must be able to trace components to the factory and determine what went wrong if they are to limit the scope of any required corrective action or recall.”

Falvey predicts technology enhancements will improve supply chain visibility and aid in compliance with regulatory requirements. “Blockchain has
already received early adoption as a way to manage traceability in food supply, whether to demonstrate produce comes from a region unaffected by a food-borne pathogen or from a farm that meets standards for organic labeling. It has practical applications that will aid legal compliance in any product manufactured and shipped globally,” she says.

RETHINK CHINA STRATEGY? MAYBE NOT

When analyzing whether to move production in response to trade conflicts, it’s important to take a holistic approach, says John Brew, a Washington, D.C.-based partner at Crowell & Moring and chair of the firm’s International Trade Group. China is a principal case. Rising tariffs and wages have many Western executives wondering whether it’s time to rethink their China strategy, and indeed, the per-unit cost of production there may be increasing.

Yet production shutdowns in China come with considerable costs, Brew says. Mass layoffs trigger notice and severance requirements. Equipment moves trigger duties. The time lost to moving and setting up new facilities elsewhere could lead to production delays. And then there’s the reputational cost of pulling up stakes. “Companies came in and built up these Chinese cities,” he adds. “If they pull out of China due to trade conflicts, will they be welcomed back when the trade winds change?”

The need to move could also be obviated by changing developments: The trade conflict could settle down, or wages in the new production country could increase. No one can predict the future, but a truly holistic spend analysis requires consulting with experts from throughout the company, including human resources, communications, tax, finance, and legal, Brew says.

WHERE DOES ALL THE DATA GO?

As with the case of goods and services, the outlook for the free flow of data across borders is decidedly mixed, says Frederik Van Remoortel, a Privacy & Cybersecurity Group partner in the Brussels office of Crowell & Moring. First the bad news: In countries such as Russia, China, India, and several African countries, data localization is on the rise. “The official reason is often the desire to protect the data of the individual and the security of the data in general, but behind the scenes, these rules are very often protectionist,” Van Remoortel says. “These governments want to ensure they can have access to the data and protect local providers.”

Data localization rules generally obliges companies to keep certain data—or a copy of certain data—inside the territory. Multinationals that would normally centralize their data or use cloud services must incur the higher costs and risks of storing, securing, and updating multiple copies. In countries such as China, the rules seem to go hand in hand with government censorship. U.S. tech industry groups are especially worried about China’s new cybersecurity laws, which have already resulted in Chinese authorities fining companies.

ANALYZE YOUR SUPPLY CHAIN: 5 STEPS

While big free trade agreements like North America’s USMCA get much of the press, dozens of other agreements still under negotiation could also affect profits at global companies. “The vast majority of companies don’t have a coherent strategy for addressing these agreements,” says Ambassador Robert Holleyman, president of Crowell & Moring International and a former deputy U.S. trade representative. “They don’t have a clear grasp on how trade rules can affect their costs, or how advocacy can influence those rules.”

The first step to making trade work for your company is to analyze how your supply chain is affected by existing or pending agreements. Here are five questions to ask when determining how a proposed agreement could affect your company:

- **Where do your products come from?** Work with your supply chain or operations managers to map out the links between your raw materials or components, assembly plants, and final markets for each good or service.
- **What are the current and proposed tariffs?** Assess tariff costs at each link of the chain and focus on the products or stage where total tariff costs are highest.
- **What are the rules of origin?** A rule of origin allows for a reduced tariff if sufficient product inputs are sourced from within the free-trade area. The shape of a company’s supply chain may determine whether the company advocates for strict or liberal rules of origin.
- **What non-tariff barriers are discussed in the agreement?** Rules on intellectual property, labor, the environment, and more can also influence your company’s advocacy positions on an agreement.
- **What about your competitors’ supply chains?** Information on where your competitors source, manufacture, or sell their products may be publicly available. Global companies have complicated footprints; a tariff that helps you might hurt your competitor, or vice versa. Make sure your company’s specific interests are understood in the negotiations.
HOT SPOTS FOR 2019

It could be an unpredictable year. Here’s what businesses should watch out for around the world in some key areas.

UNITED STATES
Now favoring bilateral over multilateral deals, the U.S. is expected to begin free trade negotiations with the UK, EU, and Japan in 2019.

LONDON
The UK plans to exit the EU. If it remains in an EU customs union, it would have limited ability to negotiate new trade deals and would not enjoy full benefits of new EU trade deals.

EU
Enforcement of the GDPR by European regulators will gather steam throughout 2019.

GENEVA
Challenging discussions on the reform and modernization of global trade rules through the World Trade Organization will continue in 2019.

CHILE
Chile will host the Asia-Pacific Economic Cooperation (APEC) Forum in 2019. The forum brings together business, government, and academia from 21 markets around the Pacific Rim to discuss health innovation, regulatory capacity building, digital skills, and more.

ARGENTINA
The Americas Competitiveness Forum is slated to take place in Argentina in 2019.

BRAZIL
The world’s ninth-largest economy has developed a data protection law inspired by Europe’s GDPR. It takes effect in early 2020.

INDIA
By last October, India required financial firms to store payment-related data locally.

Source: World Trade Organization
Source: World Bank
A trade slowdown is expected in 2019 along with a slowdown in global GDP growth.

**VOLUME OF WORLD MERCHANDISE TRADE**

Percent change

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate</td>
<td>5%</td>
<td>4%</td>
<td>3%</td>
<td>2%</td>
<td>1%</td>
<td>0%</td>
<td>1%</td>
<td>2%</td>
<td>3%</td>
<td>4%</td>
<td>5%</td>
<td>6%</td>
<td>7%</td>
<td>8%</td>
<td>9%</td>
<td>10%</td>
<td>11%</td>
<td>12%</td>
<td>13%</td>
<td>14%</td>
<td>15%</td>
<td>16%</td>
<td>17%</td>
<td>18%</td>
<td>19%</td>
<td>20%</td>
<td>21%</td>
<td>22%</td>
</tr>
</tbody>
</table>
```

**REAL GDP AT MARKET EXCHANGE RATES**

Percent change

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate</td>
<td>5%</td>
<td>4%</td>
<td>3%</td>
<td>2%</td>
<td>1%</td>
<td>0%</td>
<td>1%</td>
<td>2%</td>
<td>3%</td>
<td>4%</td>
<td>5%</td>
<td>6%</td>
<td>7%</td>
<td>8%</td>
<td>9%</td>
<td>10%</td>
<td>11%</td>
<td>12%</td>
<td>13%</td>
<td>14%</td>
<td>15%</td>
<td>16%</td>
<td>17%</td>
<td>18%</td>
<td>19%</td>
<td>20%</td>
<td>21%</td>
<td>22%</td>
</tr>
</tbody>
</table>
```

**GLOBAL TRADE AND INVESTMENT VOLUME THROUGH 2020**

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>262</td>
<td>286</td>
<td>309</td>
<td>329</td>
<td>355</td>
<td>379</td>
<td>401</td>
<td>428</td>
<td>445</td>
</tr>
</tbody>
</table>
```

**REGIONAL TRADE AGREEMENTS**

The number of regional trade agreements has increased rapidly since 1990.

Source: World Trade Organization
or ordering them to suspend operations.

Now the good news: More trade pacts and international agreements recognize the importance of cross-border data flows and include provisions to facilitate the free flow of (personal) data. Such provisions can be found in the U.S.-Mexico-Canada Agreement and the CPTPP, and the Asian-Pacific APEC countries have negotiated a cross-border privacy rule system to build trust in the cross-border transfer of personal information.

Similarly, in its recent trade agreement with Japan and in other negotiations, the EU is promoting the free flow of personal data to countries with adequate data privacy rules. The European regulation on personal data, the GDPR, has been in effect since May 2018. “In 2019, global companies can expect GDPR enforcement to gather steam,” Van Remoortel says. EU member states will also implement the directive on security of network and information systems, which will, for instance, impose additional cybersecurity obligations on operators of essential services and key digital service providers.

Moreover, countries and states such as Brazil and California are weighing or implementing legislation that enshrines Europe’s GDPR data privacy principles. Global companies will hence be busy complying with a slew of new regulations relating to the protection of personal data and data flows in general.

“Companies are taking data protection seriously, and many have someone at the board level responsible for it,” Van Remoortel notes. “We see many companies struggling with global implementation of data protection legislation.” It’s important to keep abreast of varying national regulations in areas such as data breach notification, Van Remoortel says. Given the likelihood of a data breach, companies must practice their response in many different jurisdictions well ahead of an actual occurrence. While all these laws impose their own regulatory burden, they also increase user confidence in data services, he notes.

“Many executives are still not aware of how data localization and data protection laws, in particular regarding data transfers, can impact M&A processes and related due diligence,” Van Remoortel adds. Obviously, potential acquirers should investigate whether targets are compliant in order to avoid buying risks. But the due diligence team itself may be breaking data laws if it transfers data out of the country for review.

**GROWING PROTECTION FOR INTELLECTUAL PROPERTY**

Intellectual property protection remains a big concern for global companies, and protection is still wanting in major markets such as China, India, Russia, Argentina, and Indonesia, according to recent reports by U.S. and EU authorities. Nonetheless, the trend is pointing toward stronger protection everywhere, says Teresa Stanek Rea, a Washington, D.C.-based partner at Crowell & Moring, a director with Crowell & Moring International, and former acting and deputy director of the U.S. Patent and Trademark Office.

“In general, IP is getting more respect, and protection is growing in sophistication, in each and every country,” Rea says. “In the U.S., there’s an ongoing controversy about whether the system is supporting patents and enforcement as much as it should be. Multinationals file patents and they want their inventions to be protected in all their markets. Most trade agreements recognize this, and the IP provisions in trade agreements try to provide consistency and predictability. But the rest of the world is getting strategic because they all want the innovation and industries that create jobs.”

Rea is heartened by patent modernization provisions in many of the new trade agreements discussed above and by recent national laws to protect trade secrets, a relatively new frontier in IP protection. She also points to the progress of the IP5, a working group of the world’s largest patent offices, in developing systems that make it easier for inventors to file for a patent in multiple offices.

When it comes to IP, the news media has fixated on the many tactics employed by China to strong-arm or even steal valuable knowledge from the U.S. and other nations. It’s unclear whether U.S. tariffs will compel China to fix this problem, but Rea says China is already improving IP protection as it seeks to protect its growing track record of domestic innovation. For example, some Chinese courts are showing more fairness to foreign companies in IP disputes.

Many executives don’t realize that the U.S. Patent and Trademark Office has IP attachés in U.S. embassies in 12 strategic locations around the world. Executives facing challenges in enforcing their IP rights can receive advice from their region’s attaché about how to proceed. The attaché also advocates with regional authorities for more favorable policies. “Businesses don’t always use the attaché to the extent they could,” Rea says.
“Multinational companies should think of their IP in the context of international trade,” Rea adds. “Multinationals should file patents and trademarks in every country in which they do business. They evaluate their IP to determine the strength of their proprietary position to determine likely market share.”

FINANCIAL CRIMES COMPLIANCE IS EVERYONE’S PROBLEM NOW

The Trump administration is poised to expand its aggressive use of sanctions, having commenced a new program against Nicaragua and expanded sanctions against Russia, Venezuela, and corrupt actors under its Global Magnitsky program, while reimposing sanctions on Iran. The so-called sectoral sanctions imposed on Russian and Venezuelan entities will be especially difficult for financial and non-financial companies alike because they allow some but not all transactions with designated entities, requiring U.S. persons to carefully consider transactions on an individual basis. The U.S. and the EU also have developed conflicting sanctions policies over Iran, complicating compliance decisions for companies that operate in both jurisdictions.

The low number of enforcement actions this past year was likely an anomaly; a rise is expected this year, says Carlton Greene, a Washington, D.C.-based partner at Crowell & Moring and a veteran of the Department of the Treasury’s Office of Foreign Assets Control (OFAC). Greene expects in particular more enforcement of Russia sanctions, more enforcement against nonfinancial institutions, and more detailed guidance from OFAC on what it expects from U.S. companies with respect to the administration of their internal sanctions compliance programs.

Meanwhile, the enforcement and impact of anti-money laundering laws continue to grow. In the U.S., the nearly $600 million penalty against one bank shows that financial regulators continue to prioritize enforcement against AML programs they view as under-resourced at a time when AML costs increasingly loom large in the operational budgets of banks and other financial institutions. A number of solutions to address this tension will continue to develop in 2019, including legislative proposals to alter reporting thresholds. New guidance from the Financial Crimes Enforcement Network (FinCEN) and federal banking agencies appears intended to signal a favorable enforcement policy toward AML innovation. At the same time, Greene thinks that FinCEN and the FBAs have agreed to take a relatively forgiving approach to the biggest new piece of AML regulation banks are facing, FinCEN’s customer due diligence rule. But such forbearance will not last forever and will apply only where there are good faith efforts to comply.

In Europe, enforcement appears to be just getting started. Most recently, law enforcement raided the offices of a major international bank in connection with potential AML issues, not long after it was fined nearly $700 million for AML violations. In September 2018, Dutch bank ING agreed to pay nearly $900 million in fines and disgorgement. And Danske Bank in Denmark now faces an estimated $630 million penalty for allowing Russian money to be laundered through it, with some reporting that the Department of Justice is also investigating. There has been talk of strengthening and centralizing EU AML regulatory authority in response. All of this is likely to lead to increased AML compliance expenditures for European institutions and the same pressure to seek innovative solutions that U.S. banks face, Greene believes.

Finally, Greene predicts that regulators in the U.S. are likely to make some progress in the coming year in efforts to negotiate their approach to the regulation of virtual currency and other digital assets. There are two key questions in this area: First, whether and when digital assets will be regulated as securities, and what will be the regulatory boundaries between FinCEN, the Securities and Exchange Commission, and the Commodity Futures Trading Commission. Second, nearly every U.S. state has its own money transmitter laws that may apply to such businesses. Greene sees a good likelihood for guidance from federal agencies on the first problem and for key regulatory approvals of new businesses that will help define a way forward for the exploding field of digital assets. The second issue is more complicated, but a growing number of states are working together to create reciprocal licensing arrangements. With regard to digital assets overall, the current path is toward tokenizing every conceivable form of asset, Greene says. This is complex, and “a large number of these businesses may fail,” he says. “But those that succeed are likely to change the world as we know it.”

“A LARGE NUMBER OF BUSINESSES BASED ON DIGITAL ASSETS MAY FAIL. BUT THOSE THAT SUCCEED ARE LIKELY TO CHANGE THE WORLD AS WE KNOW IT.”

—Carlton Greene

“If companies pull out of China due to trade conflicts, will they be welcomed back when the trade winds change?”

—John Brew
Federal law has long provided the president with the authority to review and block foreign investment in sensitive sectors of the American economy. Originally focused primarily on the aerospace and defense sectors, the scope of national security has expanded through law and practice to include critical technologies and infrastructure. At the behest of Congress, the governing rules are being rewritten to help maintain the United States’ status as a leader in the development of key technologies with global applications. The new rules could protect American innovation—but they could also hinder foreign investment and collaboration that would foster the development of new technologies.

“This is the most significant revision of the United States’ foreign investment review process in the last decade,” says Alan Gourley, a partner in Crowell & Moring’s Government Contracts Group. “The rules now capture a broader realm of businesses and investors and make mandatory notice of investment in certain sectors.”

A bipartisan bill enacted in August 2018 expanded the scope of investments that may be reviewed by the Committee on Foreign Investment in the United States, or CFIUS. Made up of members of the State, Defense, Justice, Commerce, Energy, and Homeland Security departments and led by the Treasury secretary, CFIUS reviews transactions and—when mitigation of national security concerns cannot be achieved—sends its findings and recommendation to the president, who can block the deal.

In some ways, the new law merely codifies the more aggressive stance CFIUS was already taking under the Trump administration in challenging investments, particularly those involving Chinese investors.

CFIUS has until February 2020 to implement the new law. It has started with a pilot program, imposing “mandatory declaration” in connection with a pending deal involving critical technologies within any of 27 industries. The list includes military-centered technologies such as guided missiles but also computer device storage, electronic computer manufacturing, ball and roller bearing, and aluminum refining. “Critical technologies” also includes a new category called “emerging and foundational technologies,” which is still being defined (see sidebar).

In the past, CFIUS limited its review to mergers and acquisitions where a foreign investor might acquire a controlling stake. Under the pilot program, CFIUS may review investments of any size if the investor could gain access to key technical information or would be given board representation or other involvement in substantive decision making related to the critical technologies. In practice, this means CFIUS could have purview over some venture capital and private equity investments in which the foreign investor has as small as a 1 percent stake. There is a limited exception, implemented in the pilot program, that excludes indirect (and passive) investment though qualified investment funds, Gourley says.

NEW HURDLES FOR FOREIGN INVESTMENT

A potentially positive feature of the law is that it provides CFIUS additional resources and expands the strict deadlines for CFIUS to come to a decision, which might mean a more predictable timeline for dealmakers eager to close. Once the new filing fee has been implemented, CFIUS may be able to hire and train even more staff to conduct the expanded reviews. In the interim, prospective investors and their targets can expect CFIUS staff to be distracted by the need to develop implementing regulations and handle the new mandatory declaration workload.

But the law is also likely to accelerate the recent downturn in Chinese foreign direct investment in the U.S., Gourley says. The trend has been fueled in part by concerns about Chinese
investors not following through on their pledges and China’s own measures aimed at controlling outbound investment, The Wall Street Journal reported last year. But greater assertiveness by CFIUS over the past two years has also played a part.

“You need to file for committee review for a much broader range of deals, and that might scare off some potential investors,” Gourley says. “A U.S. target might be interested in a foreign investor but concerned with the uncertainty and additional timing engendered by a voluntary or mandatory review. It might be easier to find financing elsewhere.”

Sometimes CFIUS recommends blocking a deal entirely; other times it requires mitigation measures for the deal to move forward. For example, a company might have to agree to forbid the foreign investor from accessing sensitive information, or to maintain certain facilities or technologies within the United States. In extreme cases, the foreign investor can be excluded from having any real voice in management, Gourley says.

EARLY PLANNING HELPS

CFIUS deliberates in secret, and its reviews are confidential. That’s a necessity, given that the reviews involve trade secrets, sensitive technologies, and classified government threat assessments. That makes CFIUS something of a “black box,” Gourley says, but there are ways to get a sense of how its members might respond to a potential deal.

Prior to filing a CFIUS notice, Gourley and his colleagues sometimes meet with CFIUS agency staff to sound them out informally. The goal is to glean useful information from which to plan and propose mitigation in sensitive cases. Through experience, Gourley also has a sense of the issues that concern the committee. The trustworthiness of the foreign investor and its activities elsewhere in the world are factors to be considered in addition to the sensitivity of the U.S. business.

To the extent possible, he says, U.S. executives should vet foreign investors interested in their companies. What businesses are they engaged in? What kind of deals have they had with the U.S. government? What is their reputation among U.S. officials? Have they been involved in countries sanctioned by the U.S.? What kinds of issues might send up a red flag?

Well before any deal is signed, potential foreign investors should assess and investigate the concerns CFIUS might raise. “There could be an array of mitigation options, some of which you can’t foresee,” says Gourley. “The sooner you plan for those possibilities, the better you can allocate the risk of mitigation in the deal documents.”

“Given the level of interest from U.S. industry and the challenges inherent in this process, it may be some time before Commerce introduces new controls under the new law.”

—Maria Alejandra del-Cerro

THE ACCOMPANYING EXPORT CONTROL REFORM AUTHORITY

The Export Control Reform Act, signed last August, provides permanent statutory authority for Export Administration regulations (EAR), which control the cross-border transfer of U.S. origin “dual-use” items.

Much of the new law codifies the agency’s existing export control practices. One provision goes further, however, as a result of the effort to strengthen control over foreign investment in the United States. It directs the Commerce Department to establish an interagency process, subject to a public notice and comment period, for the identification of “emerging” and “foundational technologies” that “are essential to the national security of the United States.” Companies dealing in these technologies would be subject not only to export controls but also to reviews of investment deals by the Committee on Foreign Investment in the United States, or CFIUS.

The Commerce Department’s Bureau of Industry and Security kicked off the process with the issuance of an advance notice of proposed rulemaking (ANPRM) in November 2018 that identifies certain broad categories of emerging technologies, including artificial intelligence, biotechnology, microprocessor technology, robotics, and data analytics. The ANPRM seeks recommendations on how to define specific technologies within these categories, the development status of these technologies in the U.S. and other countries, whether these or other categories are important to U.S. national security, and the potential impact of such controls on U.S. technological superiority.

BIS will likely need time to review industry feedback, as well as classified information, information developed from the CFIUS process, and information developed by BIS’s technical advisory committees to focus the interagency review process and formulate proposed controls. The precise wording of any new proposed controls will also require a notice and comment period prior to implementation.

“Given the level of interest from U.S. industry and the challenges inherent in this process, it may be some time before Commerce introduces new controls under the new law,” says Maria Alejandra (Jana) del-Cerro, counsel at Crowell & Moring in the International Trade Group and a member of the firm’s CFIUS team.
The Trump administration has been successful in filling open spots on the federal bench with conservative judges, with the expectation by many that a more conservative bench will go hand in hand with the president’s deregulatory agenda, and thus help shape the direction of not only the federal courts but of the administrative state, long after this administration ends. With the Supreme Court now firmly in conservative hands, some think the time is nigh for the federal judiciary to reassert itself as the final arbiter of what statutes mean in litigation involving federal agencies.

At stake is so-called *Chevron* deference, which is the deference courts typically give to federal agencies interpreting statutory programs they are responsible for administering. The doctrine has dominated administrative law for more than 30 years. If the Supreme Court reverses or narrows it, as some are clamoring for it to do, it could have major repercussions for future regulations in areas ranging from the environment to health care to communications.

The clamoring is in no small part a response to the regulatory agenda of the prior administration. “Business has been frustrated for many years as the judicial check they relied on to scrutinize agency action was viewed more as a rubber stamp,” says Dan Wolff, co-chair of the Administrative Law and Regulatory Practice at Crowell & Moring. Reversing or narrowing *Chevron* would signal that the judicial check means something again. Of course, what’s good for the goose is good for the gander, says Wolff: “A revisited *Chevron* would apply to deregulatory actions as well as new regulations.”

**TOO MUCH DEFERENCE?**

The landmark 1984 decision was the “seminal distillation of a principle of interpretation that developed over the course of the 20th century, as the administrative state grew,” Wolff says. *Chevron* articulates a two-step test for judges reviewing an agency’s construction of the statutes it administers. Step 1 analyzes whether Congress has “directly spoken to the precise question at issue.” If it has, then the statute itself provides the answer to the legal question. But if it hasn’t—that is, if the statute is silent or ambiguous—then the court moves to Step 2 and considers whether the agency’s interpretation is “a permissible construction of the statute.”

In practice, when a court finds that the statute is ambiguous, it usually defers to the agency’s interpretation. This is what many find galling, especially in light of the burgeoning number of federal regulations on the books. Indeed, for better or worse, the “administrative state” has grown inexorably. The number of federal regulations nearly tripled from about 400,000 in 1970 to almost 1.1 million in 2016, according to The Mercatus Center at George Mason University. That trend continued through both Republican and Democratic administrations.

During the Obama administration, business complained vociferously about regulatory overreach in such areas as finance, the environment, health care, and labor. At the same time, the chorus of jurists, scholars, and commentators contending that the federal courts were showing too much deference to agencies grew to a near fever pitch, with *Chevron* taking much of the blame.

*Chevron* is premised on a separation-of-powers notion that when Congress delegates to an agency the authority to administer a law and is not specific about a particular outcome, it is not up to the courts to second-guess the agency’s policy choice to address the ambiguity because that, in effect, would be legislating, which is not the proper role of the judiciary, Wolff explains. But more recent scholarship posits a counter separation-of-powers viewpoint that is hostile to deference. In 2016, then Judge Gorsuch stated that, thanks to *Chevron*, “courts are not fulfilling their duty to interpret the law.” Justice Thomas has also stated that *Chevron* is a usurpation of judicial power. Chief Justice Roberts has indicated a willingness to revisit the doctrine, as did now-retired Justice Kennedy in an opinion issued his last day on the Supreme Court, and many see Justice Kavanaugh as his natural torchbearer. “Conventional thinking is that at least four justices are ready to revisit *Chevron* in the right case,” Wolff notes.

**SIGN OF THINGS TO COME?**

Indeed, the Supreme Court has already agreed this term to reconsider *Chevron*’s jurisprudential kin: *Auer* deference. *Auer* posits that courts should defer to agency interpretations of their own regulations if, as under *Chevron* Step 2, the agency’s interpretation is not unreasonable.

Wolff points out that to administrative law wonks, while at first blush *Auer* seems to be logical and consistent with *Chevron*, it is more problematic because it effectively allows agencies to “move the goalposts” by revisiting key terms of a regulation long after the notice-and-comment rulemaking period has closed. In that way, it encourages agencies to write ambiguous
If Chevron is narrowed, “it may make it harder for an agency to peel back a regulation, especially if the prior regulation was upheld by the courts or has become part of the legal fabric.”

—Dan Wolff

regulations to give them greater regulatory flexibility at some later date—at the expense of the regulatory certainty and due process desired by business. Yet for most business folks, Auer deference and Chevron deference are more or less synonymous.

While Wolff believes Auer is in real trouble—“its day of reckoning has seemed imminent for several years now”—he thinks that the Supreme Court is unlikely to reverse Chevron outright. Instead, he thinks the Supreme Court will narrow its application and embolden the lower courts to more closely scrutinize agency interpretations. For example, the Supreme Court might direct judges to be more rigorous at Step 1 by working harder to distill the meaning of the text and to be less inclined to find ambiguity. Wolff says this was more or less the philosophy of the late Justice Scalia: “He adhered to Chevron, but judiciously,” Wolff says. The problem, he notes, is that the lower courts have not consistently applied the same rigor in agency cases as the Supreme Court.

Another path the high court might take is to encourage lower court judges to apply the “major questions” exception to Chevron, which excuses deference in instances where the subject matter of the regulation has deep political or economic significance. Chief Justice Roberts articulated a version of this exception in his 2015 decision in King v. Burwell, dealing with the Affordable Care Act, articulating the notion that where the impact to society is great, the courts should not—in contrast to the basic premise of Chevron—presume that Congress intended to delegate so much discretion to the agency. Justice Scalia said something similar in a 2014 Clean Air Act opinion, stating that the courts should be wary of deferring to agency rulemaking that “would bring about an enormous and transformative expansion” of the agency’s regulatory authority “without clear congressional authorization.”

What has become known as the “major questions” or “major rules” doctrine seems premised on a related constitutional theory favored by opponents of expansive agency authority: the idea that the Constitution vests in the Congress the exclusive authority to create new law and that agency claims on delegated rulemaking authority must therefore be viewed with a healthy skepticism, lest agencies venture from their law “executing” function to a law “making” function. Wolff points out that Chevron deference has greater logic where the agency is addressing the interstices of a statutory program that seem obviously within the agency’s statutory mandate and wheelhouse; it loses currency as a doctrine where it is invoked to justify massive expansions of agency authority into new areas that Congress itself has not yet touched.

In 2016, then- Appeals Court Judge Kavanaugh summarized the basis for the doctrine: “For an agency to issue a major rule, Congress must clearly authorize the agency to do so. If a statute only ambiguously supplies authority for the major rule, the rule is unlawful.”

BE CAREFUL WHAT YOU WISH FOR

For opponents of aggressive regulation, the narrowing or reversal of Chevron could be a double-edged sword. That’s because while the soundness of new regulations often depends on interpretations of ambiguous statutes, the repeal or replacement of a regulation may also turn on the interpretation of the identical ambiguity.

In fact, Chevron itself was a Reagan-era deregulatory victory of sorts: The deference granted was to a reinterpretation of the Clean Air Act that was favored by industry. It is well accepted, Wolff notes, that an agency’s decision to change course on the meaning of an ambiguous statute is entitled to no less deference than the prior interpretation so long as the new interpretation is a permissible reading of the statute. But if Chevron is narrowed, he says, “it may make it harder for an agency to peel back a regulation, especially if the prior regulation was upheld by the courts or has become part of the legal fabric.”

In this way, a Chevron narrowing may not necessarily redound to the benefit of the business community, Wolff adds, noting that “the business community intervenes all the time in defense of favorable agency decisions, and deference is no less important in many of those cases.”

Ultimately, the question for the Supreme Court to decide is whether separation of powers militates in favor of deference—or against it. If the high court constrains Chevron, it will likely hark back to the seminal 1803 case of Marbury v. Madison, which first established the principle of judicial review. It’s the judiciary’s obligation, the Supreme Court declared, “to say what the law is.” Of course, Marbury arose more than a century before the rise of the modern “administrative state.” Wolff thinks that if Chevron did not exist by name, some semblance of deference would still exist as a matter of judicial practicality and restraint. What is needed, therefore, is not the reversal of Chevron but a return to original principles and balance. “The Supreme Court cannot decide every case,” Wolff observes. “It would seem inevitable that it must revisit Chevron not for itself but to bring the lower courts into line.” And if it does that, then “a paring down of Chevron might really bend the historical curve of regulations that make their way into the federal code.”
Most ratepayers know little about their electricity’s fuel source and have had limited ability to buy “greener” electricity from their local utilities or to bypass those utilities entirely in favor of competing providers. Digital transformation will allow commercial, industrial, and residential customers to shape—and increasingly control—both services and pricing. Although just beginning, the increased flexibility and functionality made possible by digital transformation, Big Data, and predictive behavioral algorithms will increasingly disrupt the production, transportation, and use of electricity, and present both extraordinary risks and opportunities to incumbent utilities, competitive suppliers, and consumers.

The last major disruption to the energy sector was in the 1990s, when some states authorized retail customers to buy power directly from competitive suppliers. Digitalization of the power grid dramatically increases the degree and variety of customer choice. In response, utilities have developed increasingly energy-efficient and reliable products and have sought regulatory approvals to capture these opportunities.

The World Economic Forum estimates that digital transformation could unlock $1.3 trillion in value through 2025. The big questions are who is best positioned to capture that value, and will they be allowed to succeed. The first is a commercial and technological question. The second is a regulatory question that has yet to be fully addressed. Regulators influence market behavior both by creating or choosing between market structures and by selecting the kinds of companies allowed to participate, as well as the products and services that could be offered in these markets. Those positioned to take advantage of digital transformation will therefore have to wage both commercial and regulatory battles to secure their success.

RISE OF THE CONSUMER TECH FIRMS

“Household-name consumer technology and e-commerce companies that possess both enormous quantities of granular customer data and sophisticated data-processing capabilities are poised to disrupt the electric power industry,” says Larry Eisenstat, chair of Crowell & Moring’s Energy Group. “Their competitive advantage lies not in their ability to generate electricity, but in their knowledge of customers’ purchasing habits, demographics, and energy-usage patterns. They use data and software to understand and predict customer behavior and to communicate with customers—directly and in real time—by means of digital platforms (including in-home interactive personal assistant devices) as to what kind of electric service the customers want, when they want it, for what uses, in what amounts, and at what cost. Over time, this advantage will increase, particularly as the lines between federal/wholesale/transmission and state/retail/distribution services are blurred.”

Initially, says Eisenstat, customers will make the decisions, but eventually companies will offer products to make decisions on behalf of customers, similar to a stockbroker with full trading authority. “These companies will continue to learn more about their customers’ needs, activities, and tendencies,” he says. “When are they home? What appliances do they use? How interested are they in renewables or energy efficiency? Once you know usage patterns and behaviors, you can develop the right infrastructure mix and produce targeted offers that provide value to the customer and profits to the company.”

Using Big Data, a provider could combine customer-specific home information, smart meter data, and predictive analytics to offer a fixed price for electricity—with discounts for energy conservation. It could notify customers that a dishwasher is inefficient, for example, guarantee that a new machine would save a set amount on their electricity bills, and sell them that appliance.

Delivering solutions like these may require collaboration. For example, German power supplier E.ON teamed up with Microsoft to develop an AI-powered smart home platform to manage everything that uses electricity (appliances, solar panels, cars, etc.) and to optimize the levels of self-generated electricity versus “excess” electricity market sales.

The winners in consumer-facing energy technology will offer solutions without requiring the consumer to have any technical know-how, Eisenstat says, by making strategic use of consumer data. “These technologies will tell you how to manage your energy better,” he says. “They’ll do it automatically, using algorithms and predictive analytics. And they can sell you the right supply mix, services, and equipment.”

OUT ON THE EDGE

Big Data is being used to integrate distribution systems whose inputs include traditional central-station power delivered over the interstate transmission system and a plethora of so-called distributed energy resources, including everything from rooftop solar arrays and other customer-owned “micro” generators to energy storage and electric vehicles.

Digitalization and data analytics are keys to optimizing
electricity production and consumption, Eisenstat says, and could reduce grid reliance on older, less efficient power plants to meet “peak” energy demand. Digitally integrating distributed energy resources (including storage) can defer or avoid capital expenditures on new peaking plants and transmission lines. For example, he observes, a smarter energy grid would obviate much of the need for constructing large gas plants to firm up intermittent renewable power resources such as wind and solar.

A connected, efficient, and decentralized grid (aka the “energy internet”) has the potential to be more stable and less vulnerable to terrorism or natural disasters. Power plant owners could also extend assets through smart-grid strategies, including predictive maintenance. For example, GE’s new “Forever Turbine” initiative combines computer simulation, artificial intelligence, and 3-D printing to extend the useful life of its turbines decades beyond their current projected useful life of 30 years. The World Economic Forum estimates that digitizing asset lifecycle management could create $480 million in value through 2025.

WHO WILL WIN?

Transformation of the electric grid, when combined with customer expectations, is a recipe for industry disruption, particularly where that industry is heavily regulated, highly interdependent, and in many areas dominated by large utilities. Eisenstat believes that, as in the mid-1980s, when competitive power was in its infancy, fighting for the right to compete against incumbent utilities, the electricity sector is again at an inflection point. Issues pertaining to ownership and control of the electricity delivery system, the types of infrastructure and technology required to power that system, the rules regarding customer and competitive access, and the creation and pricing of new products and service offerings will again be hotly contested. The outcome of this inevitable conflict between incumbents and disruptors again will determine who captures the lion’s share of market opportunities.

“Who should own the solar panels, the charging stations, the smart meters?” Eisenstat asks. “Competitive suppliers? Incumbent utilities? Should incumbent utilities be limited to providing the conduit to the customer? What will the customer be able to control directly?” These are just some of the things that regulators must figure out.

Ownership and control of customer data is another key issue. While utilities have the most direct access to customer usage data, that doesn’t mean they should be the only party that can utilize it. What rights do customers have to this data? What rights should third-party companies have? How should privacy and cybersecurity considerations factor into decisions about control or distribution of such data? Eisenstat says that “while regulators must ensure a level playing field, not all competitive providers are necessarily entitled to receive all customer-related data in a utility’s possession. They shouldn’t be allowed to access a utility’s information system without agreeing to abide by cybersecurity protocols designed to protect that system from third-party intrusions. However, regulators must also ensure that these protections don’t themselves unreasonably restrict competitive entry.”

Regulators are grappling with such questions in both federal and state markets. Eisenstat points to hearings conducted as part of New York’s statewide energy strategy, dubbed “Reforming the Energy Vision.” Discussions are also occurring in California and Maryland, among other states, and he believes still more states—and the federal government—will explore these questions.

Incumbent utility companies start with an advantage in these discussions because they are known to the regulators, have political firepower, and traditionally roll their equipment and advocacy costs into base rates. Nevertheless, Eisenstat says, all stakeholders, especially new electricity sector companies, should do more than monitor or react to regulatory proceedings. “The new players, in particular, must proactively propose and advocate for regulatory regimes that catalyze the digital transformation of the electricity sector,” he says.

KEY POINTS

Customers Rule
Consumer technology companies are poised to capture value in a disrupted energy sector.

Grid Optimization
Digital transformation will optimize grid usage and defer or eliminate the need for costly new infrastructure.
Doing business with the U.S. government is about to get tougher as federal requirements for cybersecurity become stricter. While the need to protect sensitive government information and technology isn’t new, its importance in government contracting has historically—and understandably—been highest in the defense sector. The government’s heightened focus on cybersecurity will become sharper in 2019, when the Trump administration is expected to finalize a new proposed clause in the Federal Acquisition Regulation (FAR) that essentially extends the application of stringent Department of Defense cybersecurity rules to non-defense contractors, as well.

The new regulation focuses on so-called controlled unclassified information (CUI), which is government information that is considered sensitive and requiring protection but that doesn’t rise to the level of classified information. Common categories of CUI arising in government contracting include controlled technical information, export control information, privacy information (e.g., personal identifiers and health data), procurement and acquisition information, and proprietary business information.

For federal contractors, the message is clear: Cybersecurity is here to stay and will only become more critical if you want to work with government agencies.

WHAT TO EXPECT: EMERGING TRENDS

The FAR clause’s implications will likely extend beyond contractors, notes Evan Wolff, a Crowell & Moring partner and co-chair of the firm’s Privacy & Cybersecurity Group, who formerly served as an advisor to the senior leadership at the Department of Homeland Security. “Cybersecurity concerns are an increasingly common and integral aspect of corporate existence,” he says. “The application of defense-quality requirements to all government contractors will likely have a trickle-down effect on the private sector.”

Wolff sees several trends emerging as the new rule percolates through the administrative process:

- **Continued tightening of government cybersecurity standards.** As a matter of national security, the government will insist that its vendors maintain adequate protection to secure their IT networks against cyberthreats. Companies will accordingly put more effort and resources into cybersecurity.

- **Extension through the supply chain.** The government’s cybersecurity standards often apply to subcontractors as well as prime contractors, which likely will force many subcontractors to adequately protect their networks—an investment they may not be able to afford—or risk losing their government business. This scenario isn’t unusual, says Kate Growley, a counsel in Crowell & Moring’s Privacy & Cybersecurity and Government Contracts groups. “There are prime contractors that don’t appreciate how government requirements can put real hardship on subcontractors,” says Growley, “as well as subcontractors that don’t know that prime contractors have to meet the requirements in the first place. If both want to succeed, they’ll have to understand that cybersecurity is a shared responsibility.”

- **Competitive differentiation.** Increasingly, companies will be evaluated by their level of, and commitment to, cybersecurity. Those that are cybersecure will have a significant competitive advantage over companies that aren’t, whether as government contractors or more generally. They’ll be seen as more desirable vendors, partners, acquirers, or targets.

- **Corporate lifecycle issue.** Cybersecurity will become more of a determinant of corporate survival, and not simply because its absence exposes companies to existential threats.
such as hacking. Wolff notes, “We’re seeing more and more companies in M&A transactions analyzing the other party’s cybersecurity as a key criterion for making the deal. Over time, companies that aren’t cybersecure may find themselves standing still, or even going out of business, as their cyber-savvy competitors move forward.”

**Cultural imperative.** Cybersecurity will transcend its initial status as a purely technological matter and rise in importance to become part of companies’ cultural fabric, much like teamwork, safety, and cost-consciousness. It’s already a board-level concern at many companies, a standing that should grow into mainstream practice.

**CYBERSECURITY AS A TEAM SPORT**

One approach to cybersecurity counseling that has proven to be effective emphasizes cultural reinforcement and the development of a corporate infrastructure. As Wolff puts it, “Companies should think of cybersecurity as a team sport. Ideally, all parts of the company, from the board to operations, sales, legal, administration—everyone, really—should collaborate to keep the organization safe.”

An exemplary infrastructure would include these elements:

- **Appointment of a chief information security officer**—distinct from an all-encompassing CIO or CTO—commits dedicated resources to cybersecurity and signals to employees, customers, competitors, and investors alike that the company considers cybersecurity a priority.
- **Vulnerability analyses** help companies identify their weakest links—the first step toward achieving cybersecurity.
- **Conducting incident simulations, developing an incident response plan, and creating an incident response team** intensify awareness of cyberattacks and condition the company to deal with them. Think of this as the electronic equivalent to fire preparedness.
- **Training policies and procedures** are vital to maintaining cybersecurity and keeping everyone on the same page.
- **Physical, technical, and administrative controls** ensure that the right protections are in place and working.
- **Cyber-specific auditing and reporting processes** create and track accountability.
- **Due diligence capability for M&A and other transactions** evaluates the cybersecurity of potential targets and partners—and can serve as a yardstick for whether the evaluating companies are current on best practices.

- **Anticipation and assessment of litigation risks** takes on heightened importance in the constantly changing cybersecurity environment.
- **The purchase of cyber insurance** is an under-the-radar option that could be particularly helpful for smaller businesses with limited resources.

“Organizations that can build a sound infrastructure position themselves not only to deal with cyberthreats, but also to achieve greater success,” Wolff says. “The time is coming when the cost of not being cybersecure will be higher than the cost of maintaining best practices. Companies won’t want to be caught holding the bag when that happens.”

**GETTING CREATIVE TO GET THE CONTRACT**

Cybersecurity doesn’t have to be an all-or-nothing proposition for government subcontractors. Sometimes a little creativity goes a long way.

This can be the case when there’s only one subcontractor available that can provide a specialized product or service needed to satisfy a contract. Crowell & Moring’s Kate Growley notes that such sole-source providers are often small and don’t meet the government’s cybersecurity requirements. “Prime contractors should expect to deal with noncompliant subcontractors and be prepared to figure out a compliance workaround, which can be a difficult and complicated task,” she says.

The problem typically boils down to how to safeguard confidential government information when the subcontractors lack the necessary network protections. Growley says that prime contractors should start by asking, do we even need to share the information with the subcontractors at all, and, if yes, do they need to store it electronically. A straightforward, cost-effective solution can be for the subcontractor to use a third-party-managed service provider whose storage capabilities are already compliant. This isn’t always practical—which is where creativity comes in. In such instances, old-school use of paper copies can do the trick, as securing paper is usually much easier than securing a network. Another approach: have the prime contractor handle electronic storage and let the subcontractor view it on a secure portal or by visiting the facility.

“Prime contractors should expect to deal with noncompliant subcontractors and be prepared to figure out a compliance workaround, which can be a difficult and complicated task.”

—Kate Growley
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
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.
3-D PRINTING: MANUFACTURING, DISRUPTED

When it comes to 3-D printing, much of the excitement revolves around the amazing potential of the machine to build almost anything one layer at a time. In health care, that means drugs, medical devices, tissue, even hearts or lungs.

But much of the promise—and peril—of 3-D printing stems from the way it could upend the manufacturing process. And that change could have major implications for how companies in this space manage intellectual property, product liability, and cybersecurity.

Traditionally, products are built and distributed by the same company that designs them or by a handful of factories with close relationships with that company. The model that 3-D printing is moving toward—known as distributed manufacturing—is very different.

In the near future, many medical devices will be made not in factories but in hundreds or thousands of hospitals or doctors’ offices on their own 3-D printers. Here’s how that might work: A doctor would send details about a patient to a device’s maker, which would customize a design file and send it to the printer, which would “print” the device for the doctor to implant.

These devices will be personalized to an unprecedented degree and be printable on demand. This should make them cheaper, safer, more effective, and timelier than ever—if everything goes as planned.

But what if something is wrong with the printer, the software, or the materials the printer uses to make the device? What if the doctor, or a technician, fails to catch a manufacturing defect prior to implantation? What if a hacker intercepts the design file, steals the personal data, and modifies the design? What if the hacker uploads the design to the internet, so anyone with a 3-D printer could attempt to build the device with no training or experience? If any of these occur, lives could be at stake. And who would be responsible?

Distributed manufacturing is poised to disrupt a world where legal and regulatory frameworks have been built around the assumption of a close or identical relationship between designers and makers.

“So much control is being relinquished,” says Deborah Yellin, a partner in Crowell & Moring’s Intellectual Property Group. “I think you’ll see companies moving away from making things and toward saying, ‘Here are our instructions, and if you don’t follow them, you’ll be responsible.’”

HERE COME THE FEDS

Into this fray jumped the U.S. Food and Drug Administration, which has already approved more than 100 medical devices made using 3-D printing. In the past, Yellin notes, the agency could shut down a manufacturing facility if it suspected a problem with a drug or device. In the future, tracking and fixing problems may require a very different approach.

In December 2017, the agency released guidance for technical considerations for 3-D-printed medical devices. The document provides some guidelines for ensuring quality and safety across the production process, from design through printing and testing. Eventually, Yellin says, the FDA may also release guidance for bioprinting or 3-D printing of pharmaceuticals.

With its own 3-D-printing lab in-house, the FDA appears determined to keep up with the pace of technology. But there are many issues yet to be resolved, Yellin says. How will the agency regulate nontraditional manufacturing sites such as hospitals or doctors’ offices? How will it regulate the printers, the “inks,” or the design files? What about the IP covering the printers, “inks,” and design files? Patents may cover the hardware and software. And some aspects of the production process may be trade secrets. Enforcement of IP will be a big concern.

“The FDA realizes it has a long way to go, and it’s willing to

“I think you’ll see companies moving away from making things and toward saying, ‘Here are our instructions, and if you don’t follow them, you’ll be responsible.’” —Deborah Yellin
collaborate with industry to develop new regulations,” Yellin says. “More change is coming, and those active in the medical 3-D printing community should consider communicating with the FDA early and often to advocate for the best regulations possible.”

STOP, THIEVES

For a sense of what could go wrong in the new world of 3-D manufacturing, consider the so-called Four Thieves Vinegar Collective, which has posted blueprints for a 3-D-printed replica of a widely used allergy injection device and a 3-D-printed “lab” that can supposedly produce homemade versions of other popular drugs. The collective claims to be democratizing medical treatment, but experts and the FDA have warned that DIY drug making could be deadly.

Design files for drugs or devices are vulnerable to piracy just as music or video files are today, and drug or device makers may someday face a challenge similar to the one faced by entertainment companies starting in the 1990s. Unlike a leaked song, however, a leaked drug design file could ultimately result in injury or even death.

With value chains more broadly dispersed, companies will need to take stronger measures to ensure that intellectual property does not “leak” and that product quality is maintained. Yellin provides some guidelines:

■ Register for copyright (for design files) as well as patents (for other innovations) whenever possible.
■ Keep careful records of use and ownership during the R&D process.
■ Make strategic use of trade secrets. One way to make a stolen design file impossible to use is to keep details such as materials confidential.
■ Monitor the internet to ensure that design files are not being leaked.
■ Many companies may shift to licensing out their manufacturing and marketing. These firms will require “very stringent licensing agreements with very strict instructions and indemnities” to ensure that inferior products are not marketed under their names, Yellin says.

3-D printing and distributed manufacturing could disrupt the drug and device industries. New opportunities await companies that can adapt their business model and work within the new legal and regulatory landscape.

STOP, COLLABORATE, PRINT

Before 3-D printing can reshape the world of manufacturing, it needs to work through some key challenges.

One is ownership of essential technologies. The major players in smartphone technology have spent years and billions of dollars in epic litigation battles over patent royalties and damages. The major players in 3-D printing are determined to avoid these conflicts, says John Gibson, a partner in Crowell & Moring’s Antitrust Group and chair of the firm’s 3-D Printing Digital Transformation Working Group.

Gibson advises HP, the world’s leading 3-D-printer maker, on regulatory and standards issues. HP is a founding member of the 3MF Consortium, which is developing a modern, universal 3-D printing file format. The format will allow design applications to send full-fidelity 3-D models to virtually any printer or application. All consortium members have pledged to make the standard open-source or royalty-free. “To build this new ecosystem unburdened by some of the substantial legal disputes afflicting other technology ecosystems and platforms, we wanted to solicit broad input before full development and adoption,” Gibson says.

Another issue is the ease of making weapons on 3-D printers. The Texas group Defense Distributed has threatened to post digital blueprints for a 3-D-printed gun made of plastic parts that would evade a metal detector. Similar files may be available on underground sites.

The industry has begun collaborating on security efforts, Gibson says. One strategy is to design and share printer features that would prevent them from producing dangerous items. Gibson and other lawyers will advise to ensure that the collaboration takes place without triggering antitrust concerns.

The industry has also made overtures to the intelligence community about starting a dialogue so printer makers can learn more about—and be better equipped to address—threats for making 3-D-printable weaponry.

“We wanted to have a different way of thinking when setting up this ecosystem,” Gibson says. “Consumers, designers, materials suppliers, OEMs, and printer makers all win if we talk to each other ahead of time and figure out what’s best for the world, not just for each individual company.”
Congress has long had direct and indirect influence over the making, modification, and rescission of rules promulgated by federal agencies. The level and frequency of such influence have risen significantly in the Trump administration.

The most common exercise of direct congressional authority is the passage of laws that either explicitly order an agency to issue a rule and set specific parameters or requirements for the rule, provide more general rulemaking authority and discretion, or overturn an existing rule.

Until 2017, one of the most prominent recent instances occurred in 2014, when the Centers for Medicare & Medicaid Services (CMS) proposed a rule that would eliminate "protected status" for certain categories of drugs under Medicare Part D. Protection under Part D meant that Medicare was required to cover all drugs in these categories.

"Congress was outraged at the possibility that senior and disabled citizens might lose access to the drugs, which included critically needed antidepressants and antiseizure drugs, among others," notes Jim Flood, a Crowell & Moring partner and chair of the firm’s Government Affairs Group, who formerly served as a counsel to the Senate Judiciary Committee and as an assistant U.S. attorney. "The full Senate Finance Committee and a bipartisan group of two House committees wrote letters to CMS demanding withdrawal of the proposed rule. In response, CMS promptly turned tail and scrapped it."

THE CRA AS RULEMAKING AVENGER

Just three years later, Congress entered a new era of rulemaking influence with its unprecedented use of the Congressional Review Act. The CRA was passed in 1996 as a bipartisan measure enabling Congress to review and disapprove (i.e., overturn) agency-issued rules via an expedited legislative process. Once a rule is disapproved, the CRA prohibits reissuance of the rule in substantially similar form or issuance of a substantially similar rule unless the reissued or new rule is specifically authorized by a subsequently enacted law.

Prior to 2017, the CRA had successfully been invoked to disapprove a rule only once—in 2001, when Congress disapproved a workplace ergonomics rule issued by the Clinton administration. During the first two years of the Trump administration, by contrast, Congress pounced on the CRA as a means to undo regulations issued under Barack Obama.

Starting in early 2017, congressional Republicans took up this task with gusto, using the CRA to repeal 16 Obama-era rules such as a change to the Interior Department’s restriction on mining activities that can occur next to streams, the requirement that the Social Security Administration disclose information about mentally incapacitated people to agencies conducting background checks for gun purchases, and the Federal Communications Commission’s net neutrality rule.

In 2017, Congress began examining older executive branch actions such as guidance documents and interpretive rules that had not been submitted to Congress for review and had not been considered subject to the CRA’s expedited procedures. This is no small matter: A 2017 Brookings Institution study identified 348 federal rules with significant reporting deficiencies that could expose them to CRA disapproval.

Byron Brown, a senior counsel in Crowell & Moring’s Government Affairs and Environment & Natural Resources groups, who formerly served as a senior official in the Environmental Protection Agency and both houses of Congress, has seen firsthand how the Trump administration is more receptive to lobbying by both industry and Congress.

“At the beginning of the current administration, the White House put out a clear message that it was open for business..." Time-tested blocking and tackling ... could be more effective because of the administration’s interest in less rulemaking and more deregulation." —Jim Flood
and interested in hearing directly from the regulated community,” Brown says. “Not only does this mean more opportunities for direct lobbying than previously, but it also results in companies and other advocates increasingly engaging with their representatives and senators to help them articulate and make their cases through letters, appropriations language, and even holds on nominations.”

A prime example was the intense pressure exerted by Iowa Senators Charles Grassley and Joni Ernst and Texas Senator Ted Cruz over the Trump administration’s plans to reform the EPA’s Renewable Fuel Standard program. One idea would have reduced the amount of corn-based ethanol that oil refineries would be required to blend with gasoline, prompting Grassley to threaten to call for then-EPA Administrator Scott Pruitt’s resignation if the idea moved forward. It didn’t.

CAN’T WIN ‘EM ALL

Members of Congress and their constituents, of course, don’t always get what they want from regulatory agencies. Says Brown, “People are coming to agencies with wish lists of new, revised, or repealed rules without thinking through the probability or risks of litigation. They sometimes ask for actions that may be hard to defend in court. In these cases, even if a rule is administratively stayed or delayed as part of a reconsideration process, the agency and the affected industry may see only short-term relief as courts are becoming more aggressive in striking down these delay tactics.”

This scenario has unfolded most notably at the EPA and the Department of the Interior. New political appointees at the agencies agreed to delay or reconsider several Obama-era environmental regulations, resulting in some high-profile court losses that reinstated the old rules.

In one such decision, the Court of Appeals for the D.C. Circuit told government lawyers that the EPA’s rationale for delaying the Chemical Disaster Rule “makes a mockery” of the Clean Air Act. In another, a Northern District of California judge granted a bid by New Mexico and California for a preliminary injunction against an Interior rule. The judge called the reasoning behind the rule, which suspended a regulation aimed at reducing leaks of methane gas during oil production on federal land, “untethered to evidence,” among other criticisms.

Brown suggests that companies seeking regulatory relief before federal agencies may benefit from road-testing their ideas with outside counsel, who can help both to gauge the litigation risks and measure the political support that may be needed to help get the idea across the finish line and successfully through the courts.

MIDTERM ELECTION RESULTS WILL INCREASE SCRUTINY

The midterm elections produced a split Congress, with a new Democratic majority in the House of Representatives and a returning Republican majority in the Senate. Even before they took office, the anticipated new House committee chairs announced plans for aggressive oversight of Trump’s regulatory reform agenda, including the EPA’s new greenhouse gas regulations and chemical safety rules.

The expected uptick in oversight may cause agencies to divert limited resources away from work revising or repealing regulations in order to respond to congressional requests for information, and the eventual public disclosure of agency documents through this process may make it more difficult for agencies to defend their actions in court or before the public.

STRATEGIES FOR SUCCESS

How should organizations attempt to influence rule-making in today’s environment?

Crowell & Moring’s Jim Flood recommends an approach that combines legal, political, and publicity strategies. “While much of this is time-tested blocking and tackling,” he says, “it’s no less effective now than in the past. If anything, it could be more effective because of the administration’s interest in less rulemaking and more de-regulation.” He suggests companies consider these steps:

- Ask members of Congress and other interested parties to write letters to agency rulemakers.
- Develop and implement public relations strategies in selected markets and media.
- Talk to members of Congress during the appropriations process, and ask counsel to try to contribute language to the committee and conference reports that often accompany appropriations law.
- Use social media to amplify the voices of people affected by the proposed rule as well as to attract the attention of Congress and rulemakers.
IN SEARCH OF VALUE

The U.S. health care system’s efforts to incentivize “value”—i.e., achieving better patient outcomes at lower cost—have been too slow for the Trump administration to accept.

The federal government and the health care industry have tried for decades to pay for outcomes and improved health rather than volume of care. In a December 2018 multi-agency report headlined by the U.S. Department of Health and Human Services, the Department of Labor, and the Department of the Treasury, the administration blamed state and federal regulations that “inhibit adequate choice and competition” for the current state of affairs.

“Lawmakers and executive agencies under both Republican- and Democrat-led administrations want the transition to happen. Nonetheless, they continue to struggle to find common ground on the mechanics of cutting national health care expenditures without being seen as rationing care or stifling innovation,” says Stephanie Willis, a counsel in Crowell & Moring’s Health Care Group and a former attorney at the HHS Office of Counsel to the Inspector General.

With these conflicts unresolved, it’s no wonder the U.S. spends more than any nation on health care, whether measured as a percentage of the economy (a whopping 17.9 percent) or on a per capita basis ($9,892). (Both figures are for 2016.)

The pace of change may soon accelerate.

SOMETHING OLD AND SOMETHING NEW

The Trump administration is pursuing a dual approach of pressing some strategies dating back to earlier presidencies and proposing innovations to the regulatory landscape. In both cases, it’s acting aggressively to speed progress.

“A good example is financial incentives for value in the form of rewards and penalties, which have long been part of the health care regulatory regime,” says Troy Barsky, a partner in Crowell & Moring’s Health Care Group and a former senior official at HHS’s Centers for Medicare & Medicaid Services (CMS). “While the current administration continues to offer bonuses for desired outcomes, it’s placing more emphasis than previous administrations on downside risk, which means penalizing providers that don’t deliver value,” he says. “We expect a stronger push for the implementation of downside risk over the next couple years.”

One of the Trump administration’s top candidates for value-based reforms involves prescription drugs, many of which have seen dramatic price increases in recent years. Congress and the president frequently single out drug prices for disapproval and have been progressively taking more actions to achieve pricing transparency and payment reform. The president’s late October suggestion that Medicare pay for certain drugs based on their prices in other advanced industrial countries—where average prices are significantly lower, according to a new government study—appeared to be a trial balloon that faces heavy industry and political opposition.

Nevertheless, Willis notes, “The administration is heavily focused on using price transparency in a variety of forums to change the cost landscape for prescription drugs, such as in television ads, the 340B Drug Discount Program, and Medicare Part C and D benefits.”

Ironically, anti-fraud statutes specific to health care are now considered obstacles to achieving value. Foremost is a series of fraud and abuse laws designed to limit the ability of health care providers to refer patients to care-providing entities with which they have an ownership, investment, or other financial relationship—indicating potential conflicts of interest. These statutes have the unintended effect of dis-

“[Lawmakers] continue to struggle to find common ground on the mechanics of cutting national health care expenditures without being seen as rationing care or stifling innovation.” —Stephanie Willis
couraging an administration priority: coordination among individual health care providers and institutions, which could reduce costs and improve outcomes.

THE CHALLENGE OF PROMOTING COORDINATED CARE

HHS declared its intent to rectify the problem last June by launching the Regulatory Sprint to Coordinated Care, with the first of two requests for information. As the first request (which involved the physician self-referral law, also known as the Stark Law) put it, “Addressing unnecessary obstacles to coordinated care, real or perceived, caused by the physician self-referral law is one of CMS’s goals in this Regulatory Sprint.”

The second RFI came two months later and dealt with Section 1128B(b) of the Social Security Act, better known as the federal Anti-Kickback Statute (AKS). As with the Stark Law, there is some irony in efforts to revise the AKS, which imposes restrictions intended to protect federal health care program beneficiaries against overutilization, increased costs, and low-quality services—precisely the kinds of things that coordinated care could also prevent if certain requirements under the AKS were relaxed.

“The challenge of promoting coordinated care while complying with the Stark Law and the AKS is very real for health care players, whether they’re hospitals, insurers, physician groups, medical technology companies, or investors,” Barsky notes. “These players are strong advocates for the Regulatory Sprint and might even succeed in prodding Congress to address the challenge with new legislation in 2019.”

STATE VS. FEDERAL: THEY’RE JUST GETTING WARMED UP

The administration’s enthusiasm for deregulation isn’t always shared at the state level, particularly where government officials are concerned that such actions could make health care consumers more vulnerable. Some states that consider the administration’s business-friendly approach detrimental to patients and consumers have taken action against it. For example:

- Eleven states and the District of Columbia filed suit in the D.C. District Court last July to stop a Department of Labor rule that created association health plans. These plans were established to make health insurance more affordable to small businesses but were exempted from providing essential benefits mandated by the Affordable Care Act.
- Eighteen states and the District of Columbia brought suit in the Northern District of California against the Trump administration’s 2017 decision to stop making federal payments for insurer cost-sharing reductions that the ACA requires. The court dismissed the suit without prejudice in July.
- In August, HHS announced a new rule that loosened some of the restrictions on “skinny” health insurance plans, which offer limited coverage at low cost and are heavily circumscribed under the ACA. Several states have cracked down on sales practices associated with these policies.
- California enacted its Consumer Privacy Act in June. While the law is broad and not specifically directed at federal health care initiatives, it may enable consumers to limit health care providers’ access to certain medical data—which could hurt efforts to promote coordinated care.

“Our sense is that the state-versus-federal battles over health care issues are far from over,” says Barsky. “Ultimately, though, it’s clear that all parties are invested in making the system more value-driven. Value delivery should be a win-win for everyone involved.”

KEY POINTS

**Quantity over Quality**
The U.S. health care system is slowly shifting toward quality of care over quantity of treatment.

**Risk-Bearing Arrangements**
The Trump administration is aggressively pursuing risk-bearing strategies to push the system toward value-based reimbursement models.

**Coordinated Care Barriers**
Anti-fraud laws effectively discourage the coordination of care among individual health care providers and institutions.
INSURANCE/REINSURANCE

NAVIGATING INSURTECH REGULATION WITHOUT A MAP

InsurTech—the innovative use of technology in insurance—is leaving the station and pulling the industry forward at a rapid clip. Insurers that don’t jump on board soon will find themselves at a distinct competitive disadvantage: According to PwC’s 21st CEO Survey, 85 percent of insurance CEOs believe that the speed of technological change is threatening their company’s growth prospects.

A parallel sense of urgency is pushing state insurance regulators, which are legally required to provide a vibrant marketplace for insurers and consumers. Since facilitating technological innovation is part and parcel of this mission, regulators are looking for ways to enable insurers to test InsurTech initiatives that don’t clearly fall under existing laws. Forward-looking states are competing with each other for first-mover advantage.

Looking ahead, the challenge for insurers and their tech and financial partners is twofold. In addition to making successful business ventures, they must work with regulators to chart currently uncharted territory. “Companies have to determine if they can win as the regulatory environment takes shape,” says Laura Foggan, who heads Crowell & Moring’s Insurance/Reinsurance Group. “Constructive dialogue with regulators can only help them get where they want to go.”

HIGH POTENTIAL LEADS TO DEAL FEVER

InsurTech encompasses a host of technological innovations, including Big Data/advanced analytics, artificial intelligence, the Internet of Things, machine learning, blockchain, telematics, software as a service, and more. The industry is actively pursuing all of these, both to address existing issues and to identify new opportunities in a variety of areas: underwriting, product development, distribution, pricing, policy customization, sales and marketing administration, regulatory reporting and compliance, claims processing, customer service, and fraud.

The mounting pace of InsurTech deal activity reflects the industry’s excitement about a brighter future as well as expectations that the future is approaching quickly. As Willis Towers Watson reports in its Quarterly InsurTech Briefing Q3 2018:

- There were 194 InsurTech transactions in the first three quarters of 2018, the highest such total in any year to date.
- The number of private technology investments made by insurers or reinsurers also hit its highest first-three-quarters level (67 deals) in the same period.

NO U.S. SANDBOX FOR INSURTECH—YET

One promising approach for regulating InsurTech is a flexible “regulatory sandbox” structure that encourages experimentation while allowing states to oversee and evaluate what companies are trying to do. The “regulatory sandbox” concept proposes a reasonable degree of regulatory flexibility, as exemplified by enforcement safe harbors such as variances, waivers, and no-action letters, combined with continued regulator focus on maintaining consumer protection and risk mitigation.

While regulatory sandboxes for InsurTech innovations have seen widespread acceptance in other jurisdictions—particularly in Asia and Europe—the U.S. lags behind in approval of regulatory sandboxes for insurance. In fact, in some states, regulators have expressed concern that there may be a need for greater oversight arising from the use of new technology by insurers, rather than regulatory flexibility to encourage InsurTech innovation. For instance, New York’s Department of Financial Regulation recently issued Insurance Circular Letter No. 1, to advise insurers in New York of their statutory obligations regarding the use of algorithms and predictive models in life insurance underwriting. The department expressed concerns about the potential for negative impact on

“Companies have to determine if they can win as the regulatory environment takes shape. Constructive dialogue with regulators can only help them get where they want to go.”

—Laura Foggan
consumers from possible inappropriate use of algorithms and predictive models, while also acknowledging that innovation and the use of technology has the potential to benefit insurers and consumers alike.

Generally, state regulators in the U.S. have noted that increased insurer use of technology may lead to new insurance products, better customer service for consumers, and increased efficiency for insurers, while simultaneously expressing concerns about issues such as data privacy and discriminatory impact or bias in data sets. “It will be interesting to see whether regulatory sandboxes for insurers finally gain traction in 2019 or state regulators find other ways to promote innovation,” says Foggan.

HOW TO NAVIGATE AN EVOLVING REGULATORY REGIME

So the state of play for InsurTech regulation entering 2019 is evolving but as yet officially unchanged. How can industry players navigate a path forward when there’s no map?

“The industry and its regulators are on the same side,” says Foggan. “Both want InsurTech to succeed, and they know they have to figure it out together. This could help the process move faster and with a solid base of mutual understanding.”

The first step is for insurers and tech providers to coordinate their efforts in cooperative ventures that will secure regulatory approval, including through mergers, acquisitions, or joint ventures. Seasoned counsel with experience in technology and intellectual property matters can ease the way for acquisitive insurers, just as insurance-savvy counsel can give tech providers a clear picture of the specific regulatory hurdles that insurers face.

Companies that are developing InsurTech initiatives are advised to meet with their regulators to educate them about the technologies involved. Foggan notes: “Regulators know they need to be educated about the technologies they’re being asked to regulate, and they often don’t have the staff, budget, or internal expertise to do it themselves. In this context, the potential benefits for both sides are significant. Industry players that can bring regulators up to speed are doing more than improving their own odds of getting a regulatory green light—they’re also helping the states get a regulatory jump on other states.”

LLOYD’S OF LONDON: ILLUSTRATION OF AN INSURTECH INCUBATOR

Lloyd’s of London, the world’s largest market for specialist insurance and reinsurance, has put its own spin on the concept of the InsurTech sandbox.

Lloyd’s Lab is a 10-week program in which 10 competitively chosen InsurTech developers work to create solutions for challenges faced by the Lloyd’s market in four areas: enhancing the customer experience, building a relationship-driven culture, powering data-driven underwriting, and creating smart insurance products.

Lloyd’s is offering a unique opportunity to test new products and ideas, says Mark Meyer, a partner in Crowell & Moring’s Insurance/Reinsurance Group and leader of the firm’s European insurance practice, but it still has to pass muster with one of the world’s most advanced InsurTech regulatory regimes.

“In the UK, insurance is governed by two jurisdictions,” notes Meyer, who advises insurers as well as brokers. “First there is the UK via the Financial Conduct Authority (FCA), which recognized InsurTech’s potential to transform the insurance business years before its counterparts elsewhere. FCA launched its own InsurTech regulatory sandbox in 2014. There also is the European Union, which is playing catch-up but is working toward setting up its own sandbox.”

Meyer cites a synopsis of key insurance policy terms as an example of how InsurTech can help with regulatory compliance. The EU mandates this plain-language synopsis so that policyholders can better understand their coverage. The trick is to automate the production of synopses, which must be customized for each policy. InsurTech’s focus on artificial intelligence, machine learning, and advanced analytics can make this process much faster and cheaper as it meets regulatory requirements.

The specter of Brexit also looms large. “While no one yet knows how Brexit will affect insurance regulation in the UK,” says Meyer, “the industry is monitoring developments closely and will adjust as needed.”
Among federal regulatory regimes, few cry out for improvement as much as the environmental review process mandated by the National Environmental Policy Act of 1969 (NEPA). The Trump administration has taken major steps to make the process less burdensome and more efficient. Whether these steps succeed going forward is an open question, though, with federal courts most likely to have the final say.

NEPA requires federal agencies that grant approvals for development projects—infrastructure such as highways, bridges, and power plants, as well as commercial, industrial, mineral, and oil and gas—to determine whether a project will have a significant environmental impact. If this determination is positive, the agency must prepare a detailed analysis known as an environmental impact statement (EIS).

The problem is that implementing NEPA has become complex, long, and costly, with extended delays common. A permit review, for example, typically takes five to seven years (and sometimes 10 or more), while an EIS has many moving parts and often costs $2 million to $3 million. The Empire State Building, which opened in 1931, by contrast, was completed in just one year and 45 days.

But that’s not all: Once a project is approved, it’s usually challenged in federal court. Cases can last three to four years, meaning that the project developer must be prepared to spend millions and often wait at least a decade before breaking ground—and that’s if the challenge is rejected. And if the project actually survives this gauntlet, the sheer passage of so much time could jeopardize its financing or render it out of sync with changing market conditions.

The Trump administration has acted aggressively to streamline the NEPA process and reduce its complexity.

Regardless of one’s political views, it’s hard to dispute that this is a desirable goal.

“I’m hard-pressed to think of another administration in the last 40 years as focused on fixing the NEPA approval process,” says R. Timothy McCrum, a partner in Crowell & Moring’s Environment & Natural Resources Group and a former attorney-advisor with the Energy and Resources Division of the Solicitor’s Office at the U.S. Department of the Interior. “Cutting the time and costs of a NEPA review is something everyone should agree on.”

EXECUTIVE ORDER 13807: THE NEW PLAYBOOK

On August 15, 2017, the president issued Executive Order 13807, the first in a series of major steps taken by the administration to streamline the NEPA process.

The order laid out how the administration intended to bring greater rigor to the process, specifically for infrastructure. Among its key directives:

- Establishing a “One Federal Decision” system in which a designated federal agency leads an infrastructure project through the process and coordinates the participation of the other agencies involved. Once the lead agency issues a centralized Record of Decision that includes the decisions of all agencies, all authorization decisions must be completed within 90 days.
- Slashing the time for reviews and authorizations to not more than an average of approximately two years.
- Creating a performance accountability process to track major infrastructure projects.

TRENDS TO WATCH

McCrum expects several NEPA trends to play out starting

“Because most federal agency leaders are committed to implementing Trump’s agenda, they’ll succeed in reducing approval times. We’re already seeing indications of this at the Department of the Interior.” —Timothy McCrum
in 2019 and, given the amount of time even an expedited process should consume, in subsequent years.

**Shorter approval times.** In McCrum’s experience, the most important factor in obtaining agency approval of a project is the agency’s level of commitment to the project—the stronger the commitment, the more likely the approval. “Because most federal agency leaders are committed to implementing Trump’s agenda, they’ll succeed in reducing approval times,” he says. “We’re already seeing indications of this at the Department of the Interior, where the commitment runs very high.”

The caveat, of course, is that the threat of anti-project litigation is as great as ever. Project developers can help reduce this threat in two ways. First, they should engage outside counsel experienced in working with agencies and planning for potential litigation. Second, they should make it a point during the review process to emphasize their project’s economic benefits in terms of jobs created, spending generated, taxes raised, etc.

**Turning a traditional argument on its head.** Agencies have often rationalized their long review times in part by saying that they strive to make the environmental impact statement as litigation-proof as possible. Skeptics see this as a convenient excuse for bureaucratic foot-dragging.

McCrum believes that project opponents will use this rationale against the agencies as approval times shorten. “They can go to court and say that because the agency rushed the review in its eagerness to meet the administration’s guidelines, it failed to subject the project to an appropriate level of scrutiny. If courts agree, they could force the administration to backtrack, on the flimsy—but-historical premise that being thorough means taking longer.”

This scenario, he adds, highlights the necessity for project supporters to work closely with agencies to build a robust case for project approval.

**Increased litigation.** While the administration may well succeed in accelerating NEPA reviews, its efforts will likely compel project opponents—particularly non-governmental organizations, which are skeptical of NEPA reform—to litigate more frequently and aggressively.

“Thousands of administrative appeals and federal court judicial review actions have been brought under NEPA since the law took effect in 1970,” McCrum says, “and there’s no reason to expect the volume of these challenges to decline. Federal courts will ultimately decide whether the administration’s efforts prevail.”

State courts will weigh in, as well, most probably in California, whose Environmental Quality Act is the nation’s toughest state-level NEPA equivalent. Richard McNeil, a partner in Crowell & Moring’s Environment & Natural Resources Group, notes, “There’s certainly a sense among many California NGOs that they have a heightened obligation to challenge Trump’s environmental policies. If the federal government won’t protect the environment, this thinking goes, then challenges brought under state laws may be necessary to fill the void.”

---

**IT’S DIFFERENT IN CALIFORNIA**

While several states have their own equivalents to the National Environmental Policy Act, California’s stands out for its wider scope and stricter standards.

The California Environmental Quality Act mandates that every state and local agency action (including approvals of private-party development) adequately consider environmental protection. CEQA applies to all public actions (i.e., not just public projects), and requires state and local agencies to adopt all feasible mitigation measures to reduce or eliminate the environmental impacts of proposed projects—a step not required of federal agencies under NEPA.

“Because of CEQA, project developers must play by two different sets of rules in California,” says Crowell & Moring’s Richard McNeil. “The outcome of CEQA review could be very different from the outcome of NEPA review of the same project, which can cause big headaches. And opponents of projects could bring simultaneous litigation in federal and state courts, where cases can have very different lengths and results.”

The Trump administration’s efforts to streamline environmental reviews may have met its match in California, McNeil adds. “Given the extent of CEQA’s procedural requirements and the state’s pro-environment stance, there’ll be a limit to how successful federal streamlining can be in moving forward proposed projects subject to both NEPA and CEQA.”
It’s often said that there is opportunity in uncertainty. This is currently the case in the world of corporate taxation, where the Tax Cuts and Jobs Act of 2017 has created much confusion—and provided an opening for companies that aggressively pursue regulatory endorsement of their tax strategies. The TCJA is the most sweeping tax legislation since the Tax Reform Act of 1986. It significantly reduces the income tax rate for corporations, and it makes major changes related to the taxation of foreign income.

While it’s normal for tax laws—which are notoriously dense and arcane—to require clarification in the form of regulatory guidance, the TCJA stands out for its opacity. It was written largely by congressional Republicans behind closed doors, without any public hearings, and with considerable direct input from the business community. The rushed result was nearly 1,100 pages that many senators were unable to fully read and assess before the final vote. There were numerous typos, drafting errors, and provisions that raised more questions than they answered.

To date, the Internal Revenue Service has issued more than 150 guidance documents for the TCJA. Tax professionals say that this is only the beginning of what will ultimately be a mountain of guidance.

“WE’LL GET BACK TO YOU”

For an example of why guidance is necessary, look no further than section 451(b) of the Internal Revenue Code, which concerns revenue recognition and was established by the TCJA. Section 451(b) requires that companies using the accrual method of accounting (under which revenue can be recognized as income for taxation in a year different from the one in which it is received) recognize revenue no later than when it’s included in their financial reporting.

Sounds straightforward, right? According to Dwight Mersereau, a partner in Crowell & Moring’s Tax Group and a former advisor in the IRS’s Office of Chief Counsel, it isn’t. “Section 451(b) replaces the rule for timing of accrual revenue recognition that had been in place since 1939,” he says. “This seemingly simple provision has raised numerous questions from taxpayers trying to understand its requirements, such as whether ‘gains’ should be treated as ‘revenue.’ Other questions arise from taxpayers seeking relief from a literal reading of the statute, which could be interpreted as requiring a taxpayer to include an amount in income before the taxpayer has realized the income, such as when the taxpayer holds a security that has increased in value but hasn’t sold the security. In other words, section 451(b) cries out for clarification—like so much else in the TCJA.”

A major question raised by section 451(b) concerns changing a company’s method of accounting, i.e., from accrual to cash or vice versa. Companies that used accrual under pre-TCJA law must change their method to comply with the TCJA. As Mersereau explains it, “If companies want to change their method—which is a big deal—they need permission from the IRS commissioner. The problem is that the TCJA isn’t clear about how to get this permission, and the IRS hasn’t yet provided guidance, which can leave companies in accounting limbo.”

POSSIBLE TIME SQUEEZE IN FILING RETURNS

Another timing issue concerns the filing of corporate tax returns for calendar-year filers. Returns are due to the IRS by the following April 15, and many companies typically take advantage of the option for an extension of the deadline to October 15.
But the process for 2018 returns takes on added urgency as a result of the TCJA, notes Charles Hwang, a partner in Crowell & Moring’s Tax Group.

“It’s standard for companies to rely on IRS guidance in order to properly prepare their returns,” Hwang says. “And because preparing returns is complex and labor-intensive, they need these comments well ahead of when the returns are due. Since the TCJA is so confusing and there’s still a lot of guidance that hasn’t come out yet, more companies might find themselves in a time squeeze to file even by October 15.”

Hwang adds that while corporate tax departments and CFOs are well aware of this possibility, it might be news to general counsel and other senior executives. “Tax departments and outside counsel should make sure to alert GCs about this,” he says. “The increase in uncertainty may require additional resources or budget as well as SEC disclosure of certain issues.”

The IRS itself may also be an issue in the filing process. Congress has slashed the agency’s funding and staffing levels in recent years, including the imposition of a hiring freeze that started in 2010. So, at a time when taxpayers badly need IRS guidance to navigate the TCJA and properly file their returns, the agency is ill-equipped to handle the huge volume of inquiries that will come its way as filing deadlines approach.

There’s some cause for optimism in this regard, as Congress appropriated $320 million in early 2018 to help the IRS address the new law, with much of it presumably to be used for additional hires. But observers point out that the IRS has said it will need $495 million over two years to implement the TCJA, meaning it’s been given only 65 percent of the money to do 100 percent of the work (see chart).

THE BOTTOM LINE: GET INVOLVED EARLY AND OFTEN

Mersereau and Hwang are urging organizations to be both proactive and persistent in engaging with the IRS and Treasury Department to address their TCJA questions. Squeaky wheels will get the grease, they say.

Many organizations already have embraced this approach, as there are numerous instances of companies using private meetings and/or public gatherings to raise issues that the IRS hadn’t thought of.

The following are specific steps companies can take to ensure that regulators are fully informed of their concerns:

- Meet directly, one on one, with the IRS and Treasury.
- Submit written comments in response to IRS and Treasury requests for feedback. Both entities encourage such comments and are eager to receive them.
- Participate in public hearings on TCJA-related topics. The IRS and Treasury welcome this, as well.
- “Play defense as well as offense” by monitoring guidance issued to other companies to see whether such guidance is relevant.

“Getting in front of the IRS and Treasury can only help companies get in front of their tax concerns,” says Mersereau. “Considering that millions or even billions are riding on regulatory interpretations, it’s critical that companies do everything they can to engage and communicate.”
ANTITRUST

ANTITRUST ENFORCEMENT POLICY FOR BIG DATA?
STAY TUNED.

What, exactly, is Big Data? Rather than referring to a particular industry or amount of information, it’s about how firms that interact with consumers and other businesses use technology to aggregate data and extract value from it to create or enhance products and services.

The importance of Big Data to both businesses and consumers is surging. It has attracted particular attention in the antitrust world, where enforcement authorities are wrestling with growing concerns about how collecting and controlling Big Data may affect competition. As they review mergers and acquisitions—and assess the conduct of high-tech firms with troves of data—regulators are increasingly focusing on whether Big Data could be a barrier to entry, inhibit innovation, or enable large firms to stymie competition.

European competition authorities have taken an aggressive approach to antitrust issues that revolve around data, opening several investigations and industry inquiries. But their U.S. counterparts, the Department of Justice and the Federal Trade Commission, are acting more cautiously. All around the globe, antitrust authorities are confronting two fundamental issues:

1. Are existing laws sufficient to address concerns with Big Data, or do regulators need new tools (i.e., laws, regulations, economic models, and technical expertise)?
2. How should they pursue Big Data enforcement when their policies aren’t yet clearly defined?

As in previous periods of rapid, disruptive innovation, a debate has broken out about the adequacy of antitrust principles to tackle new competition issues. Some say enforcement authorities are playing catch-up instead of setting the pace.

This year could be the year in which this changes. Or not. “The U.S. antitrust agencies haven’t brought a case alleging that a firm’s mere acquisition or use of data constitutes an antitrust violation,” says Alexis Gilman, a partner in Crowell & Moring’s Antitrust Group, who formerly served as assistant director of the Mergers IV Division in the FTC’s Bureau of Competition. “That said, we know that Big Data issues are very much on the minds of officials at the DOJ, the FTC, and other antitrust authorities—their public comments make that clear. But we don’t know when this attention to Big Data issues might turn into enforcement action.”

IT’S ALL ABOUT DATA COLLECTION, USAGE, AND CONTROL

While the head of the DOJ’s Antitrust Division has expressed confidence that existing antitrust laws can address any competition issues raised by Big Data, the FTC is taking a more open-minded stance and working methodically to fashion its own view (see sidebar). The centerpiece of this assessment is a series of public hearings collectively titled “Hearings on Competition and Consumer Protection in the 21st Century.”

There have been nine hearings since last September, with more scheduled for 2019. More than half of them have addressed data, technology, and related issues in the context of competition or consumer privacy.

One of the hearings featured a presentation by a deputy director in the FTC’s Bureau of Competition that summed up some key questions about data in competition analysis:

- Is the data unique? What other sources are available at similar cost? Is it difficult or costly to replicate, or are there other barriers to replication?
- Data is often combined with analytics to make information useful in a business setting. How does this affect competition?
- Do incumbents have a data advantage?
- Current antitrust analysis accounts for how companies

“Companies considering transactions with a significant data component should be prepared for increased scrutiny—even while the agencies’ enforcement policy in this area evolves—and be prepared to address agency concerns.” —Alexis Gilman
compete using data as a product or input, or as a tool for making decisions. This may present additional complexity if data is proprietary or subject to intellectual property protection.

- Data sets can be highly differentiated; non-price factors of competition such as quality and innovation are important.

Ultimately, notes Andrew Gavil, a senior counsel in Crowell & Moring’s Antitrust Group and former director of the Office of Policy Planning at the FTC, data enforcement boils down to three things. “Antitrust thinking should concentrate on how data is collected, used, and controlled,” he says.

“Some critics,” Gavil adds, “are challenging the historical approach to enforcement, which focuses on competition in narrowly defined markets for products and services, arguing that it may be missing the mark in some of today’s evolving markets. We’ll be watching to see if—and, if so, how—antitrust enforcers respond to these challenges.”

A FOGGY FORECAST

The vigorous discourse on the ability of antitrust agencies to address Big Data competition issues is likely to intensify. Combined with factors such as potentially different approaches by the DOJ and the FTC and by European and U.S. antitrust authorities, continuous technological and business-model innovation, and political considerations, this suggests that tackling Big Data competition issues could take unanticipated twists and turns in 2019. Against this backdrop, Gilman and Gavil see a number of potential developments:

- The FTC might use its hearings to help it generate new policy papers, guidance documents, and enforcement priorities that indicate how its thinking is changing.
- Even if the DOJ and the FTC take little or no action to step up enforcement directed at Big Data, state attorneys general—who have the authority to enforce state and (in some cases) federal antitrust laws—may undertake their own investigations and enforcement actions. They’ve already begun to do so.
- With Democrats taking control of the House of Representatives, the new chair of the House Judiciary subcommittee covering antitrust has signaled plans to conduct further hearings targeting large technology companies, which will keep the pressure on the antitrust agencies to address any perceived enforcement gaps. But with control of Congress divided, prospects for the passage of new legislation are murky.
- European regulators will likely press ahead in their efforts to rein in the data-driven practices of the tech giants and, in the process, push the boundaries of antitrust enforcement.

“Regardless of what happens,” Gilman says, “companies considering transactions with a significant data component should be prepared for increased scrutiny—even while the agencies’ enforcement policy in this area evolves—and be prepared to address agency concerns.”

DOJ AND FTC: TWO AGENCIES, TWO VIEWS?

There’s lively debate in the antitrust community about whether current antitrust laws and enforcement policies sufficiently address Big Data-related competition concerns. Adding to the uncertainty are the different tacks taken by the DOJ and the FTC. The agencies’ dissimilar institutional structures amplify this uncertainty.

The DOJ speaks with one voice—that of Makan Delrahim, head of the Antitrust Division. Delrahim has aggressively advocated the view that existing antitrust laws are flexible enough to handle the issues of the digital age.

The FTC’s view is still developing, primarily because the agency has five recently appointed commissioners who don’t necessarily agree with each other (or with the DOJ) but generally try to operate by bipartisan consensus. In addition, FTC Chair Joseph Simons is using the agency’s “Hearings on Competition and Consumer Protection in the 21st Century” to gather evidence and consider all arguments before taking any hard-and-fast positions that might include pursuing a new enforcement approach.

“Visibility into the government’s antitrust thinking will remain low until the agencies reveal their preferences through concrete policy statements and enforcement decisions—especially new cases and case settlements—and, possibly, closing statements that explain their reasoning,” notes Crowell & Moring’s Andrew Gavil. “For now, although there’s uncertainty, it seems unlikely that the agencies will pursue any radically different policies, despite continued debate and political pressure.”
Successful businesses anticipate and embrace change. In the 40 years since Crowell & Moring opened its doors, that kind of forward-thinking strategy has perhaps never been more challenging. The pace of technological change has revolutionized commerce and industry, and those charged with developing and enforcing regulations have struggled to keep up. An increasing emphasis on global trade has been met with a shift in regulations across borders that have had an impact on all aspects of business, from data to supply chains. This has been complicated by tariffs, sanctions, and other geopolitical tensions. The result, as documented in this Regulatory Forecast, is that businesses need regulatory strategies that are as nimble as they are forward-thinking, enabling them to chart a course when the routes they're traveling are less predictable than ever. For 40 years, we’ve partnered with you to help you plan those routes and move your businesses forward. We look forward to working with you to find solutions that will prove best for you in the years ahead.

—Philip Inglia
Chair, Crowell & Moring

CROWELL & MORING'S LITIGATION FORECAST

As a companion piece to the Regulatory Forecast, Crowell & Moring has produced the Litigation Forecast. This year’s volume includes not only a look at the impact of technology on litigation case strategy, but also coverage of trends in a range of practice areas and specific industries. For an electronic version, go to crowell.com/litigationforecast.