REGULATORY FORECAST 2018

WHAT CORPORATE COUNSEL NEED TO KNOW FOR THE COMING YEAR

BLOCKCHAIN: PROGRESS AND PROMISE

NATURAL DISASTERS: DEALING WITH THE NEW NORMAL

DIGITAL TRANSFORMATION: THE SKY'S THE LIMIT

TECHNOLOGY IS HELPING COMPANIES SOAR TO NEW HEIGHTS. HOW CAN REGULATION HELP THESE COMPANIES TO SUCCEED?

crowell moring

REGULATORY FORECAST 2018

Technology and Regulation in the Trump Era

DAN WOLFF

RICHARD LEHFELDT

The theme of last year's *Regulatory Forecast* essentially wrote itself: 100 days after a watershed election, we pulled out our crystal balls to wonder how President Trump might translate Candidate Trump's deregulatory fervor into concrete actions. The verdict: the chief executive had considerable but finite leeway to undo many of the later regulatory actions of his predecessor, but would ultimately grapple with some material, practical, and legal constraints, such as the other two branches of government and the Administrative Procedure Act. And sure enough, many of Washington's political and legal conventions have begun to impose themselves on this administration, even if unconventionally so.

This year's *Regulatory Forecast* focuses on technology and regulation. The nation is in a prolonged and inspirational technological explosion that outpaces the more deliberate timelines of the regulatory process. Deregulation, where feasible, can remove some roadblocks to innovation. But innovators also need rules of the road to circumscribe risk, ensure compliance, and at times seek the helping hand of government to nurture emerging technologies. Achieving the right balance between entrepreneurship and regulation allows both nations and corporations to compete.

We reiterate the plea and challenge we made last year: don't be scared of Washington; engage in the regulatory process. As co-editors of this book and co-chairs of Crowell & Moring's Administrative Law & Regulatory Practice, we urge you to take seriously the challenges and opportunities available in this still very new world.

—Dan Wolff
and Richard Lehfeldt

FOCUS AREAS

COVER: GETTY IMAGES

GETTY IMAGES

A Corporate Call to Action

Digital technologies are suddenly driving the future of business and corporate strategy across industry sectors worldwide. For many in government, these technologies are requiring a rethinking of regulatory philosophies, rules, and priorities. The mission in Washington and other world regulatory centers is to juggle competing interests smartly—to enable innovation, not impede prosperity, spell out well-understood law, and protect consumers.

The opportunity this presents to forward-leaning companies is considerable. Digital innovation proceeds at breakneck speed, and regulators recognize the need to act to keep pace.

The doors in Washington are open for industry to collaborate with government to ensure that each learns from the other, enabling innovation and regulation to move forward in lockstep.

The theme of this *Forecast*'s cover story, and indeed of the entire publication, is a call to action. We take a look at key developments across industries and agencies to identify both challenges and opportunities ahead in 2018. Along the way, we identify regulatory minefields to avoid and actions to be taken, as businesses seek to master their digital destinies.

We hope you'll find this year's edition useful as you raise your voice and champion the interests of both your company and your people. For more information, please reach out to us at www.crowell.com.

—Scott L. Winkelman
Management Board Member and Regulatory Department Chair, Crowell & Moring

CROWELL & MORING LLP

Co-Editor Dan Wolff
Co-Editor Richard Lehfeldt
Project Manager Tricia Wyse
Contributing Editor Nicole Quigley

LEVERAGE MEDIA LLC

Editorial Director Michael Winkleman
Art Director Carole Erger-Fass
Writers David Craig, Peter Haapaniemi
Chartist Alex Reardon
Copyeditor Sue Khodarahmi
Proofreader Jerry Goodbody
Project Manager Andrea Olstein
Production Manager Rosemary P. Sullivan

crowell moring

STATE OF PLAY

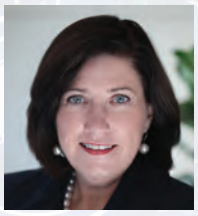
DIGITAL TRANSFORMATION: THE SKY'S THE LIMIT

Technology is helping companies soar to new heights. How can regulation help these companies to succeed?

The digital revolution has arrived. Cars are becoming computers on wheels. 3D printing is producing everything from medical devices to industrial machinery to consumer goods. Advances such as artificial intelligence are changing the way patients seek treatment. Banks and other financial institutions are forging ahead with new technologies such as blockchain. Technologies ranging from the cloud to mobile devices, embedded sensors, and the Internet of Things are being used to create new products and services, rethink existing processes, and develop new business models. According to a report from the World Economic Forum, digital technology "can be applied consistently at all levels of business and government to help unlock the estimated $100 trillion of value that digitalization could create over the next decade."

Almost every industry is looking to digital technology to provide a competitive edge. "Business executives see technology as key to innovation, and they will tell you that technological change is creating a 'disrupt or be disrupted' environment," says Cheryl Falvey, a Crowell & Moring partner and former general counsel of the Consumer Product Safety Commission. "Companies are working to understand where they fit in this space and what they need to do to take advantage of the value that's on the table."

Just how that all plays out will be determined in large part by regulation. Creativity and new technologies are critical, of course, but innovation and its impact on business will be shaped by government rules. Often, regulators do not yet have these rules in place, and that creates uncertainty for innovators. "If we wake up and find out down the road about a regulatory limitation we weren't anticipating, it can have a serious impact on business," Falvey says. "The White House has said it wants to achieve a regulatory framework that will enable innovation. Right now,



"COMPANIES HAVE AN OPPORTUNITY TO ENGAGE WITH REGULATORS AND HELP SHAPE THE DIGITAL TRANSFORMATION FOR YEARS TO COME."

—CHERYL FALVEY

GETTY IMAGES

"THERE'S A COMPETITIVE RACE TO SEE WHICH REGULATORS AND ENFORCERS ARE GOING TO BE FIRST IN ANSWERING THESE QUESTIONS, AND WHICH WILL LAG BEHIND."

—SCOTT WINKELMAN

companies have an opportunity to engage with regulators and help shape the digital transformation for years to come."

By understanding how regulators are thinking about this changing landscape—and by having a voice in the process—companies can drive their own digital destinies.

THE REGULATORY CHALLENGE

Regulation often lags behind technological development, and this is truer than ever given the dizzying pace of digital innovation. But that does not mean regulators are necessarily a barrier to innovation. "Most of them are trying to be helpful and provide guidance, but they are also trying to stay fairly high level with that guidance in order to let manufacturers innovate," says Falvey. "They know that if they get too prescriptive, it could hamper or stifle innovation."

Regulators find themselves needing to strike this balance on a number of fronts. For instance, the FDA is overseeing regulations for 3D printing of medical devices, the DOT is embracing a "tech-neutral" approach to autonomous driving, and the FAA and the White House are looking for the right balance for unmanned aircraft system (UAS) regulation, says Scott Winkelman, chair of Crowell & Moring's Mass Tort, Product, and Consumer Litigation Group. Some digital technologies are familiar to regulators, but others are not—and these can present new regulatory challenges. Winkelman points to blockchain and distributed ledger technologies, for example, which are steadily gaining traction in the financial services industry for securely conducting transactions and forming agreements. However, he says, "blockchain technology has applications in many industries, and there is really no mechanism out there as yet for comprehensively regulating distributed non-centralized contracts." As government bodies worldwide work through such issues, he adds, "there's a competitive race to see which regulators and enforcers are going to be first in answering these questions, and which will lag behind. With lag comes uncertainty, which helps no one. Agencies are at work seeking to carve out their jurisdictional territories and their regulatory philosophies in these evolving areas."

Several states have joined that race, and even taken the lead in regulating technology-based innovations. Some now regulate the use of drones, with law enforcement and others prohibiting their use to violate privacy, observe critical infrastructure, or interfere with hunters. Now the federal government is starting to push back on localized regulations. "States understandably want some say over their local airspace, while the FAA equally understandably resists a patchwork of regulations," says Winkelman. "These age-old federalism clashes are now playing out across digital arenas."

With this evolving landscape, says Winkelman, "astute companies are seeking a seat at the table in helping regulators confront the uncertainties that innovation presents. Government is having to address a hilly landscape, with regulations varying across geographies, and with some of their own regulations not adapting naturally to new technologies. That's going to be a real challenge for enforcers, but also for corporate compliance programs and regulatory functions. Industry will need to move quickly to determine whether it prefers the uniformity of federal preemptive regulation to the diversity of differing, and often conflicting, state regulatory regimes."

SELF-DRIVING CARS AND THE AGE OF "REGULATORY HUMILITY"

This complex interplay of corporate and regulatory philosophies can be seen in one of today's most prominent disruptive technologies. "The autonomous vehicle is really a meeting place of many different technologies and regulatory issues," says Kate Growley, a counsel at Crowell & Moring and a member of the firm's Privacy & Cybersecurity Group. "Many of the discrete technology capabilities that are part of the digital economy come together in these vehicles—things like 3D-printed parts, connected sensors, artificial intelligence to make driving decisions, and so on." Moreover, she notes, "We are even seeing car manufacturers focusing on health care, where a car can monitor health indicators, such as blood pressure or heart rate, which raises new legal and regulatory issues."

With the swirling change associated with the driverless car, a range of regulators are showing interest. In June 2017, the National Highway Traffic Safety Administration and the Federal Trade Commission held a joint meeting to explore the impact of autonomous vehicles. The then-acting chair of the FTC told the attendees that the commission intended to practice "regulatory humility" with regard to autonomous vehicles, adding that the FTC and other agencies should work together "to avoid unnecessary or duplicative regulation that could slow or stop innovation,

and ultimately leave consumers worse off."

In September 2017, the Department of Transportation and NHTSA released new voluntary guidelines for autonomous vehicles, which included 15 best practices for designing, developing, and testing them. These guidelines were seen by many as innovation-friendly. The DOT more recently announced that it plans to release yet another update in 2018—a clear sign of continued interest and momentum. "Regulators have wisely made clear that they are for autonomous vehicles," says Growley. "They want this to work for industry, for consumers, and for the U.S. economy more broadly—but they want it to work safely."

States have also passed laws on autonomous vehicles, filling in for what they perceive to be years of federal inaction. Since 2012, 41 states have considered legislation relating to autonomous vehicles. Twenty-one now have such laws, and five governors have issued executive orders on the point.

With varying state laws comes uncertainty among innovators—one reason the feds are stepping up. In September 2017, the U.S. House of Representatives passed, by unanimous vote, the bipartisan Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution Act (SELF DRIVE). That same month, a similar bill was introduced in the Senate. While no law has yet been enacted, both bills take a relatively permissive approach to regulating autonomous cars (heavy trucks were not included) and streamlining the testing of such vehicles. At the same time, both assert the federal government's authority in this arena. The Senate version, for example, would block state and local governments from creating regulatory barriers for autonomous vehicles while permitting states to regulate such matters as insurance and licensing, but not vehicle performance.

"While companies are getting some guidance, regulatory uncertainty can cause an anxious void

INTERNATIONAL DATA FLOWS: OPEN OR CLOSED?

Many technology-driven innovations rely on the sharing of data—and in an era of global business, that means being able to move data across national boundaries. But there are no global principles governing the movement of data, and "that is a challenge for businesses that want to operate globally," says Ambassador Robert Holleyman, president and CEO of C&M International and a former deputy U.S. trade representative.

Many countries have been busy developing their own data-transfer regulations. Often, these involve "data localization" rules that require information about citizens and more to be housed in the country. "With no accepted global norms, we are seeing these types of barriers cropping up," says Holleyman.

This issue is now part of several trade agreement discussions. For example, the 11 countries currently in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) are adopting provisions that favor open data flows and prohibit forced localization of data. In the renegotiation of NAFTA, "the U.S. has proposed a series of rules around cross-border data flows. The U.S., Canada, and Mexico have open borders now, but these would enshrine the concept that those borders remain open in the future," says Holleyman (for more information, see page 16).

On the other end of the spectrum, "China and some other countries are imposing highly restrictive rules that seek to preserve what they describe as their national data sovereignty—meaning cross-border data flows are not guaranteed," says Holleyman. China is also involved in negotiations for the Regional Comprehensive Economic Partnership, made up of a number of Asia-Pacific nations, many of which are part of the CPTPP. Holleyman says that this agreement is likely to end up as a compromise between the open and closed models.

"How these discussions play out in the coming year or two will have implications for how businesses use new technologies like cloud computing and artificial intelligence," says Holleyman. "Will they be able to use truly global solutions, or will they have to isolate data and maintain local storage in markets, and live with the cost and complexity that creates?"

"HOW THESE DISCUSSIONS PLAY OUT IN THE COMING YEAR OR TWO WILL HAVE IMPLICATIONS FOR HOW BUSINESSES USE NEW TECHNOLOGIES."

—ROBERT HOLLEYMAN

"YOU WANT TO MAKE SURE YOU'RE TALKING THE SAME LANGUAGE AS THE PEOPLE WHO WILL HAVE REGULATORY CONTROL OVER MUCH OF WHAT YOU DO."

—KATE GROWLEY

"IF SOMEONE KNOWINGLY TAKES ACTION TO RESTRICT THE AVAILABILITY OF HEALTH INFORMATION, THEY MAY BE IN VIOLATION OF THE LAW."

—JODI DANIEL

across a spectrum of industries," Falvey says. "Regulators know this and are eager to learn from innovators about what is coming next and what they need, so that we don't end up with a product that is in shambles and a company facing a new mountain of litigation."

One seismic effect of a disruptive technology is its unsettling of traditional boundaries between companies, industries, and markets—and autonomous vehicles are no exception. "You have everything from the big OEM car companies to tech giants and very early stage technology companies involved," says Jeffrey Selman, a partner in Crowell & Moring's Corporate Group. For tech companies in particular, stepping into the auto industry takes them into new regulatory waters, requiring them to enhance and expand their compliance capabilities and work with a set of regulators foreign to them until now.

DIGITAL HEALTH: REGULATING FOR INNOVATION

Digital transformation is especially taking hold in the health care industry. The sea change comes from all sectors, as medical providers, device makers, app developers, and patients find new ways to use data to improve care and outcomes and drive down costs. Health care's experience with regulation offers a window into how agencies in general might adapt to the digital revolution.

With the vast majority of health records having moved to digital platforms in the past few years, "data and digital technology are becoming increasingly important in patient care," says Jodi Daniel, a partner in Crowell & Moring's Health Care Group and the founding director of the Office of Policy in the Office of the National Coordinator for Health Information Technology at the U.S. Department of Health and Human Services.

For example, digital tools can enable a shift from traditional fee-based payments to value-based care, or precision medicine, in which payments are based on health care outcomes. "Medicare and Medicaid are trying to figure out how to reimburse health care providers based on value and outcomes. The only way to measure and pay for outcomes is if you have good data," says Daniel. The shift in payment models has been a key goal under past administrations, and it remains one today.

The federal government is also interested in making data readily available to researchers and to have health care data "follow" patients as they move through the health care system. As a result, says Daniel, "we're seeing a push for interoperability of systems and the ability of patients and technology services to access clinical data through APIs and innovative tools." Interoperability was a goal of the bipartisan 21st Century Cures Act, passed in December 2016; federal agencies are still working through the rulemaking process to implement the act.

While data sharing is critical to innovation, many hospitals and providers are reluctant to share patient information, in part because of concerns about privacy. The 21st Century Cures Act addresses this concern by prohibiting injurious forms of information blocking. "The law provides that if someone knowingly takes action to restrict the availability of health information, they may be in violation of the law—and for some entities, the fines can be $1 million per violation," says Daniel. Regulations implementing this new law are likely to be released by mid-2018.

Meanwhile, high on the FDA's agenda is "software as a medical device"—a critical component of digital innovation. Software innovation often involves ongoing updates, rapid learning, and improvements and bug fixes, which can lead to challenges for approved medical devices. The agency has indicated it is working to adapt its policies "to better align [its] regulatory approach to the iterative nature of digital health products." The FDA, Daniel adds, "has released guidance on decision support tools and software as a medical device and is considering new approaches to its regulatory oversight through its PreCert pilot."

CYBERSECURITY: A YEAR OF COMPLEX RISK

While digital innovations vary across technologies and industries, all have in common cybersecurity and data-privacy threats. From a regulatory perspective, meeting those challenges is not getting easier.

Companies have a growing, increasingly interconnected digital footprint. Protection of those systems and their data, once a sleepy back-office matter, has taken center stage. Digital-related laws and regulations increasingly contain cybersecurity elements—meaning companies face a growing regulatory burden. "2018 will be a year of complex cybersecurity risk and, especially, regulatory risk," says 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.

Take government contracting. The final aspect of the Defense Federal Acquisition Regulation Supplement (DFARS) Safeguarding Clause recently took effect, requiring contractors working with the Department of Defense to have in place certain cybersecurity-related technologies and controls. "There are now more than 45,000 defense contractors that have contractual obligations requiring them to implement the DFARS security measures and report sensitive cybersecurity incidents," says Wolff. "The potential cost of non-compliance, which may include losing the ability to contract with the federal government, can be severe."

Similarly, the Federal Acquisition Regulation for government contracts in general has expanded cybersecurity requirements. "We've seen recent cybersecurity guidance from NHTSA on autonomous vehicles and from the FDA on medical devices, and the National Institute of Standards and Technology recently updated its voluntary framework for cybersecurity across industries," says Falvey.

Changing consumer expectations can also contribute to regulatory risk. "People expect that the companies that they are buying products from or investing in are managing cyber risk through proper governance and will have invested in state-of-the-art security infrastructure," says Wolff. Thus, if cybersecurity issues arise, the problems are likely to invite scrutiny from not only the SEC (on behalf of investors) but also from consumer-oriented agencies such as the FTC. Indeed, in September 2017, three companies agreed to settle charges brought by the FTC contending that they had misled consumers by saying they were participating in the EU-U.S. Privacy Shield framework designed to protect consumer data moving across borders. Companies with a global footprint will also be expected to comply with the General Data Protection Regulation (GDPR), which addresses the export of personal data outside the European Union and goes into effect in May 2018.

Congress, too, is weighing in. The Cyber Shield Act of 2017 directs the secretary of commerce to convene an advisory committee to develop recommendations for cybersecurity benchmarks for the Internet of Things within two years. "The government is thinking about the 50 billion connected devices that are projected to be in our homes and in our pockets by 2020, and before long, we can expect to see more regulations focusing on the Internet of Things," says Wolff.

SHAPING THE FUTURE

Although burdensome regulation can hinder innovation, companies pursuing digital strategies abhor a vacuum. "Innovators usually want to know what the rules of the game are. If you're working with autonomous vehicles, for example, you want a framework that gives you an idea of what the agency might do later, so you're not caught flatfooted by the actions it eventually takes," says Falvey.

Still, technology and the marketplace are evolving quickly—and from the innovator's perspective, "it can be a competitive disadvantage to wait for the regulatory dust to settle," says Growley. Companies need to look for directional guidance wherever they can, whether from industry and trade associations, voluntary frameworks for various technologies, or from regulators themselves.

Falvey also suggests "working by analogy." For example, she explains, if an innovation in the consumer products industry does not yet fall under any regulatory scheme, "you might draw on the same principles that NHTSA uses for cars or the FDA uses for medical devices."

It's also important to understand the regulatory "baseline," says Growley—the traditional rules that are already in place. With automated vehicles, for example, "you need to be conversant with Federal Motor Vehicle Safety Standards. If you're a new tech entrant, that might not be right up your alley. Now it must be. You want to make sure you're talking the same language as the people who will have regulatory control over much of what you do," she says.

And innovators need to engage with regulators to shape the regulatory environment. Agencies are inviting input about technology-driven innovation, and particularly want to hear from those they regulate who deeply understand the digital revolution. Likewise, companies need to understand and listen to their regulators as their own practices evolve.

"Innovation is not going to stop," says Selman. "The question is, as innovation proceeds, will regulation be shaped in such a way that it works well with innovation? Innovations need to be safe and effective, but innovation must also bring commercial success. This is most likely to happen when companies engage with regulators."

Digital innovation is with us for good, and few industries are immune. With the speed of change, innovators have a promising opportunity to be heard by regulators—an opportunity they should not miss. "As the saying goes," Wolff notes, "if you're not at the table, you might end up on the menu."

"INNOVATIONS NEED TO BE SAFE AND EFFECTIVE, BUT ... BRING COMMERCIAL SUCCESS. THIS IS MOST LIKELY ... WHEN COMPANIES ENGAGE WITH REGULATORS."

—JEFFREY SELMAN

"PEOPLE EXPECT [COMPANIES] ARE MANAGING CYBER RISK THROUGH PROPER GOVERNANCE AND ... STATE-OF-THE-ART SECURITY INFRASTRUCTURE."

—EVAN WOLFF

BLOCKCHAIN

PROGRESS AND PROMISE

"Blockchain has the power to transform industries, and leading companies are wondering what it means for the future of their businesses."

— Mitchell Rabinowitz, Crowell & Moring Partner, Blockchain/Distributed Ledger Technology Practice

Blockchain technologies offer a way to transact or to share information in a secure, non-centralized system. Currently, these technologies are probably best known for their use with cryptocurrencies, but blockchain is absolutely not synonymous with Bitcoin. Instead, blockchain technologies are being explored for diverse applications across numerous market sectors.

Blockchain is not just hype. These technologies are seeing meaningful investment—the World Economic Forum estimates that more than $1.4 billion has been invested in distributed ledger technology (DLT) over the past three years. With a growing number of companies committing serious time and resources to deploying these technologies in their businesses, that figure is expected to increase exponentially over the next five years.

DATA PRIVACY

Regulatory programs like the European Union's General Data Protection Regulation (GDPR) are forcing companies to rethink how they handle personal data, and the possibility of significant fines have these issues high on boardroom agendas, including for non-EU companies. While the security aspects of blockchain technologies are a strength, some aspects such as permanent data retention and inter-jurisdictional transfers remain challenges that need to be addressed. *—Maarten Stassen*

SUPPLY CHAIN

Blockchain technologies are being put to use to address supply chain challenges related to provenance, sourcing (origin claims), import admissibility issues (forced labor), and even emerging issues such as conflict minerals. While many early applications have focused on high-value goods like diamonds, initiatives like the Maersk-IBM program that puts routine records on the blockchain, or Singapore's use for import record processing, illustrate that DLT is moving into the mainstream. However, supply chain users should understand that DLT is not currently a substitute for on-the-ground inspections, and ensure that they can still accommodate audits. *—Jeffrey Snyder*

INSURANCE

In insurance and reinsurance, blockchain technologies are being developed to streamline payment and claims processing, among other applications. However, blockchain implementations in this sector should be sure to account for industry-specific regulatory concerns like consumer protections and the financial regulation of insurers. Engaging with state regulators on blockchain applications will be a key step in working toward broader acceptance of blockchains in insurance, and early adopters have invited regulators into the process. *—Laura Foggan*

ENERGY

Blockchain technologies are being tested throughout the energy supply chain, including those that track ownership and country of origin for commodities like oil; decrease variance between energy supply and demand by allowing utilities and demand response providers to record energy usage in real-time; deploy "smart" devices to minimize consumers' energy costs; and facilitate peer-to-peer transactions, such as in community microgrids where neighbors can buy and sell electricity among each other. Because the energy industry is highly regulated, companies should understand how local, state, and federal regulations impact the blockchain technologies they are considering, and if public utility commissions' approval is needed. *—Matthew Welling*

INITIAL COIN OFFERINGS

Many blockchain startups are raising funds through "initial coin offerings" (ICOs)—sales of assets tracked through blockchain technology. The "coins" issued through an ICO can represent the right to use a startup's services or be the means of processing distributed applications. Most issuers are taking the position that their coins are not regulated under securities laws, commodities regulations, or money transmission rules. However, the SEC has spoken out about the potential of virtual coins to be subject to its regulations. Companies considering ICOs should be aware that consumer protection authorities may investigate token sales, and state governments are seeking to implement their own regulations. *—Jenny Cieplak*

HEALTH CARE

Blockchain technologies are being explored to address the significant challenges associated with managing health data, which is currently siloed. Problems exist with interoperability at all levels, but blockchain solutions show promise in applications such as connecting clinical data and creating longitudinal health records; managing wearable and patient-generated data; managing patient consent; facilitating patient-centered outcomes research and precision medicine research; and managing patient and provider identity. However, organizations should be aware that these exciting applications must also address the unique legal and regulatory challenges associated with health data. *—Jodi Daniel*

FINANCE

Although some in the FinTech industry have assumed that it will take years to replace legacy systems with new blockchain systems, 2018 is likely to see the first broad-based implementations. From a blockchain-based reporting platform for credit default swaps, to trading platforms for syndicated loans, companies are planning production launches for early 2018. Regulators have already begun making updates to accommodate new technologies—such as the CFTC's changes to its record-keeping requirements to make them technology-neutral—but additional rulemakings may be required to fully implement production solutions.
—Mitchell Rabinowitz

2018 is the year that many blockchain and DLT providers expect to move from proof-of-concept to live solutions. But before live use, providers will need to demonstrate—both to regulators and to their customers—that their solutions help users comply with a wide array of regulations. Data privacy, know-your-customer, and sanctions and export control compliance must all be addressed.

Nevertheless, blockchain and DLT offer too many benefits for these technologies to be ignored. General benefits such as more accurate data, faster back-office processing, automated transactions, and the elimination of reconciliation requirements are applicable to all industries. Industry-specific use cases are being developed for energy, insurance, and health care, and participants will need to understand and evaluate these use cases.

As blockchain continues to move into the mainstream, companies will need to develop a blockchain strategy, and to decide whether and how to participate in and use blockchain. Organizations should be preparing for those discussions.

NATURAL DISASTERS

DEALING WITH THE NEW NORMAL

"IT'S A MATTER OF GLOBAL IMPORTANCE. THE ISSUE IS WHAT TO DO ABOUT IT."

—RICHARD LEHFELDT

More than 50 inches of rain in five days in Houston. The first mass evacuation of the Florida Keys in decades. Puerto Rico's electric grid essentially destroyed, with at least a year until full power will be restored. With millions of people affected and hundreds of lives lost, the full damage is still being tallied, and the financial cost is now estimated in the hundreds of billions of dollars.

The devastating hurricanes in 2017—Harvey, Irma, and Maria—on top of the deluge of other major storms in recent years, have raised new questions about whether the U.S. electrical grid is up to the task, given the "new normal" of severe weather.

"It's a matter of global importance," says Richard Lehfeldt, a partner in Crowell & Moring's Energy Group. "The issue is what to do about it. It's not as if it arose out of nowhere."

The severity of the threat is daunting. A U.S. Government Accountability Office study found that Superstorm Sandy-like events that once took place every 500 years in 1800 are now occurring every 25 years. Worse yet, by 2045, those superstorms could come once every five years.

That growing hazard prompted the U.S. Department of Energy last year to direct the U.S. Federal Energy Regulatory Commission to examine, among other things, whether the U.S. electrical grid is reliable and resilient enough to address these severe and recurrent stresses to the system, and what resources are needed to strengthen resiliency and respond rapidly to major weather events. While that rulemaking ended early this year, the commission reiterated its commitment to ensuring that the national grid is able "to withstand or recover from disruptive events."

Several entities share responsibility for monitoring and ensuring the safety and reliability of the grid. The North American Electric Reliability Corporation is designated by FERC to ensure the grid's reliability. The Department of Homeland Security and the Department of Defense each look at the grid from the perspective of national security. The key questions: What are vital resources and critical energy infrastructure? Which facilities must be capable of operating in a severe weather event, no matter what? And how do we restore resources after an incident?

A LOCAL MATTER

Government policymakers can require resilience planning, seek to formally price reliability and resiliency, and offer subsidies to promote preferred behaviors in order to make the grid more reliable. Federal and state regulators can issue specific regulations compelling risk management in the design and management of electrical generation and transmission facilities. But part of the problem is that while safety and reliability are of national importance, the federal government doesn't have direct control over maintenance of the grid. Currently, most key resources' choice decisions about what to build and what kind of power generation to have are made by state regulators, through contested regulatory hearings, and not the typical authorization and appropriations process used for most public works projects.

"All of those state-level decisions are then somehow supposed to be integrated and harmonized at the federal level, which doesn't always happen," says Lehfeldt. "The questions that are now increasingly being asked by regulators and legislators, at both the state and federal level, pertain to security, reliability, and now the new word 'resiliency.' The issue is: What resources do we need now that these extreme weather conditions are becoming the new normal?"

THINKING OUTSIDE THE GRID

One way being considered to protect the grid from severe weather is the establishment of so-called microgrids—full-fledged, miniature utility systems, capable of "islanding" their operations and continuing to function even in the event of a long-term, regional power outage. These can be expensive systems, but cities and states now see an increasing need for microgrids to prepare for outages that can last weeks or even months. The city of Princeton, New Jersey, for example, has one, as does the New York University Manhattan campus. The Princeton microgrid maintained service through the worst of Superstorm Sandy.

Another tactic under consideration rests on the

question of whether some retail customers might settle for a reduced level of service, essentially paying less in exchange for agreeing to suffer service interruptions during severe weather disruptions. Such multi-tiered service already exists during power restoration, when utilities triage service calls to ensure that essential customers (hospitals, fire and police departments, food suppliers) return first to full service.

IS INSURANCE A SOLUTION?

Of course, one of the biggest issues is who should bear the financial burden. "How are we going to pay for the added security or reliability that is necessary because we are no longer talking about a 100-year storm, but about something that occurs more frequently?" asks Laura Foggan, a Crowell & Moring partner and a member of the firm's Insurance/Reinsurance Group. "Insurance is an important part of the solution. Of course, the higher number of weather events means there are greater losses and increased costs for insurers as well, but insurers can help minimize or prevent loss, as well as spread the financial burden of losses from climate change."

The insurance industry can play a role in helping prepare for future severe weather because the companies have a tremendous amount of data and knowledge about loss avoidance and prevention, Foggan says. "One of the things insurers can do is partner with government regulators both at the state and federal level to identify and articulate loss-prevention strategies that will benefit society as well as insurers," she says. Loss prevention or mitigation of physical damage to key infrastructure—such as electrical grids—saves costs of repair, as well as the important downstream costs to private industry and society that result from loss of infrastructure function.

Policymakers must also consider whether government help in financing recovery may promote repetitive losses. Currently, the federal government is the last line of defense for many victims of hurricanes and floods through the National Flood Insurance Program, which provides coverage for about 5 million homes and businesses.

As the costs of hurricanes increase, so do the questions about whether this subsidized insurance is the best solution, because it costs all U.S. taxpayers yet benefits so few homeowners. And Foggan says questions continue to be raised as to whether such pricey, subsidized insurance products in fact incentivize real estate development in geographic areas that are just too high risk to sustain such projects.

"HOW ARE WE GOING TO PAY FOR THE ADDED SECURITY OR RELIABILITY THAT IS NECESSARY BECAUSE WE ARE NO LONGER TALKING ABOUT A 100-YEAR STORM, BUT ABOUT SOMETHING THAT OCCURS MORE FREQUENTLY?"

—LAURA FOGGAN

WHO PAYS FOR DISASTER?

If a home or business is built in a known floodplain, should the government have to help pay for the damage when a flood occurs? What role should private insurance companies play?

Those are questions that the U.S. Congress is debating as it restructures the National Flood Insurance Program. The NFIP provides subsidized insurance to homes in at-risk flood areas that might not otherwise be able to get coverage.

Many countries are struggling with how to handle flood coverage. The U.K. has a new approach to addressing the availability and affordability of private homeowners' flood coverage through Flood Re, a not-for-profit levy and pool system that is designed to provide affordable insurance to up to a half-million households in high-risk flood areas.

The closest thing the U.S. has to this is in Florida, where a law allows private flood insurance.

Michelle Linderman, a London-based partner at Crowell & Moring and a member of the firm's International Trade Group, says that as forward-looking as Flood Re is, it does have its faults.

The first is that despite the program's goal to provide affordable insurance, critics say its policies are still too expensive. Moreover, it is only available to homeowners and not for commercial properties.

Finally, it does not provide any means to encourage actions that might reduce future risk from flooding.

However, Linderman notes, "despite its shortcomings, Flood Re is a good example of how government can work with the private sector to bring about change that benefits hundreds of thousands of households."

"FLOOD RE IS A GOOD EXAMPLE OF HOW GOVERNMENT CAN WORK WITH THE PRIVATE SECTOR TO BRING ABOUT CHANGE THAT BENEFITS HUNDREDS OF THOUSANDS OF HOUSEHOLDS."

—MICHELLE LINDERMAN

INSURANCE/REINSURANCE

INSURANCE COMPANIES EMERGE FROM BANK-LIKE OVERSIGHT

Shortly after being sworn into office, President Donald J. Trump set in motion a change that will likely alter regulation for the entire U.S. insurance industry.

Trump signed an executive order two weeks into his term instructing Treasury Secretary Steven Mnuchin to undo large parts of the Dodd-Frank Act, which was signed into law in 2010 in response to the 2008 financial crisis.

Mnuchin recently delivered, issuing guidance in a report that, among other things, said that the federal Financial Stability Oversight Council will be much less likely to treat non-bank companies that deal primarily with insurance as systemically important financial institutions (SIFI).

The SIFI designation, also known as "too big to fail," grew out of the Obama administration's reaction to the near-collapse of the financial system in 2008. Essentially, it means that a company's operations were so intertwined with the financial system that its collapse could endanger the broader U.S. economy. It was first used on banks and then extended to a small group of non-bank institutions.

The reversal was expected. "I would have been surprised if the Trump administration had continued the Obama administration's policy of subjecting certain large insurance companies to enhanced oversight by the Federal Reserve," says Richard Liskov, senior counsel to Crowell & Moring's Insurance/Reinsurance and Corporate groups and former deputy superintendent of the New York State Insurance Department (now the New York State Department of Financial Services).

The non-bank SIFI designation subjects an insurance company to additional oversight by the Federal Reserve as well as stricter capital requirements. It was prompted by the federal government's $182 billion bailout of American International Group (see "How AIG Shed the SIFI Label," opposite).

Now, nearly a decade after the financial crisis, a SIFI change directly affects just two insurers: Prudential Financial and MetLife. But, as Liskov notes, "it portends less federal regulation of insurance generally."

MetLife, which was designated a SIFI in December 2014, successfully sought in court to have the label removed when U.S. District Court Judge Rosemary Collyer ruled in March 2016 that the FSOC was "fatally flawed" in its process designating MetLife a non-bank SIFI. On January 18, the Trump administration agreed to drop the appeal of Judge Collyer's ruling, which its predecessor had filed in 2016.

THE RIGHT THING TO DO

Now that the administration has decided to accept the de-designation of MetLife by not prosecuting the appeal, Liskov expects Prudential to be de-designated as well. It is the appropriate move to make for another reason, he says. That's because state regulators are perfectly capable of overseeing insurance companies and don't need any help from the Federal Reserve. Periodic on-site exams, annual risk-based capital measures, restrictions on investments, and independent audits by certified public accountants are "among the numerous tools that state insurance regulators have for monitoring the solvency of the insurance companies," Liskov says.

Additionally, state regulators, because of their long experience with insurers, are better acquainted with their operations. For instance, New Jersey has been overseeing Prudential for more than a century. Liskov says one of the weaknesses of the non-bank SIFI rules is that they don't require the Federal Reserve to accede to any objections from the state regulators tasked with overseeing insurance companies. He adds that the only way a SIFI designation would make sense is if the Dodd-Frank treatment applied

"The [SIFI] designations are potentially confusing and detrimental because ... the consumer has reason to believe that state regulation is insufficient." —*Richard Liskov*

to non-insurance operations while state insurance regulators handled the rest.

SENDING THE WRONG MESSAGE

There are further problems with the non-bank SIFI labels. "The designations are potentially confusing and detrimental because, to the extent it is being regulated by both the state and federal governments, the consumer has reason to believe that state regulation is insufficient," Liskov says. "It erodes confidence in state insurance regulators as being protectors of consumers' interest."

The confusion doesn't stop there. An insurer bearing the SIFI designation "can be viewed unfairly as having an advantage in the marketplace and lead to harmful expectations on the part of the consumer and companies that deal with SIFI companies that the federal government will do whatever it can to bail them out," Liskov says. Making that perception even more off base is the fact that the federal government doesn't have a specific fund set up to cover claims against insurance companies.

So the removal of non-bank SIFI designations should essentially be a vote of confidence from the Trump administration in state regulators. As Liskov notes, "It would be a reaffirmation that insurance in the U.S.—except for certain narrow categories such as flood, terrorism, and crops—should be regulated at the state level."

Finally, Liskov says that the position Treasury has adopted appropriately recognizes the lead role of state insurance regulation, particularly in the view that SIFI designations should be made on the basis of what a company does, not what kind of company it is. "Before the federal government designates an insurance company as a SIFI, there needs to be full consultation with concerned state insurance regulators," he says.

INTERNATIONAL IMPLICATIONS

Scrapping the non-bank SIFI label should also help quiet broader concerns about the U.S. insurance industry's having to adhere to tough international standards. The Federal Reserve and the Treasury Department have been in talks with officials from other countries that regulate insurers and banks. Liskov says U.S. insurance companies fear the federal government is willing to acquiesce and follow the international standards that treat banks and insurance companies the same, requiring stiffer capital standards for insurers.

The U.S. insurance industry and state insurance regulators both argue that there is a big difference, and, notes Liskov, correctly so. "You can't call up MetLife and say, 'Give me back my money,'" he says. "These are not deposit institutions."

So the administration's decision to end virtually all non-bank SIFI designations for insurers should not only put state regulators back in charge, Liskov says, it should also signal to the international community that the U.S. will regulate insurance companies and banks differently—and be a welcome relief to U.S. insurers. Says Liskov: "The way that regulators monitor their solvency should be different from the way bank examiners look at the solvency of deposit institutions."

HOW AIG SHED THE SIFI LABEL

The insurer that started it all won't even be affected by the Trump administration's dropping the non-bank SIFI designation.

American International Group was the first company to be designated a non-bank systemically important financial institution after its near-collapse forced a $182 billion bailout by the federal government. On September 29, 2017, AIG slipped the surly bonds of the SIFI badge when the Financial Stability Oversight Committee ruled it no longer deserved the designation because its performance no longer posed a risk to the U.S. economy.

AIG was one of four non-bank SIFIs. General Electric shed the designation when it sold off most of its GE Capital arm. In 2015, MetLife successfully argued in court that it no longer deserved the designation, and the Justice Department recently dropped its appeal in that case. Prudential Financial is still trying to shake its SIFI label.

Crowell & Moring's Richard Liskov says that while MetLife and Prudential don't deserve the SIFI label, there was a stronger argument for SIFI oversight of AIG before it sold off assets and fully repaid the U.S. government.

TRADE

NAFTA: RENEGOTIATE—OR SCRAP?

The U.S. is on the verge of the most sweeping changes on the trade front in nearly a quarter-century as it seeks to renegotiate or possibly scrap the North American Free Trade Agreement.

In several rounds of often-contentious talks during 2017, NAFTA's three partners were not able to agree on changes the U.S. proposed that now have it squaring off against Mexico and Canada.

The three have agreed that the negotiations should extend into at least the first quarter of 2018. But that is only delaying the inevitable reality that NAFTA is going to be changed or scrapped, says Ambassador Robert Holleyman, president and CEO of C&M International and a partner in Crowell & Moring's International Trade Group.

So if U.S. companies haven't already started, they should look now at how what is being dubbed "NAFTA 2.0" will affect their North American and global operations.

A CHILD OF THE '90S

The original NAFTA was hammered out under President George H.W. Bush and signed into law in 1994 by President Bill Clinton. It eliminated most tariffs on trade between the U.S., Mexico, and Canada. At the time, proponents praised its potential to add a million or more jobs and be a major source of growth for the U.S. economy.

But during his campaign for president, then-candidate Donald Trump called NAFTA and the Trans-Pacific Partnership unfair to the United States and promised to end or renegotiate the trade agreements. True to his word, the U.S. withdrew from the 12-country TPP three days into President Trump's term. Then, last June, President Trump announced he would demand a renegotiation of NAFTA or the U.S. would walk away. Mexico and Canada, having previously agreed to renegotiate NAFTA through the TPP, joined in formal NAFTA-only talks that began in August.

Mexico and Canada are among the 11 nations still in the TPP. Holleyman says the two are using some strategic gamesmanship in their current NAFTA negotiations. While the U.S. demands causing the most controversy are new, many other elements in NAFTA 2.0 are not. Mexico and Canada are now refusing to commit to many provisions that they had already agreed to with the TPP.

The Canadians and Mexicans want to see how the

KEY POINTS

Trade facing changes
Companies should look at possible impacts to global operations.

No agreement yet
The U.S. is squaring off against Mexico and Canada.

The main event
Digital trade is no longer a sideshow, though it's largely escaped the attention of regulators and lawmakers.

"The new proposals from the U.S. are far outside the norm from what the U.S., Canada, and Mexico have sought and agreed to in the past." —*Ambassador Robert Holleyman*

U.S. handles items it has placed on the negotiating table that may be too difficult for them to accept, Holleyman says. The two "essentially said no, this is a new negotiation," he says. "Yes, we agreed to some of these things in prior TPP negotiations in 2015, but the landscape has changed."

NEW U.S. DEMANDS BRING CONTROVERSY

It's possible that before or soon after the March 31 deadline, the U.S. will decide that the talks have reached an impasse and the Trump administration will signal its intent to withdraw from NAFTA altogether.

"The odds of that happening now are at least 50-50," says Holleyman, who served as deputy U.S. trade representative from 2014 to 2017, holding the rank of ambassador. "For the longest time, I didn't think that was likely. But the new proposals from the U.S. are far outside the norm from what the U.S., Canada, and Mexico have sought and agreed to in the past; it's unclear whether the Canadians and Mexicans can or will agree to those things."

Specifically, the U.S. reportedly is seeking to ensure that a guaranteed percentage of production in the NAFTA region, particularly for autos and auto parts, will come out of the U.S. and not North America as a whole.

The U.S. also has reportedly proposed restricting the overall ability of Mexican and Canadian companies to supply U.S. government procurement—transferring significant shares of government procurement opportunities away from Mexican and Canadian companies to U.S. companies.

And for any trade disputes among the three countries, the U.S. wants to end the current arbitration process and instead have these matters handled in domestic courts.

BE PREPARED

The auto industry has much at risk in the new trade negotiations. The Trump administration blames NAFTA for adding to the U.S. trade deficit and costing more than 700,000 American jobs. A coalition of automakers, auto parts makers, and auto dealers argues that NAFTA is responsible for more than $1.2 trillion in annual trade and that undoing it would put auto industry jobs at risk.

What Ambassador Holleyman says is clear is that companies in the auto, agriculture, food products, textile, and other sectors should put contingency plans in place, assessing their North American manufacturing and supply chains, and be prepared to react to any tightening of trade barriers in what has long been a free trade zone.

Companies should prepare for three scenarios, Holleyman says. The first is a modest adjustment to the status quo. The second is a substantial reordering of their supply chain if the U.S. is able to get Mexico and Canada to accede to its proposals. The third, and critical for contingency planning, is an outcome in which the U.S. withdraws from NAFTA and companies have to decide where to locate their primary source of production.

The country that companies ultimately pick will be a test of whatever the new trade relationship is, Holleyman says. Companies are going to have to decide if the U.S. market is large and important enough for them to have tariff-free, ready access to the U.S. in exchange for higher tariffs in Mexico and Canada. On the other hand, a company might decide that Mexico and Canada have such favorable trade relationships with other countries outside of North America that it makes sense to locate manufacturing in either Canada or Mexico. Then they would access the U.S. by accepting the relatively low rate of U.S. tariffs, as a trade-off to having duty-free or low-tariff access to other markets outside the U.S.

THE DIGITAL REALITY

If the squabbling NAFTA partners can agree on one thing, it's that age is probably one of the trade pact's biggest weaknesses, because the internet barely existed in 1994 when NAFTA was signed into law.

Fast-forward 24 years. Digital trade has gone from a quiet sideshow to the main event as an area of explosive growth for all countries. Yet it's also something that has largely escaped the attention of regulators and lawmakers.

That changed with the Trans-Pacific Partnership, an agreement between 12 countries that Crowell & Moring's Robert Holleyman says was the first global agreement with a robust blanket of digital trade provisions.

Holleyman would know. He was the deputy United States trade representative from 2014 to 2017 and on the front line in TPP and digital negotiations.

A rare bright spot in the rocky NAFTA 2.0 negotiations is that everyone recognizes the need to cover digital trade.

The TPP has a framework of groundbreaking digital initiatives that Canada, Mexico, and the U.S. all signed off on to enable cross-border data flows and promote a free and open internet. Holleyman thinks those will be incorporated into NAFTA 2.0, if there is one.

Holleyman suggests the U.S., Mexico, and Canada need to be leaders. "It is important that any modern trade agreement recognizes the digital economy and that the NAFTA countries go on record in favor of open, barrier- and tariff-free digital trade," he says.

ANTITRUST

TRUMP'S FIRST YEAR: NOT AS 'MERGER-FRIENDLY' AS EXPECTED

Despite the anticipated "pro-business" approach of the Trump administration, the Department of Justice and the Federal Trade Commission have both continued to challenge mergers. Indeed, late in 2017, DOJ signaled that it might be taking a tougher stance on vertical mergers and might be unwilling to accept behavioral remedies to settle such matters.

"A year or so ago, there was a general assumption in the business community and antitrust bar that there was going to be something of a lapse in antitrust enforcement under the Trump administration," says Juan Arteaga, a partner in Crowell & Moring's Antitrust Group and a former deputy assistant attorney general in the Antitrust Division at DOJ. But that did not happen. In May 2017, the DOJ blocked Anthem's proposed $54 billion acquisition of Cigna when the D.C. Circuit affirmed the trial court's decision. The next month, DOJ blocked a $367 million merger between EnergySolutions and Waste Control Specialists (continuing another suit filed by the prior administration).

In September 2017, DOJ brought its first merger challenge under the Trump administration when it sued to partially unwind Parker-Hannifin's $4.3 billion acquisition of CLARCOR. DOJ took the unusual step of challenging a consummated deal that it had previously cleared without even seeking additional information during the statutory review period. In its challenge, DOJ stated that the companies had failed to disclose certain information during the investigation, showing that DOJ will not hesitate to keep scrutinizing a merger's competitive effects even after the deal has closed. This case was recently settled when the companies agreed to divest the business that was the subject of the suit.

The FTC, too, has continued to be active on the antitrust front. "We haven't seen any major shifts in antitrust enforcement at the FTC since the election. The commission has continued to challenge deals, filing four challenges in the past year alone," says Alexis Gilman, a partner in Crowell & Moring's Antitrust Group who was previously assistant director of the Mergers IV Division in the FTC's Bureau of Competition. For example, he says, in June 2017, the FTC moved to stop the merger of DraftKings and Fan Duel, the two largest online daily fantasy sports sites, saying the combined company would create an organization that controls more than 90 percent of the U.S. market for such fantasy offerings. That move prompted the companies to call off the deal.

That same month, the FTC authorized a federal court action to block the proposed acquisition of a physicians' group, saying that the move would significantly reduce competition for various physician services in one part of the state. "That was in keeping with the agency's long line of active enforcement in the health care space, which is likely to continue," says Gilman.

In the recent past, he notes, "roughly half of the FTC's antitrust enforcement actions have been health care-related. Health care is an industry where the FTC continues to be very active and act in a bipartisan way."

Recently, the FTC has filed two more merger challenges, including one to unwind a consummated merger. In 2017, DOJ and the FTC brought three separate actions seeking to unwind consummated mergers. Gilman says the FTC is also likely to keep pursuing non-merger antitrust actions, especially where pharmaceutical companies pay generic drug makers not to bring their lower-cost products to market.

Overall, adds Arteaga, "to the extent that GCs and business executives were expecting a big pullback in antitrust enforcement, they might need to recalculate their assumptions."

"Companies and their advisors have to take these developments into account when formulating their M&A strategies for the upcoming year." —*Juan Arteaga*

"We haven't seen any major shifts in antitrust enforcement at the FTC since the election. The commission has continued to challenge deals." —*Alexis Gilman*

DOJ: A FUNDAMENTAL CHANGE

Late in 2017, the new assistant attorney general for the DOJ Antitrust Division, Makan Delrahim, shook basic assumptions about federal antitrust policy when he strongly suggested that behavioral remedies will almost always be inadequate to address DOJ's concerns in merger investigations, including those involving vertical mergers. A short time later, DOJ challenged the AT&T-Time Warner vertical merger.

In discussing the ramifications of these recent DOJ developments, Arteaga says that "it's too early to say whether there has been a long-lasting change in DOJ policy toward vertical mergers and behavioral remedies, but companies and their advisors have to take these developments into account when formulating their M&A strategies for the upcoming year." Arteaga adds that "these developments and subsequent press releases issued by DOJ strongly suggest that companies relying primarily on behavioral remedies, instead of putting asset divestitures on the table, will likely run into significant difficulty when trying to negotiate a settlement with DOJ."

It may not take long to find out if the change is systemic. "DOJ is reviewing other significant vertical mergers," says Arteaga. "The way these deals are handled could tell us if the AT&T-Time Warner suit was a unique situation or the result of new policy toward vertical mergers."

Whether the FTC follows suit on vertical mergers remains to be seen. There are a number of vacancies on the commission. In the coming year, says Gilman, "we will likely have five new commissioners. That makes it hard to predict exactly what direction the commission could take."

We may see early signals soon. The significant vertical cases at the FTC are still pending, but should be in the latter stages of review. "How the FTC handles these deals will probably be an early indication of what approach it is going to take with vertical mergers," says Gilman.

"However," he adds, "the director of the FTC's Competition Bureau recently emphasized that the FTC has always had a strong preference for structural, rather than behavioral, remedies in merger investigations. And he noted that vertical-merger enforcement is not unusual, which could be a signal that the FTC may try to take an approach consistent with that of DOJ."

A NEW FOCUS ON IP AND ANTITRUST

The new head of the DOJ Antitrust Division is signaling change, including in how the department will look at IP and antitrust.

In November, Assistant Attorney General Makan Delrahim announced that DOJ will carefully scrutinize the concerted actions of members of standards-development organizations that restrict the legitimate exercise of patent rights. Going forward, Delrahim says, the division will focus on what he sees as the true competitive threat in the IP area: parties in standards bodies that use key IP but drag their feet on paying for licenses, or simply refuse to take a license. These "holdouts" and their activities, he says, will be receiving hard looks in the coming year.

"Delrahim basically said that the division has been too focused on protecting people and companies that use IP and hasn't offered enough protection to people and companies that create IP, which he believes ends up harming competition and consumers by minimizing the incentive to innovate," says Crowell & Moring's Juan Arteaga. He notes that while this represents a change from the division's recent focus, it is actually a return to previous DOJ policy around antitrust and IP law.

Meanwhile, at the FTC, the two sitting commissioners (Acting Chair Maureen Ohlhausen and Commissioner Terrell McSweeny) appear split, and because we will likely have five new commissioners by the end of the year, the future is less certain. "We don't have a clear view yet on what the FTC's position will be on this key issue," says Crowell & Moring's Alexis Gilman. "Thus, the views of the incoming commissioners as to the proper balance of IP and antitrust issues in general will play an important role in the course that the FTC takes in this area."

As a result of the DOJ shift and the uncertainty at the FTC, Arteaga says, "standards bodies and the companies that participate in them need to be more cautious in the way they handle technology patents. They should review their antitrust compliance programs and think carefully before changing their policies in ways that might end up disadvantaging IP owners."

INTELLECTUAL PROPERTY

PATENT REVIEWS: THE JOURNEY CONTINUES

After the passage of the landmark America Invents Act in 2011, courts and the United States Patent and Trademark Office spent several years sorting out how it would work in reality and making adjustments along the way. Now that interest in modifying patent laws and procedures is back—and gaining momentum.

Today, a number of observers believe that changes made under the AIA have tilted the process in favor of patent challengers and made it easier to invalidate patents. This has led to a growing discussion about how to improve things—and now, "some people are asking for changes in the patent system," says Teresa Rea, a Crowell & Moring partner, vice-chair of the firm's Intellectual Property Group, and a director with C&M International.

Much of that discussion has centered on the USPTO's *inter partes* reviews. In the IPR process, patent holders and challengers present their cases to the Patent Office's Patent Trials and Appeals Board, much like they would in a courtroom. Designed to be a faster and lower-cost alternative to litigation, IPRs quickly became a popular forum for patent cases. Many saw IPRs as a way to rein in the activity of trolls, or non-practicing entities, because they provided an avenue for invalidating their marginal patents.

However, compared to litigation, IPRs use less stringent standards when it comes to claim construction and burden of proof, and in practice, the process has had a significantly higher patent-invalidation rate than the courts. "Some patent holders now consider these PTAB proceedings to be unfairly good at invalidating their patents—and for doing so more cheaply and quickly than the district courts," says Rea, who was formerly the acting and deputy director of the USPTO and the acting and deputy undersecretary of commerce for intellectual property.

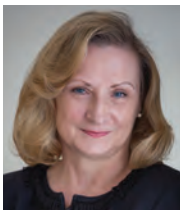
This has created tensions across various industries. For example, says Rea, high-tech companies, which may have thousands of patents in a device, see the IPR proceedings as a chance to invalidate the patents of trolls and, therefore, as something critical to innovation. Pharmaceutical companies, on the other hand, often have just a few patents involved in one of their products, making each patent more critical. In their view, IPRs make it difficult to protect their patents, and therefore, they see IPRs as something that tends to stifle innovation. Originally, says Rea, "the AIA and IPRs were designed to bring those varying viewpoints together. But now, there is more separation than ever between the high-tech and life sciences sectors on these issues."

KEY POINTS

Focusing on the Patent Office
Several years after the AIA passed, many look for change in USPTO processes.

Congress weighs in
Legislators are considering several changes to patent law that may alter USPTO practices.

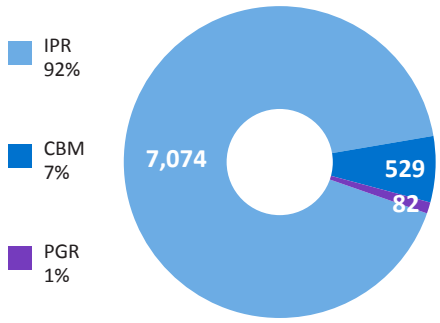
The litigation factor
Court actions may reshape—or eliminate—the popular *inter partes* reviews.



"We're seeing industries going back to Congress to ask for modifications to various procedures and laws relating to the PTAB." —*Teresa Rea*

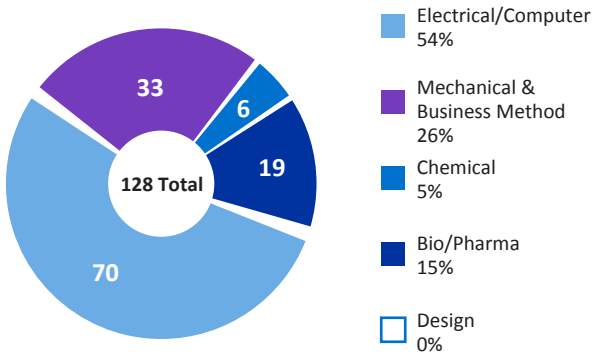
Petitions by Trial Type
(All Time: 9/16/12 to 10/31/17)

IPR is by far the most common trial type at the USPTO



Petitions Filed by Technology in FY18
(FY18 to date: 10/1/17 to 10/31/17)

High tech industry cases make up a large portion of the PTAB work



Source: United States Patent and Trademark Office

CONGRESS AND THE COURTS: LOOKING AT CHANGE

These differing perspectives are making patents, and especially the USPTO reviews, an issue for legislators. "We've had a couple of years to see how the IPRs work in practice, and it may not be playing out as a lot of people had anticipated," says Rea. "We're seeing industries going back to Congress to ask for modifications to various procedures and laws relating to the PTAB."

That congressional interest, and some patent holders' dissatisfaction with the system, came together in September 2017, when a pharmaceutical company transferred some of its patents to the St. Regis Mohawk Native American tribe. The goal was to shield the patents from IPR hearings, with the company saying that because the tribe was not subject to U.S. laws, it could not be required to participate in such hearings. Many in Congress were not pleased, and in October 2017, Missouri Senator Claire McCaskill introduced a bill saying that Native American tribes could not claim sovereign immunity to avoid patent hearings.

Congress is also looking at ways to further curtail some of the non-practicing entities' actions—a goal that the AIA addressed to some extent, but not completely. "While the trolls' activity is less than before, there is still pain for a lot of small companies that don't have the resources to fight them in legal battles," says Rea. With that in mind, some members of Congress have been exploring the idea of making attorney fee-shifting—the "loser pays" system—the legal default, rather than just an option. This would presumably make parties less likely to bring weak claims in hopes of a settlement.

Perhaps the biggest potential change to watch is the Support Technology & Research for Our Nation's Growth and Economic Resilience Act (STRONGER), introduced in June 2017. Sponsored by senators from both sides of the aisle, STRONGER calls for a variety of changes to the Patent Office's processes with the general aim of boosting protection for patents. Among other things, the bill would tighten rules about burden of proof, harmonize the PTAB's claim construction standard with the district court standards, limit petitioners' ability to challenge a patent repeatedly, and require petitioners to have a business or financial reason to bring a case before the PTAB.

Court cases, too, are driving change at the USPTO. Traditionally, when a patent holder offered an amended patent during an IPR, it was up to that patent holder to prove the patentability of its claim. In October 2017, however, the U.S. Court of Appeals for the Federal Circuit shifted that burden of proof to the petitioner in its *Aqua Products Inc. v. Matal* decision. The court also said that the patent office could, if it wants, issue a new rule to move that burden back to the patent holder. "In general, it was a complex, 15-page opinion, and the issue may well end up with the Supreme Court," says Rea.

Meanwhile, the Supreme Court is expected to rule in early 2018 in *Oil States Energy Services v. Greene's Energy Group*, which is challenging the legality of IPRs. Here, the plaintiffs say that the process is unconstitutional because it violates the separation of powers by giving the executive branch authority that really belongs with the judicial branch, and uses an administrative body to take away an individual's property rights. "This threatens the very existence of the IPRs, which would be a very dramatic change on the regulatory front," says Rea.

As these developments unfold, the USPTO has a new director, Andrei Iancu. In his confirmation hearings, Iancu's comments led many to believe that he will be working to provide more protection to patent owners—but in today's changing landscape, it remains to be seen what that will mean for the PTAB. For the time being, "we need balance, and a lot of things are still up in the air," says Rea.

GOVERNMENT CONTRACTS

WILL PURCHASING BE STREAMLINED?

As government contractors know, past efforts to streamline the government's approaches to buying commercial items have often fallen short. But there is now renewed interest in such improvements, and they may be gaining some traction.

That interest has its roots in the Federal Acquisition Streamlining Act of 1994, which simplified commercial item acquisitions and tried to make them more like private-sector procurements. The Federal Acquisition Regulation implemented FASA the following year, but in the intervening decades, additional regulations and executive orders brought increased complexity. "In 1995, there were 17 contract clauses potentially applicable to commercial item procurements through FAR 52.212-5(b). By 2017, there were almost 60," says Robert Burton, a partner with Crowell & Moring's Government Contracts Group and former acting and deputy administrator of the Office of Federal Procurement Policy. With that kind of growing complexity in commercial procurement, he says, "many commercial companies that are trying to do business with the government have become frustrated with the process."

That reality has prompted a range of responses from the government. For example, "agencies with other transaction authority have looked to use such authority because it provides agencies more flexibility to meet their needs and enhance mission effectiveness," says Lorraine Campos, a partner in Crowell

BIG PLANS FOR BIG CHANGE

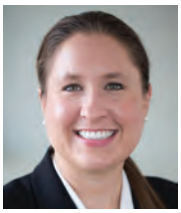
The Section 809 Panel, which was established by Congress to find ways to improve Pentagon procurement processes, has a wide-ranging mandate. To handle it all, the panel has set up 10 teams, each with a specific area of focus. At least three of those are working on simplifying or streamlining acquisition.

One group, known as Team 3, aims to simplify the Defense Department's commercial buying practices to improve access to companies and make acquisitions more adaptable and agile. Team 2 is exploring the streamlining of acquisitions involving less than $15 million. And Team 4 is looking for ways to encourage companies that have not previously done business with the DoD to enter the federal marketplace—especially technology companies.

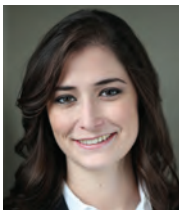
The panel intends to do more than produce yet another report on government red tape. "We anticipate there are going to be wholesale changes recommended by the panel," says Olivia Lynch, a counsel in Crowell & Moring's Government Contracts Group. "People on the panel have said they are not just playing around the edges. They are looking to make bold changes, with recommendations to Congress not only to change and remove regulations, but also to implement those into statute."

"Many commercial companies that are trying to do business with the government have become frustrated with the process."
—*Robert Burton*

"Agencies with other transaction authority have looked to use [it] because it provides agencies more flexibility to meet their needs and enhance mission effectiveness." —*Lorraine Campos*



"The government in general is looking for better ways to buy these products and services and increase efficiency in commercial procurement." —*Elizabeth Buehler*



"People on the panel have said they are not just playing around the edges. They are looking to make bold changes."
—*Olivia Lynch*

& Moring's Government Contracts Group.

Congress, too, has been looking at the issue of streamlining procurement. In December 2017, President Trump signed the National Defense Authorization Act providing a number of measures, including the creation of a government-wide e-commerce portal to streamline the purchase of commercial items. At the same time, says Campos, the NDAA requires "the secretary of defense to conduct a review of 'certain contract clause requirements applicable to commercial item contracts' and 'commercially available off-the-shelf item subcontracts,' while also requiring the Department of Defense to propose revisions to the Defense Federal Acquisition Regulation Supplement, which would eliminate regulations accordingly."

Perhaps one of most far-reaching streamlining efforts is the Section 809 Panel, named after the section of the 2016 NDAA that created it. The 18-member panel is exploring ways to streamline and improve the DoD's acquisition processes, and several of its initiatives focus on areas related to commercial item purchasing. The panel is expected to provide a comprehensive report to the House and Senate Armed Services Committees in early 2019 (see "Big Plans for Big Change," opposite).

Altogether, these efforts "indicate that the government in general is looking for better ways to buy these products and services and increase efficiency in commercial procurement," says Elizabeth Buehler, a counsel in Crowell & Moring's Government Contracts Group.

READY FOR REFORM

There are several reasons why those intentions may translate into meaningful change this time around. The government has made it clear that it wants to rely more on commercial items, especially when it comes to current and leading technologies. However, Buehler says, with the complexity of the purchasing processes, a growing number of companies have decided not to compete in the federal market—which only limits the government's ability to get what it needs.

The impact of that can be significant. In its May 2017 interim report, the Section 809 Panel noted that a convoluted acquisition process "makes DoD an unattractive customer to large and small firms with innovative, state-of-the-art solutions." That, in turn, could cause the Defense Department to fall behind in rapidly evolving technology. "Essential equipment needed on the ground may be either unavailable to the department or egregiously tardy, leading to genuine threats to the nation's security," the report noted.

Overall, says Buehler, "there's a theme that if the government wants more involvement from the private sector, the government needs to make it easier for companies to enter the federal marketplace."

The current political landscape may also give streamlining efforts a boost. "The idea of simplifying commercial item procurement comports with the administration's goal of simplifying regulations," says Burton. In addition, the procurement process has been used to some extent as a way to push social and economic policies, which always have to be balanced with the need for efficiency—and today, the pendulum seems to be swinging toward efficiency. Finally, he says, "you have one party in control of the House, Senate, and White House, so there may be an opportunity to get some acquisition reform legislation passed."

In this environment, government contractors are likely to have opportunities to weigh in on the issues. The Section 809 Panel, for example, is involving companies in meetings and seeking commentary from industry about process improvements. Says Campos, "The stars are somewhat aligned right now for industry to be much more vocal and to make contributions to improve government purchasing processes."

TAX

NEW BURDENS FOR THE IRS

In 2018, tax regulation writers at the Internal Revenue Service and the Department of the Treasury face a perfect storm of demands to produce new regulations, fewer resources, and judicial and executive scrutiny of their regulation-writing procedures. Their response will influence the tax law and practice for years to come. In the short term, taxpayers may see the IRS and Treasury rely more on informal guidance, such as rulings, notices, press releases, and FAQs on IRS.gov. Longer term, expect an increase in tax controversies and litigation challenging that informal guidance and the manner through which the guidance is adopted.

Congress's enactment of the Tax Cuts and Jobs Act of 2017 means that the IRS and Treasury have to quickly produce a slew of new regulations. The TCJA is the most significant overhaul of the tax code in a generation. It makes fundamental changes to the taxation of corporations and pass-through entities and creates new international taxes as well as different classes of taxpayers and income that are taxed differently. It is up to the IRS and Treasury to implement those changes. In November, Treasury estimated that the then-proposed bill included 80 delegations of regulation-writing authority.

At the same time, the IRS is facing a budgetary and manpower crisis that will severely hamper its ability to staff these projects. The IRS budget fell 10 percent from 2010 to 2017, and its staff fell 20 percent from 2012 to 2016.

Meanwhile, the IRS and Treasury regulations are facing increased scrutiny by the courts and the White House—particularly with respect to their adherence to the procedures that apply to agencies like the IRS when promulgating regulations. "The IRS has been pulled sort of kicking and screaming into the modern law related to issuing regulations," says David Blair, a partner at Crowell & Moring and chair of the firm's Tax Group.

THE RULES OF REGULATION

- **The Administrative Procedure Act**, signed in 1946 by President Harry S. Truman, established rules by which U.S. agencies propose and establish new regulations. The APA generally requires that an agency file a notice about a proposed regulation in the Federal Register and then solicit public comments. An extensive body of case law applying the APA clarifies that an agency must engage in "reasoned decision-making" in the notice-and-comment process, including addressing points raised in the public comments.

- **Executive Order 12866**, issued in 1993 by President Bill Clinton, established additional executive branch procedures requiring cost-benefit analysis by the Office of Management and Budget Office of Information and Regulatory Affairs of "significant regulatory actions," defined broadly by the anticipated effect of the regulation on the economy.

For many years, the IRS took the position that tax regulations were not subject to the Administrative Procedure Act. More recently, however, a series of cases, including the Tax Court's decision in *Altera v. Commissioner*, made it clear that the IRS and Treasury are subject to the APA no differently than other agencies, have to follow notice-and-comment procedures, and must engage in reasoned decision making.

The IRS also took the position that almost all Treasury regulations were not "significant regulatory actions" that required OIRA cost-benefit analysis under EO 12866, in part on the theory that the tax statutes alone create economic burdens and the tax regulations merely interpret those statutes.

"The IRS has been pulled sort of kicking and screaming into the modern law related to issuing regulations." —*David Blair*

"Taxpayers may be able to challenge tax regulations, at least in a class of cases, ahead of time, without incurring the tax in question." —*David Fischer*

TRUMP WEIGHS IN

In 2017, the Trump administration issued an executive order that pointedly told the IRS to reconsider its views on whether Treasury regulations constitute significant regulatory actions.

Executive Order 13789 directed Treasury and the IRS to identify "significant tax regulations" issued since January 2016 that impose undue financial burden, add undue complexity, or exceed IRS statutory authority. It also told them to "reconsider the scope and implementation of existing exemption for certain tax regulations from the review process."

That prompted Treasury and the IRS to reconsider 105 IRS regulations issued since January 1, 2016. The result? "To no one's surprise, they found that more tax regulations imposed 'significant' regulatory burdens than previously thought," says David Fischer, a tax controversy and tax litigation partner at Crowell & Moring.

UNINTENDED CONSEQUENCES

The IRS and Treasury now recognize that in many cases they are required to follow the reasoned decision-making standard of the APA and conform to the OIRA procedures, including cost-benefit analysis, before adopting tax regulations. The new procedures, and the increased scrutiny of the IRS and Treasury's regulation-writing process by the courts and the administration, when coupled with the 2017 tax reform and recent IRS budget cuts, may have negative effects on the development of tax guidance and ultimately lead to more tax controversy and litigation. The IRS is ill-equipped to take on additional regulation-writing responsibilities and, at the same time, improve its notice-and-comment rulemaking process to meet the standards imposed by the APA and EOs 12866 and 13789.

There are two questions, says Blair. How will the IRS get all that work done, and what kind of regulations will it issue? "They don't have the resources to write a whole bunch of new regulations," he says. So there is going to be a significant amount of time between when the law is written and when the IRS issues new regulations.

During that period, Blair says, the IRS may rely on informal guidance in the form of notices and press releases. In recent interviews, Treasury officials have conceded as much. "That is the more troubling piece," Blair says, because informal guidance doesn't go through the notice-and-comment process, "yet as a practical matter, IRS field agents and appeals officers tend to follow IRS informal guidance."

Fischer adds that we will see challenges to informal guidance under the APA. "Whether challenges to IRS guidance for failure to satisfy the APA will be successful is yet to be seen," he says. In the meantime, he notes, it is easier for extreme positions to make it into informal guidance.

A CRACK IN THE IRS'S ARMOR

The IRS and Treasury already face tough adjustments as they adhere to federal rules for issuing new regulations. A recent court ruling could make things worse.

A U.S. District Court in Texas sided with the U.S. Chamber of Commerce when it sued the IRS on behalf of its members, charging that the agency scuttled a merger between Irish and U.S. drug makers because of the potential tax burden from the agency's "anti-inversion" regulations.

The Chamber of Commerce decision represents a possible major change to the process of challenging tax regulations because the taxpayer succeeded in challenging a tax regulation before paying any taxes under the regulation, says Crowell & Moring's David Fischer. "Taxpayers have tried preemptory challenges to tax regulations many times, with no success," he says.

The Chamber of Commerce argued that IRS anti-inversion rules "chilled and killed the merger," says Fischer. They argued on behalf of the drug companies, "We were hurt even though we don't owe tax yet."

Other federal agencies often face such preemptory challenges to regulations, but the IRS has consistently won in court, he says. The Internal Revenue Code includes an anti-injunction act and a declaratory judgment act providing that taxpayers may not sue to restrain assessment or collection of tax. These acts protect the IRS's ability to collect taxes necessary to operate the government. This time the court ruled the acts didn't apply.

"This doesn't happen in the tax area," Fischer says. "It may be that there is now a crack in the armor. Taxpayers may be able to challenge tax regulations, at least in a class of cases, without incurring the tax in question." The federal government is appealing.

ENFORCEMENT

DESPITE A SOFTENING IN REGULATIONS, ENFORCEMENT CONTINUES

The Trump administration's focus on reducing government regulation continues, but reduced regulation does not necessarily mean government enforcement will abate. In fact, steady enforcement continues, and agencies are focusing their resources on the administration's priorities.

"The regulatory landscape is fluid," says Paul Rosen, a white collar, investigations, and cybersecurity partner at Crowell & Moring and a former federal prosecutor and chief of staff for the Department of Homeland Security. "It will evolve and change with significant events, and companies need to stay prepared and nimble."

Even with an overall softening in regulation, there are several key areas where the federal government will devote significant enforcement resources, such as drug trafficking, violent crimes, and immigration enforcement. And in the areas that the administration may not consider top priorities, such as consumer protection, in many cases, state attorneys general are likely to step up and fill the regulatory voids.

HEALTH CARE FRAUD AND OPIOIDS

Health care fraud clearly has the Trump administration's attention. Attorney General Jeff Sessions affirmed his support for prosecution of health care fraud, and civil and criminal enforcement across the health care industry continues unabated.

But that support comes with a caveat. "We will not likely see a significant number of new regulations, which means outdated and ambiguous regulations will continue to present a challenge for companies in the health care industry," says Laura Cordova, a partner in Crowell & Moring's White Collar & Regulatory Enforcement and Health Care groups who served as assistant chief and head of the Corporate Health Care Fraud Strike Force in the Fraud Section of the Department of Justice Criminal Division. "A lack of new regulations could actually have negative implications for companies that struggle to develop new and innovative business models that comply with ambiguous or outdated regulations," she adds.

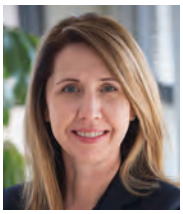
In addition, some resources that were typically focused on traditional health care fraud are now being diverted to the opioid crisis, something the Trump administration has said is a top priority. "On the enforcement side," Cordova says, "when an investigator has a dozen cases sitting on her desk and one of those cases involves opioids, it will get the investigator's attention. Even though it might not be the biggest case with the highest dollar value, it will get attention because the administration has made clear that its strategy to address the opioid crisis includes prosecuting those engaged in illegal activity involving opioids."

FIGHTING FINANCIAL CRIME

Anti-corruption, foreign bribery, and securities fraud—offenses that occur across a broad range of industries and companies—are going to stay firmly in the government's crosshairs. "DOJ continues to focus on financial crimes, and that is likely to continue," Rosen says. These investigations include a more focused effort to work closely with foreign governments, to the point of embedding DOJ officials with law enforcement agencies overseas to increase cooperation in parallel cross-border investigations. Such cooperation will make it easier for federal investigators to get access to foreign evidence and witnesses that are otherwise potentially outside the reach of U.S. authorities.

Rosen notes that the Trump administration has clarified how it expects companies to stay in compliance with the Foreign Corrupt Practices Act. It recently unveiled a revised FCPA enforcement policy that essentially made permanent many provisions of a pilot program started under the Obama administration. However, the Trump policy comes with one key additional olive branch: a presumption of a criminal declina-

"The regulatory landscape is fluid. It will evolve and change with significant events, and companies need to stay prepared and nimble." —*Paul Rosen*



"We will not likely see a significant number of new regulations, which means outdated and ambiguous regulations will continue to present a challenge for companies in the health care industry."

—*Laura Cordova*

tion (no criminal charges) if a company voluntarily self-discloses misconduct and cooperates early and fully.

"We're continuing to see large FCPA and securities fraud cases," says Cordova. "Enforcement continues at much the same pace, which is to be expected because prosecutors are making their cases. It's not as if the whole workforce changed with the administration."

BATTLING THE BREACHES

Over the past year, many have learned what experts and security insiders have long known: cybersecurity threats and attacks are here to stay. As digital attacks on companies such as Yahoo!, Equifax, and Uber—and even the SEC—have dominated headlines, the stunning speed with which the Petya/NotPetya ransomware viruses attacked thousands of companies around the world further underscores the seriousness, permanency, and global nature of the threat.

The government and the private sector are working hard to manage existing threats and prevent future attacks on their networks and systems. Meanwhile, courts are wrestling with damage claims by shareholders and consumers whose information may have been taken. As high-profile breaches continue, the government will keep evaluating and refining its asset protection and consumer protection regulatory role.

"Increasingly sophisticated cyberattack capabilities are a boon to criminals and state-sponsored actors seeking to get rich or wreak havoc from afar," says Rosen. "No longer does somebody have to walk into a bank to rob it—they can simply conduct a ransomware attack from halfway around the world. And foreign adversaries that don't have the skill or the will to innovate can just try to hack American companies that do. The stakes are high, and American businesses are on the front lines."

The government is taking the cybersecurity challenge and threat seriously. It has the unique ability and set of tools to hold hackers accountable, and it will continue to do so.

KEEPING UP WITH INNOVATION

Technology has defined American innovation and advancement. But recently it has presented regulatory uncertainty because of the rapid advances in autonomous automobile and drone technology and the issues they raise regarding physical safety, cybersecurity, consumer protection, and insurance. In a sign of how the administration is approaching its regulatory treatment of these technologies, the Department of Transportation and the National Highway Traffic Safety Administration issued new Automated Driving System guidance to encourage the development of self-driving cars while maintaining the safety of the roadways, with as little interference as possible from the federal government. In doing so, it relaxed the already flexible guidance issued at the end of the Obama administration.

The DOT and NHTSA guidance demonstrated that the Trump administration will, as expected, take a hands-off approach as companies roll out products based on the new technologies, Rosen says. "But the regulatory rope that these companies enjoy could quickly be curtailed if a significant cybersecurity or physical safety incident occurs, or if the power in Congress shifts—which is why businesses should tread carefully in this space," he adds.

HOLDING INDIVIDUALS ACCOUNTABLE

As part of its new policy on the FCPA, the Department of Justice sent a message that it is continuing its focus on individuals by maintaining pressure on companies to turn over information on culpable individuals.

The FCPA policy announcement followed an October 2017 speech in which Deputy Attorney General Rod Rosenstein previewed that any changes to the policy detailed in the Yates Memo would reflect a continued resolve to hold individuals accountable for corporate crime.

The Yates Memo was the September 2015 pronouncement by then-Deputy Attorney General Sally Yates that called on DOJ prosecutors to focus their resources on investigating and charging individuals involved in criminal activity even when the crimes were committed on behalf of a corporation.

When it comes to individuals, Crowell & Moring's Laura Cordova says there is likely to be little change to the policy and practice that individuals should be criminally charged where the evidence supports it. Indeed, we are likely to see a continued focus on prosecuting individuals. In the end, the government—and in particular DOJ—will continue to enforce laws by bringing civil enforcement actions and criminal charges against individuals and corporations across industries.

HEALTH CARE

MERGERS: KEEPING CARE COMPETITIVE

The U.S. government has made it a top priority to make sure that any consolidation in the health care industry doesn't hurt competition, and it has been aggressive in trying to block mergers that it believes will hurt consumers.

That campaign has resulted in several key litigation victories for the government that show what types of transactions raise concerns with the federal government, providing valuable information for merger-minded health care companies preparing to navigate the antitrust waters.

The Department of Justice and the Federal Trade Commission represent a powerful combination in the federal government's efforts to keep health care competitive, with DOJ reviewing mergers involving insurance plans and the FTC reviewing mergers involving hospitals and physician groups.

DOJ won two big cases in 2017 when a federal judge blocked Aetna's $37 billion takeover of fellow insurer Humana just a few weeks before another federal judge stopped Anthem's $54 billion merger with Cigna. In both cases, DOJ argued that the marriage of two rivals would hurt competition.

That came in the wake of major wins for the FTC in late 2016, when separate appellate court decisions reversed lower-court decisions to side with the agency's efforts to block two hospital system mergers: the combination of Chicago's Advocate Health Care Network and Northshore University Healthcare System, and the tie-up of Penn State Hershey Medical Center and PinnacleHealth System in the Harrisburg, Pennsylvania, area. The FTC said both of those transactions would harm competition in local geographic areas.

Those victories were part of a revitalized antitrust campaign that the government launched in the early 2000s focused on hospital mergers that has gained traction in the courts.

Although the court decisions stopped these mergers, they still provide helpful intelligence for what kinds of acquisitions and mergers companies can pursue in the rapidly changing health care landscape, says Joseph Miller, a partner at Crowell & Moring and a member of its Antitrust and Health Care groups.

Health insurers and hospitals are both working in an uncertain atmosphere in terms of how health care reform and shrinking Medicare and Medicaid payments will affect them. "One way they think about dealing with those systemic changes is bulking up through acquisitions," Miller says. "Now there is more legal clarity that can affect the way they think as they go forward in their business strategy."

The most important takeaway is that "horizontal" combinations of head-to-head competitors, as all the blocked cases were, may face significantly greater antitrust hurdles than "vertical" mergers, in which the merging companies have complementary businesses and don't compete.

WHEN THE FEDS AND STATES PART WAYS

Health care is one of the FTC's primary focus areas. In the four-year period between 2013 through 2016, 50 percent of FTC enforcement actions involved health care, pharmaceuticals, and medical device companies, FTC statistics show. "Using enforcement as its primary tool, the commission works to prevent anticompetitive mergers and conduct that might diminish competition in health care markets," the FTC says in its mission statement.

That mission has produced results for the agency. "For about the past decade, the FTC has been on a winning streak in hospital and health care provider merger enforcement," says Alexis Gilman, a partner at Crowell & Moring and a member of its Antitrust Group. But the health care providers that have been on the losing side argue the FTC doesn't fully appreciate the challenges they face or fully account for the benefits of mergers.

"Now there is more legal clarity that can affect the way [health insurers and hospitals] think as they go forward in their business strategy." —*Joseph Miller*

"It is less risky from an antitrust perspective to look for merger partners in adjacent markets as opposed to partners in your local geographic area." —*Alexis Gilman*

"Health care providers generally try to explain that they are doing these mergers to gain efficiencies, lower prices, improve quality, and really tackle health care challenges in their local communities," Gilman says. "Their view has been that federal antitrust law has gotten in the way or doesn't understand those challenges."

While that argument hasn't been persuasive at the federal level, some states are more sympathetic. When health care providers think the FTC has a good chance of successfully suing to block their merger on federal antitrust grounds, some are turning to their state legislatures for something known as "state action immunity." Recently, certain state legislatures have passed laws creating a state system of active regulatory oversight displacing federal antitrust laws, and giving the merging health care providers immunity from federal (and sometimes state) antitrust liability.

That is what happened in West Virginia in 2015. The FTC sued to block Cabell Huntington Hospital's purchase of St. Mary's Medical Hospital on antitrust grounds even though West Virginia's attorney general had already approved the deal. To save the merger, the West Virginia legislature created a new system for the state to approve or reject health care providers' so-called cooperative agreements. Soon afterward, the merging parties' cooperative agreement was approved by the state health care authority, and the FTC dropped its opposition.

NEIGHBORING STATES TAKE NOTICE

The success of that deal, despite FTC opposition, could prompt similar attempts by other health care companies whose planned merger is headed for federal antitrust trouble, Gilman says.

A case in point is Mountain States Health Alliance and Wellmont Health System. Following in West Virginia's footsteps, Tennessee and Virginia recently passed "Certificate of Public Advantage" (or COPA) and cooperative agreement laws, respectively. Mountain States and Wellmont sought approval of their merger, and state action immunity, under these laws. Recently, both states approved the merging hospitals' applications, subject to certain conditions. The FTC hasn't signaled any interest in trying to block the merger following the states' approvals. Gilman says, "If West Virginia is any indication, it will probably not challenge the transaction."

Now that three states have adopted this tactic to circumvent the FTC and federal antitrust law, there is precedent. "So if you are a hospital and you want to get your deal through and you think the FTC is going to challenge you, this is another path forward," says Miller.

But the U.S. government isn't likely to sit back and watch if too many more hospital systems that it would have otherwise blocked from merging decide to seek state help. "If you see a continuing trend toward hospitals seeking immunity to get deals done, you can anticipate a counterreaction from the federal government," says Miller.

Miller and Gilman both predict that DOJ and the FTC will continue to aggressively challenge health care mergers. Adds Gilman, "If health care providers are looking for a transaction to add scale or generate efficiencies, it is less risky from an antitrust perspective to look for merger partners in adjacent markets as opposed to partners in your local geographic area."

GETTING STATE SUPPORT

When the federal government steps in to block a health care merger, it likes to have a state's attorney general standing by its side in filing a complaint.

"For the FTC, having state support is particularly important in health care cases, where the markets are very local," says Crowell & Moring's Alexis Gilman. "The agency is sensitive to the perception that it is the big, bad government coming in to tell the state or local community how to run health care."

State AGs are also known to intercede and file suit on their own even when the federal government doesn't. "Health care antitrust cases are almost by definition local because that is the way health care is delivered," says Crowell & Moring's Joseph Miller.

One thing to watch in health care antitrust enforcement is whether the state attorneys general end up playing a bigger role in policing antitrust violations in the health care industry under the Trump administration. "If for whatever reason the health care antitrust enforcement were to slow down during this current administration, you'd still have the states out there as enforcers of antitrust," says Gilman.

PRIVACY & CYBERSECURITY

RISKY BUSINESS: PREPARATION, PREVENTION, REGULATION

DATA BREACHES: DEALING WITH THE AFTERMATH

Data breaches have become more and more common, to the point that companies essentially have to assume that sooner or later, they will experience one. That makes it critical to have a clear understanding of the regulatory requirements for notifying regulators and affected individuals in the wake of a breach. But the rules don't always make that process clear.

In the U.S., there is no single federal law covering breach notifications, but there are quite a few at the state level. Today, 48 states (in addition to the District of Columbia, Guam, Puerto Rico, and the Virgin Islands) have some type of breach notification laws in place—with Alabama and South Dakota being the exceptions. "If a company experiences a breach of personally identifiable data about customers in one of these jurisdictions, it is obligated to notify those individuals, as well as regulators," says Jeffrey Poston, a partner at Crowell & Moring, co-chair of the firm's Privacy & Cybersecurity Group and a member of its Litigation Group. "A large company could easily be subject to dozens of state laws—if not all 48."

State notification laws typically define factors such as what constitutes a breach, what type of notice has to be given, and who must be notified—and these details can vary. For example, says Poston, "there are different triggers for having to notify the state attorney general. Some states say the breach has to involve more than 500 people; others say notifications are required based on the incident itself, regardless of the number of residents affected." The time frames for notifying individuals also vary—some states don't have a notification deadline except that it must be made without unreasonable delay; many states allow 45 or 90 days. Florida, with the strictest deadline, provides just 30 days for notice to be given.

Different states are likely to apply different degrees of scrutiny, as well. "Some state regulators just don't have the resources or the technological expertise to really mount a formidable investigation," says Poston. "Some are more aggressive than others—but, of course, that will depend on how many of the state's citizens are affected by the breach."

Beyond all those state laws, companies also need to be aware of a growing trend toward industry-specific federal regulations that include provisions covering data breaches. HIPAA has such notification requirements for the health care industry, and the Defense Contracting Agency has them in the DFARS (Defense Federal Acquisition Regulation Supplement) regulation. Even commercial agreements are starting to address the issue. "You may have to notify your business partners of a breach if you're handling data on their behalf or if you've got contracts that require you to notify them," says Poston.

Congress is aware of the challenges that companies face in trying to find their way through this thicket of notification requirements. A number of related bills have been proposed in recent years—including one in November 2017, the Data Security and Breach Notification Act. This legislation would preempt state laws and standardize notification requirements, provide a 30-day notification deadline, and call for prison sentences for those knowingly concealing a breach. However, these legislative efforts have so far failed to gain much traction—and for the time being, companies will have to navigate the nuances and variations across jurisdictions.

"You don't want to compound the problem by sending out an untimely or inadequate or incomplete notification to regulators and affected individuals." —*Jeffrey Poston*

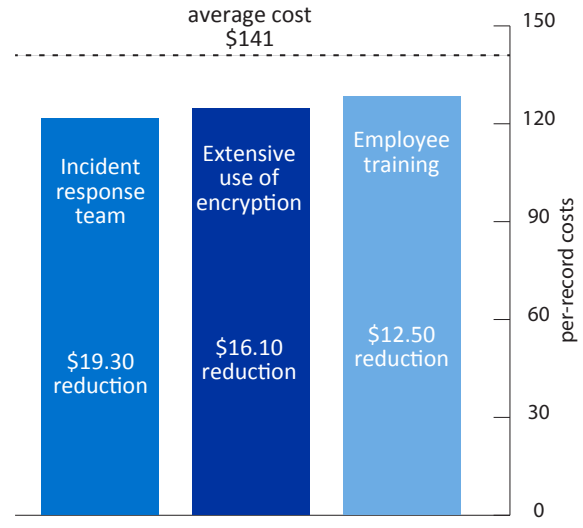
AN OUNCE OF PREVENTION

In this environment, companies should have a rigorous incident response plan in place. This plan should spell out how investigations and notifications will be handled and, as much as possible, try to anticipate problems that might arise. "As general counsel who have been down this road know, this can get complicated," says Poston. "You have to commence a privileged investigation right away, which typically involves very tricky forensic and technical information. It can take a lot of time and effort just to find out what data has been accessed or stolen and who has been affected."

Nevertheless, companies need to produce notifications that are both timely and accurate. "You've got just one shot at this," says Poston. "You don't want to compound the problem by sending out an untimely or inadequate or incomplete notification to regulators and affected individuals." Regulators will take a dim view of language that appears to be downplaying the problem, and if the notification (and related press releases) turns out to have significant errors, the company may have to re-notify everyone. "A breach is bad and embarrassing, but with today's news cycles, something else is likely to come along the next day

PREPARATION PAYS OFF

On average, a data breach costs a company $141 per compromised record. But research shows that certain activities can reduce those per-record costs.



Source: "2017 Cost of Data Breach Study," Ponemon Institute

A LONG TO-DO LIST

When a company experiences a significant cybersecurity breach, the range of necessary follow-on actions can be daunting. For example, legal departments will typically have to contend with:

- Deciding whether and when to provide notification to individuals and regulators, looking across dozens of state laws.
- Creating notifications that are timely and accurate.
- Communicating with external sources, such as media, law enforcement, and consumer-reporting agencies.
- Preparing statements, email notices, and personalized correspondence to reach employees affected by security incidents.
- Determining whether and how to provide post-incident assistance, such as credit-monitoring services or insurance, to affected individuals.
- Engaging a forensic investigation team covered by legal privilege.
- Assessing and addressing any criminal, employment, contract, or other legal issues arising from incidents that involve the conduct of an employee, vendor, or business partner.
- Defending against state and federal regulatory investigations, state attorneys general lawsuits, and individual and class action lawsuits arising from data and privacy breaches.

Later, when the crisis is under control, companies should conduct a "lessons learned" analysis of the incident and the response. This should focus on identifying potential improvements in privacy and data security—and the response plan itself—in order to reduce risk and limit the damage from future incidents.

that gets people's attention," says Poston. "You don't want to have to come back and re-focus the spotlight on yourself."

Response plans should consider possible litigation, as well as regulatory developments. With large data breaches, companies usually conduct an investigation to determine if a notification is necessary and, if it is, go through the notification process. But that may be just the beginning. "All of a sudden," he says, "you could have federal regulators opening up an investigation, state regulators opening up an investigation, and class actions being filed—and now you're in a three-front war. So you've got to be able to deal with each front in a way that doesn't jeopardize you on the other two."

With all these factors in play, response plans should be in place well before a breach happens. "You don't want to be reacting on the fly to a crisis," says Poston. "You want a plan that's been tested through dress rehearsals, fire drills, and tabletop exercises. Then, when there is an event, you have the muscle memory to react to it in an efficient, effective manner—without a mad scramble."

MEETING CLIENTS' EXPECTATIONS

Cybersecurity, a main concern for companies of all stripes, is of the utmost importance to law firms, where the protection of confidential client information is paramount.

Hackers, from lone wolves to nation-states, have figured out that law firms are a back door to the secrets of some of the world's top companies.

"Everybody is a target, no matter how big or how small, how important or unimportant they think they are," says Mark Sportack, chief information officer at Crowell & Moring. "Cyber is a scary thing."

So scary, in fact, that law firms must devote time, resources, and attention to making sure they are protected. "The only way to defend yourself in an environment with unknown, unseen risk is to have many, many layers of overlapping defenses," Sportack says.

RAMPING UP PROTECTIONS

"No law firm is ever fully prepared, and we are constantly benchmarking and looking to upgrade our protections," says Sportack, who runs Crowell & Moring's cybersecurity systems and strategy, adding that the ever-evolving nature of cyberattacks makes them a tough threat to effectively head off.

Crowell & Moring, like most law firms, takes cyber threats very seriously, viewing cybersecurity as a major new element of the attorney-client relationship. Sportack oversees a team that takes a multi-step process to safeguard the firm's network and sensitive data, working to ensure that its cybersecurity meets clients' exacting expectations.

First, Crowell locks down the computers it provides to employees so that nobody has local administrator privileges and therefore can't change the operating environment. "If you do that, you can address up to 80 percent of the risks you're facing," Sportack says.

Next, the firm requires that all remote access clear two levels of authentication. In addition, the firm locked away all administrator and other privileged access accounts to make sure they are activated only when specific operating environment changes are needed.

DELAY CREATES HACKING OPPORTUNITY

In addition, Sportack has a dedicated team available at all times to identify and fix security vulnerabilities as they occur. "You want to have a rigorous patch-management program because delay creates opportunity," he says.

The final piece in the protection pie is properly training employees about cybersecurity risks and how to deal with them. "The single biggest weak link in any given network is going to be the people," he says. A law firm might not be able to completely train user mistakes away, but Sportack says it can train them down to a minimum.

With the potential fines, investigation expenses, and reputational costs associated with data breaches, those response plans are likely to be well worth the effort. With the growing frequency and visibility of breaches, the public has become somewhat desensitized to news about security compromises. As a result, says Poston, "you have a chance of being forgiven by your customers if you experience a breach. But you have very little chance of being forgiven if you don't respond in an effective way to notify and protect them. If you don't act nimbly, it's not going to sit well with those individuals—or with regulators."

BRINGING HARMONY TO THE EU

In Europe, companies have been contending with a fragmented privacy and security regulatory landscape much like that facing U.S. companies. But that is about to change, when the EU General Data Protection Regulation goes into effect in May 2018.

For more than two decades, the protection of personal data has fallen under the EU's Data Protection Directive 95, which

"The only way to defend yourself in an environment with unknown, unseen risk is to have many, many layers of overlapping defenses." —*Mark Sportack*

THE SOFT UNDERBELLY OF THE SUPPLY CHAIN

As in any battle, the cybersecurity war has its hard and soft targets. Defense contractors have long been targets of hacking attacks and now have so many digital defenses that they are no longer worth the time and effort it would take for a successful breach. So hackers have turned their attention to the companies that supply the major defense contractors, in the hope that a successful breach in the supply chain will work its way back up into the defense contractor's network. This has national security implications, because the Chinese, Russian, and Iranian governments have been implicated in recent global cyberattacks.

Law firms face exactly the same risk. "Foreign nation-states are recognizing our clients as very hard targets," Sportack says. "They realize that in a lot of ways, we're an equally hard target. So now they're reaching into our supply chain. They're attacking companies two levels removed in the chain of commerce from their actual target."

TAKING THE FIGHT TO THE SUPPLIERS

To counter that threat, Crowell & Moring has begun systematically vetting all its vendors to make sure that they meet its strict cybersecurity requirements—standards that seek to meet the demands of the firm's clients. "We are taking the fight to them," Sportack says.

All new vendors must pass the cybersecurity test or they are turned away. The law firm is also starting to hold existing vendors to the same standards. So far, roughly one in three existing vendors isn't making the cut and has to be dropped.

All law firms now recognize that they (and therefore their clients) are vulnerable to cybersecurity attacks. A 2017 survey of more than 200 law firms by LogicForce found that 80 percent are not vetting their third-party vendors' data practices. That can and will change. By definition, no cybersecurity system is impenetrable. But Crowell & Moring is working every day to make that system more secure.

provided some harmonization of regulations. However, EU directives provide only a regulatory framework with minimal rules, which then need to be incorporated into national laws in member states. As a result, those laws have often diverged, leaving significant variations in regulations across the EU.

"Spain has had very strict data protection regulations, and regulators in France, the U.K., and Germany have been very active," says Maarten Stassen, a senior counsel at Crowell & Moring and a member of the firm's Privacy & Cybersecurity Group. "On the other hand, in other countries such as Belgium, the data protection authority had a more advisory role but could not impose any sanctions in case of a data breach. These different approaches made it quite challenging for companies to be compliant."

The GDPR essentially replaces the EU Data Protection Directive. As a regulation, it will be directly applicable in all EU member states as of May 25, 2018. Individual countries have leeway to make some adjustments, but "in general there is a much more harmonized approach," says Stassen. Under the GDPR, there is still no single enforcement authority. Instead, each country has an independent supervisory authority that hears complaints and applies sanctions. The activities of these various authorities are coordinated by a European Data Protection Board that helps ensure consistent enforcement across the EU.

Along with the harmonization of regulations, the GDPR was developed to help "move privacy and the protection of personal data up higher on companies' agendas," says Stassen. To that end, the regulation provides significant penalties for noncompliance and data breaches. These can be as much as 4 percent of a company's annual revenues, or up to €20 million, whichever is higher. While those top fines might not be levied immediately, the risk is significant, and "these potential fines have succeeded in getting the C-suite's attention and getting this on boards' agendas," Stassen says.

Much of the GDPR is based on the previous EU directive, so the concepts behind it are familiar to companies doing business in Europe. But there are some key changes. In addition to the substantial fines now on the table, for example, the GDPR requires companies to notify authorities of a breach—a requirement familiar to U.S. companies but not covered under previous regulation. It also requires that such notification happen quickly—within 72 hours of a breach being discovered. "In general, the big differences are that the GDPR makes companies more accountable and requires them to demonstrate to authorities that they are in compliance," says Stassen.

These new rules do not apply only to European companies. U.S. companies with a physical presence in the EU will also need to comply. What's more, the GDPR will also apply to com-

THE EU'S BILL OF DATA RIGHTS

The GDPR grants a number of rights to individuals, or "data subjects." Companies are obligated to respect those rights in their handling of data.

- Right to information—the right to receive detailed information about the processing of personal data collected from the data subject or from other parties.
- Right of access—the right to obtain confirmation from the controller—the party that determines how the data will be used—as to whether the subject's personal data is being processed and, if so, the right to access and receive certain information about personal data stored by the controller.
- Right to rectification—the right to rectification/correction of personal data that is inaccurate, and to have incomplete personal data completed.
- Right to erasure ("right to be forgotten")—the right, under certain circumstances, to have personal data deleted.
- Right to restriction of processing— the right to require that the use of personal data be limited.

"If the people in the business don't know that's a requirement, then they can't comply with the regulation. So these things need to be built into business processes." —*Maarten Stassen*

panies located in the U.S. that actively market to EU citizens and gather their personal data or monitor their behavior within the EU, as well as to companies that process data for these companies.

ADAPTING TO THE GDPR

In practice, the GDPR will require companies to make some operational changes. For example, it guarantees the "right to be forgotten," meaning individuals will have the right to request that companies in specific cases erase personal information from company records. While EU individuals already had significant data protection-related rights, it is likely that they will now exercise those rights more often, and companies will need to have processes in place to handle that. The regulation also raises the bar on how data usage consent is gathered from individuals. Consent, it says, must be informed, given freely, and apply to a specific purpose. Furthermore, it must be given in an unambiguous way. Therefore, companies will need to find ways to have individuals take "affirmative acts," such as opting in to provide consent. "Companies will need to demonstrate that individuals are actively making an informed choice," he says.

Among other things, the GDPR requires companies to keep records of data processing activities. This includes identifying the personal data they have, explaining how data privacy will be ensured, and justifying why they need that data—information that is used to show regulators that the company is in compliance.

Companies also need to conduct a data protection impact assessment (DPIA) before beginning any processing operations that pose a significant risk to individuals' information. This might be required when creating new customer profiles, using a new technology, or starting a program involving the monitoring of public areas on a large scale. If the assessment shows that risk would be high and requires actions to reduce that risk, companies will need to consult with the relevant supervising authority before proceeding and clarify how that risk will be mitigated.

The changes necessary to meet these kinds of requirements will be felt throughout the company. With the DPIA, for example, compliance is not just an issue for the company's law department. "Everybody in the company needs to be aware that when they are at the start of a new project or initiative that is going to do something new with personal data, they need to consider whether to do a data protection impact assessment," says Stassen. The same is true of the data breach notification rule. "If the people in the business don't know that's a requirement, then they can't comply with the regulation," he says. "So these things need to be built into business processes."

Effective GDPR compliance, Stassen continues, requires a "change of mind-set" in the company. That can mean adopting new policies and procedures, implementing new technology, and providing training to staff to increase GDPR awareness. Operations are usually relatively siloed at most companies, but data moves horizontally through the organization. "The GDPR forces you to look at the data flow beyond your silo and think about the whole business," he says. "Companies are going to have to look at their business processes through the lens of data privacy."

BRIDGING TWO WORLDS

The GDPR continues the EU's prohibition against transferring personal data outside of the EU unless certain conditions are met. But for companies in the U.S., the EU-U.S. Privacy Shield program provides a way to keep the data flowing.

Put in place in May 2016, Privacy Shield is a framework in which U.S. companies publicly certify that they will follow EU data privacy regulations, thereby gaining approval to move personal data from the EU to the U.S. Some observers have said that such programs are often little more than a "check the box" exercise. But that's not the case with Privacy Shield, says Crowell & Moring's Maarten Stassen. For one thing, he explains, "companies that sign up are really putting themselves on the radar of EU and U.S. regulators."

Those regulators are taking an active approach to the program. EU data privacy authorities have shown in the past that they are willing to follow up with companies to explore the processes being used to protect data. In addition, in September 2017, three companies agreed to settle charges from the U.S. Federal Trade Commission that they had misled consumers about their participation in Privacy Shield. A commission official noted the agency's "commitment to aggressively enforce the Privacy Shield frameworks," adding that participating companies "must keep their promises or we will hold them accountable."

Privacy Shield may not be perfect, says Stassen, "but it's a reasonable solution, and companies in the program need to make sure they have the compliance processes in place to back up their certification."

crowell moring

For more information, contact:

Scott L. Winkelman
swinkelman@crowell.com
Phone: 202.624.2972
1001 Pennsylvania Avenue NW
Washington, DC 20004-2595

To access an electronic version of this publication, go to www.crowell.com/regulatoryforecast

REGULATORY AS A COMPETITIVE DRIVER

The digital age is bringing radical transformation to companies of every shape and size—from new uses for data to new technology that is disrupting entire industries. The pressure to compete and achieve speed to market is intense. For corporate legal departments, it means the job is changing, as well. The rate of innovation is outpacing the regulatory framework that governs it—not to mention solutions for the risks that are identified along the way. Never before have in-house counsel and the law firms that serve them played a more pivotal role in helping to shape business strategy. And one of the frontlines in the race to innovate is found in the regulatory landscape, where compliance is making and breaking competitive advantages. The impact of technology underlies much of the content in this, our fourth annual *Regulatory Forecast*. We hope to hear from you about how you are navigating the digital age and where the discussion needs to go next.

—Phil Inglima
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 a look at how to position your company to survive and thrive in the data revolution, as well as a range of practice-specific, industry, and business-of-law sections. For an electronic version, go to www.crowell.com/litigationforecast.