# LITIGATION FORECAST 2020

WHAT CORPORATE COUNSEL NEED TO KNOW FOR THE COMING YEAR

Annual Jurisdictional Analysis

Non-Compete Agreements: Harder to Enforce?

# A Tangled Web

## How the Internet of Things and AI Expose Companies to Increased Tort, Privacy, and Cybersecurity Litigation

crowell moring

# LITIGATION FORECAST 2020

## Regulation by Litigation

Not so long ago, if you were expecting a legal battle, you probably knew where it would come from. If a safety regulation was being promulgated, you'd hear about it from OSHA. Now that battle may take the shape of a class action or many separate litigations across federal and state courts. If your competitor had a beef with your advertising claims, you'd be in front of the NAD or you'd hear from the FTC. Now you might end up in federal court under the Lanham Act or face down multiple class actions (see page 34). Antitrust mergers were once largely the purview of federal enforcers. Today the plaintiffs' bar has taken up that fight (page 12). Increasingly, the role between regulators and courts is being blurred as employees fight non-competes in court on public policy grounds (page 26), as the disabled pursue senior living facilities (page 22), as patent licensing fees are supposedly fought on behalf of the consuming public.

Today we are moving into an era of regulation by litigation, an era where plaintiffs' lawyers, government advocacy groups, and state attorneys general are stepping up to fill in when they think the federal government hasn't done its job. Navigating this new fraught environment, predicting what has become unpredictable, requires a new kind of focus. The articles in this year's *Litigation Forecast* are intended to help point the way. We hope you'll find them both helpful and inspirational. To keep the conversation going, please visit www.crowell.com/forecasts.

**Mark Klapow**
Partner, Crowell & Moring
Editor, *Litigation Forecast 2020*




CROWELL & MORING LLP

Creator and Editor Mark Klapow
Senior Editor and Project Manager Ezra Crawford
Associate Editor Jared Levine
Contributing Editors Nicole Quigley, Nicole Steckman

LEVERAGE MEDIA LLC

Editorial Director Michael Winkleman
Art Director Carole Erger-Fass
Writer Peter Haapaniemi
Chartist Olivia Reaney
Copyeditors Jerry Goodbody, Sue Khodarahmi
Project Manager Andrea Olstein
Production Manager Rosemary P. Sullivan





COVER: LuckyStep48/Getty

crowell moring

# Focus Areas









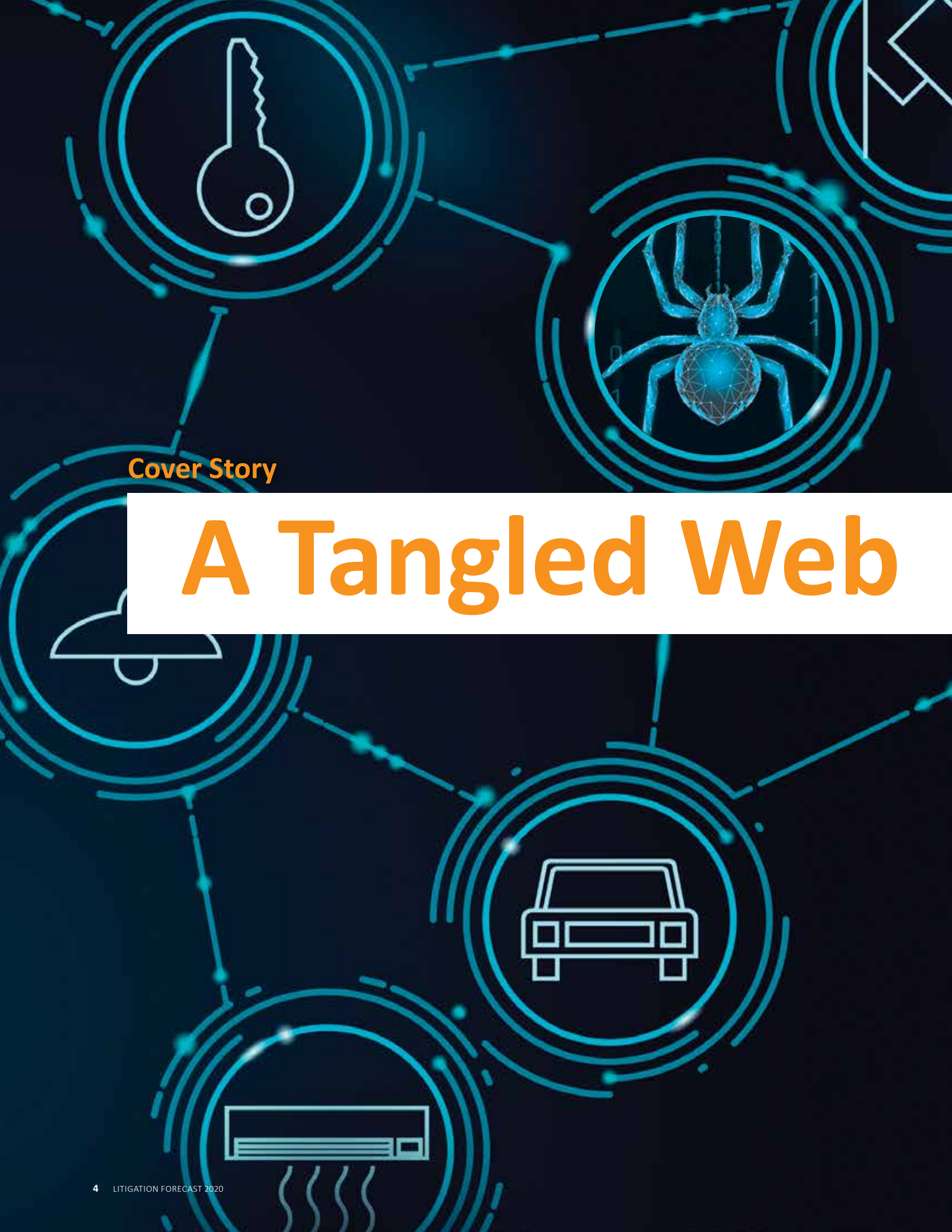








## Special Coverage



Cover Story

# A Tangled Web

# HOW THE INTERNET OF THINGS AND AI EXPOSE COMPANIES TO INCREASED TORT, PRIVACY, AND CYBERSECURITY LITIGATION

**NEARLY EVERY BUSINESS IS GOING THROUGH ITS OWN** digital revolution. And every day, more and more companies are realizing that they are a digital company—or need to become one. The digital revolution is transforming not only high-tech companies but also traditional industries whose products, business models, and workforces are being affected by increased connectivity, artificial intelligence, and the ability to collect and use tremendous amounts of data.

Manufacturers use robots and machine vision to make products, and they are building more "intelligence" into those products, from toys to autonomous vehicles. Electric utilities use smart grids to manage the distribution of energy. Agribusinesses use drones and advanced imaging to manage crops. Health care companies use 3D printing to customize medical devices. Chemical producers use collaborative technology, such as blockchain, to track the provenance of products. Banks use AI to improve service and personalize offerings. And the list goes on.

"The increasing sophistication of digitally enabled, intelligent products will drive new litigation in the coming years as these products are inevitably breached, either because a product fails or a cybersecurity incident occurs," says Jeffrey Poston, a Crowell & Moring partner and co-chair of the firm's Privacy & Cybersecurity Group in Washington, D.C. "Newer technologies have been commercialized to the point where people now have smart and internet-connected products in their homes, their cars, and their pockets. These products bring together components and technologies from an ecosystem of companies, and they are very complex and morphing all the time through updates and software improvements. When they fail, litigation will ensue and companies will scramble to reduce and redirect liability."

The rise of AI-enabled products raises new questions—and to date, regulators have not provided much insight into how AI should be used. "The main guidance that's out there is a basic standard that simply says that companies need to make sure that AI works in a way that doesn't create an unreasonable risk of injury," says Cheryl Falvey, a partner at Crowell & Moring in Washington, D.C., and former general counsel of the Consumer Product Safety Commission. "In product liability litigation, however, guidance is one thing and juries are another. In the courtroom, a jury is going to decide whether the things the company did in designing the product were enough to reduce the risk of AI not operating as it should. And when you combine artificial intelligence with the Internet of Things to create what

"The increasing sophistication of digitally enabled, intelligent products will drive new litigation as these products are inevitably breached." **Jeffrey Poston**

the industry calls AIoT, you are pioneering technologies that can impact consumers' lives in a powerful and positive way, but you are also opening up litigation risks that can make or break the long-term viability of a business."

In addition to digitally enabled products breaking, their reliance on vast amounts of data creates ever-evolving risks of breach. "As companies embrace digitalization, they are also facing a new realm of exposure," says Evan Wolff, co-chair of Crowell & Moring's Privacy & Cybersecurity Group in Washington, D.C., and a former data scientist and Department of Homeland Security advisor. That exposure is driven by two phenomena: the increasing sophistication of cyberattacks, and the growing array of statutes and regulations governing data security and, increasingly, data privacy. While the new regulations vary, many create litigation opportunities for regulators, class action plaintiffs, and even whistleblowers—and raise the stakes of that litigation significantly. As a result, says Wolff, "the legal impact of cyber and privacy risk is not just an IT or security issue, and it is not only connected to the possibility of a system breaking. It affects the health and even the survival of the entire business."

## Litigating the Internet of Things: When Breaks Harm Consumers

The emergence of smart, connected products has been rapid and widespread. According to the World Economic Forum, there will be more than 20 billion devices connected to the Internet of Things by the end of this year, from smart watches to doorbells, refrigerators, security cameras, and voice-powered assistants. The first wave of product liability attacks against IoT devices foundered on a basic legal problem: the products had not failed. Plaintiffs' lawyers tried to create causes of action based on the potential for failure, but those claims were dismissed for lack of standing.

Now, however, as more IoT devices are in service and performing critical life- and safety-protecting applications, product failures have begun. And as breaks occur, a new wave of tort litigation threatens to derail a company's digital business innovations.

These digitally enabled products, which often involve components from many suppliers and partners, are not only subject to traditional problems such as defective batteries. They can also run into software and connectivity issues that can impair their performance and even lead to safety concerns. These can be difficult to sort out. "With these complex products, we now have enough experience to know that it's never easy to figure out exactly which component or software led to an issue," says Falvey. "We are going to see even more finger-pointing in court about who's liable, as different suppliers dispute whether they are responsible for the product's failure."

Consumer warnings and disclaimers do not necessarily provide protection. The current race to market can drive companies to add functionalities that are sometimes unproven. "There's a general feeling among tech start-ups that you can just disclaim or warn away that lack of performance as a software 'glitch,'" says Falvey. "But when that performance glitch relates to safety, a warning may not be enough. The law is very clear that if you can design away a product defect, you can't just stick a warning on the product and hope things don't go wrong."

The growing role of software also creates some special challenges for litigators. "You might have several software developers contributing to the functionality of the product," says Falvey. To get to the root of the problem, companies may need to carefully scrutinize each piece of software. "But you might not have the right to look into that proprietary software," she says. "So we think there will be litigation fights over discovery asking for software source code as companies try to figure out what went wrong."

One type of software in particular—AI—will play a growing role. With AI, the technology, rather than the consumer, makes various decisions about the product's operation. "If the wrong decision is made and the product does something unsafe, that opens up the manufacturer to responsibility. And it takes away certain defenses that have traditionally been available in a product liability case, such as the consumer's contributory negligence," says Falvey. If an AI-enabled car causes an accident, you can't blame the driver for being contributorily negligent. In future litigation, then, plaintiffs can be expected to push defendants with questions about what the company did to understand its AI capabilities, what inputs were used to guide AI, and how the product was programmed to react to the various inputs it receives.

"AI is dramatically improving business operations, but it is also opening up new frontiers for litigation exposure," says Poston. For example, algorithms used for employment hiring, predicting recidivism, and even bank lending carry risks of bias embedded in AI's machine learning and thus create concerns about discrimination. "As companies improve their products

"Companies need to think about what data they will need to preserve in the event of product liability litigation."
**Cheryl Falvey,** *former general counsel, CPSC*

## Fighting Back

Completely eliminating the risk of a cyberattack is unlikely, but there are things that companies can do to push back, and even go on the offensive. "There are very sophisticated investigative tools that let you collect a great deal of data about the bad actors coming into your network," says Crowell & Moring's Gabriel Ramsey. For example, he says, some companies are employing "denial and deception" techniques that use decoy systems and fake information to make attackers believe that they are successfully working their way through systems to find valuable targets. "You lead them down the path and monitor them and guide them to a quarantined space where they are blocked from the real systems," he says. "Along the way, you can collect a lot of information about how they operate and even who they are."

That knowledge can be used not only to improve cyber defenses but also to pursue the hackers. "Once you identify them, you can use the legal system," says Ramsey. That might mean turning the information over to state or federal investigators, or it might mean a company takes action on its own through lawsuits or cooperation with authorities in other countries to hold the perpetrators accountable. In some cases, companies have an advantage over U.S. officials in such efforts. "They can move more quickly and aggressively, especially when working with partners across borders," he says. "Companies often don't realize they have these options, but these kinds of efforts can be quite effective."

and operations through new technologies, they must carefully assess how those improvements may also expose them to new risks," he says.

### The Potential Downsides of Product Data

In managing new waves of product-litigation risk, companies will have to pay close attention to the large amounts of data about product performance and usage generated by smart and connected devices. A smart home, for example, might produce 1 gigabyte of data a week, while a connected car might produce 25 gigabytes an hour. Much of the data generated by products can be captured by the manufacturer, but that often doesn't happen. "With today's volumes of data, it can't all be saved—it would cost a fortune. So in many cases, data is constantly being written over or discarded," Falvey says. "Companies need to think about what data they will need to preserve in the event of product liability litigation."

Companies will also need to consider how they use that data. Are they analyzing it proactively to identify performance or safety problems? If not, plaintiffs and regulators may ask why. "Would a reasonable company be using technology to mine that data to help meet a safety goal, for example," says Falvey. "Certainly, companies do that for life-saving products such as pacemakers. To what extent do they need to be thinking of doing it for other types of products where an adverse event might result in a safety hazard?"

With connected, software-enabled products, the data can flow in both directions—and that can help companies stay ahead of liability issues by more easily fixing broken products. For example, companies need to be ready to address hacking vulnerabilities and software problems as they become evident in products. In those cases, says Falvey, "there may be a post-sale duty to inform the customer, if not an express legal obligation to fix it."

Yet repairs can create some gray areas in product liability. "Often, fixing a software glitch in a product can affect the original functionality of that product," Falvey says. "Maybe the battery charge doesn't last as long, or maybe some of the performance characteristics aren't exactly as they were before. When a company decides to fix a product proactively so that something bad doesn't happen, the lawyers need to consider whether any resulting change in functionality may open up the company to consumer protection and deceptive trade practices claims. And what about the fact that the consumer bought the product knowing that it was going to be constantly morphing, like a phone where new apps and functions are always being added? Have they expressly or impliedly consented to product changes over time, or not? These are questions and areas that general counsel should watch."

In the long run, the data generated by connected products could have a far-reaching impact on a range of lawsuits and

"As companies embrace digitalization, they are also facing a new realm of exposure." **Evan Wolff,** *former data scientist and DHS advisor*

trials. "These devices are tracking virtually every aspect of our engagement with the product, not just the product functionality," says Falvey. "They tell us what someone was doing, where they were, how fast they were driving. And that data is going to be incredibly important in litigation."

## Data Breaches: The Never-Ending Challenge

As the benefits of technology have spread, so, too, have the challenges associated with data protection and individual privacy. Cyber risk comes in various forms, from individual hackers to company employees downloading sensitive information onto USB drives. Often, however, criminal organizations and state-sponsored actors are involved. "Increasingly, cyber espionage seeks to take advantage of companies' weakest links, including through phishing emails that target companies' intellectual property and other crown jewels," says Paul Rosen, a partner at Crowell & Moring in Los Angeles who is a former chief of staff at the DHS and a former federal prosecutor.

Data breaches involving the loss of hundreds of millions of records have made headlines. But in reality, most breaches are relatively small—the average attack involves just 25,575 records, according to the Ponemon Institute, an independent research group focused on data privacy. "Cybersecurity now impacts virtually every business—from large and midsize companies to small businesses in the United States and around the world," says Rosen. "This phenomenon is likely to continue since businesses are increasingly reliant on and intertwined with the digital economy."

All 50 states now have some sort of data breach notification law in place, and several federal agencies require breach reporting. This has led to a growing number of follow-on class action suits, and defending against those claims has become more complicated. "The go-to defense in these consumer class actions is to argue that the plaintiffs lack Article III standing because the complaint does not assert a concrete and particularized injury and damages are speculative or conjectural," says Poston. "But now we are getting different Circuit Court approaches to the standing analysis." The 6th, 7th, 9th, and D.C. Circuit Courts have ruled that the future risk of identity theft may be enough to provide standing in data breach lawsuits, while the 2nd, 3rd, 4th, and 8th Circuits have said it may not be enough. "These cases are all fact-specific, but these different approaches and outcomes are something to keep an eye on," says Poston. In the meantime, he notes, "the attacks and breaches are not slowing down, and neither are the class action lawsuits."

## Government Oversight: A Growing Emphasis on Data Privacy—and Litigation

In early 2019, Congress began to discuss a federal data privacy law. But by midyear, the effort had stalled, largely over the question of whether it would preempt state laws, which could be stricter than the new federal law. "The question of whether a new federal privacy law would preempt state law will be hotly debated because federal presumption would have a direct impact on how states could regulate privacy and cybersecurity that affects their own citizens," says Rosen.

Many states have been filling that gap by passing some form of privacy law, and more are adopting or modifying such laws all the time. On this front, all eyes are on the new California Consumer Privacy Act, which took effect on January 1, 2020. The most extensive of U.S. data privacy laws, it gives consumers control over the collection, use, and sale of their personal data and imposes a number of specific breach-disclosure and operating requirements on companies. Enforcement by the state's attorney general can result in an injunction or penalties of up to $7,500 per intentional violation. It also grants a right of private action, with potential statutory damages ranging from $100 to $750 per California resident and incident (or actual damages, if higher).

"Cyber espionage seeks to take advantage of companies' weakest links, targeting companies' IP and other crown jewels." **Paul Rosen,** *former DHS chief of staff*

"Imagine that a company is sued in a class action by a million people, with damages of $750 per person. That's $750 million in potential liability." **Jennifer Romano**

Companies could find themselves facing a two-pronged challenge, says Jennifer Romano, a partner at Crowell & Moring in Los Angeles and co-chair of the firm's Litigation Group. "Victims of cyberattacks could have to respond to an investigation or inquiry by the attorney general's office while responding simultaneously to a daunting class action complaint filed in the wake of a breach," she says. Importantly, California does not have a constitutional standing requirement to bring suit, and California courts have been less stringent with respect to whether a plaintiff must suffer injury before filing suit. "Having the possibility that any person with data that was involved in a breach can bring a class action creates great potential exposure and risk for companies that are victims of cyberattacks," she says.

Romano believes companies may be able to learn from litigants' past experience with California's Confidentiality of Medical Information Act, which supplements federal HIPAA privacy protections. Both the CMIA and the CCPA provide for statutory damages, which can be sought in class action lawsuits, and neither requires class members to prove they suffered damages or any actual harm. And both "require some sort of unauthorized access, exfiltration, theft, or disclosure of the information," Romano says. "What we've found in cyberattacks is that companies will sometimes know that somebody has gotten into their systems, but they can't tell what data has been viewed or if anything has been accessed." It is then up to the plaintiff to prove a theft took place, and that can be difficult when they can't point to any harm or damage. With CMIA cases, she says, "many courts in California have been careful to hold plaintiffs to their burden to prove that the access or theft actually happened. That case law may be relevant to CCPA cases, and it may not be enough to know that a system has been attacked. Plaintiffs will need to show that their non-encrypted or non-redacted personal information was accessed."

The CCPA could raise other questions as lawsuits work their way through the courts. "There may be some due process arguments being raised," says Romano. "Imagine that a company is sued in a class action by a million people, with statutory damages of $750 per person. That's $750 million in potential liability, even though the company is the victim of an attack and there may be no proof that the class members suffered financial loss."

In the coming years, privacy statutes can be expected to be an ongoing challenge. "Companies are wrestling with how to comply with CCPA and other laws," says Poston. "The bottom line is that you want to be able to demonstrate that you have a serious, thoughtful privacy protection program in place, and you also need to be as practical as possible to create a way for ongoing business operations."

## The FTC: The Leading Federal Enforcer on Privacy

Without overarching national laws, the Federal Trade Commission remains the nation's lead data security and privacy enforcer at the federal level—and its view of those issues has significant ramifications for litigation. A few years ago, the FTC seemed poised to take a posture of so-called "regulatory humility," an approach that aims to recognize certain limitations of regulation and avoid overprescription on complex issues. But regulatory humility has not meant inaction. "Over the past year or so, the FTC has been very active and has demonstrated that it intends to exercise its authority as the leading civil enforcer of privacy and data security," says Kristin Madigan, a partner with Crowell & Moring's Privacy & Cybersecurity Group in San Francisco and a former attorney at the FTC's Bureau of Consumer Protection, Division of Privacy and Identity Protection. "The FTC is continuing to pursue major data security matters involving questions of whether companies provided reasonable security for personal information and the representations companies make about their data security."

The FTC has also been actively enforcing the Children's Online Privacy Protection Act. In September 2019, a video-sharing plat-

"The FTC has demonstrated that it intends to exercise its authority as the leading civil enforcer of privacy and data security." **Kristin Madigan,** *former FTC attorney*

Companies should also put themselves in the bad actors' shoes. "Ask yourself, what kind of victim are we? How do the cybercriminals see us?" **Gabriel Ramsey**

form agreed to pay $170 million to settle COPPA allegations that its service had illegally collected personal information from children to support the targeting of ads. Perhaps more important, says Madigan, "the personal information at issue was limited to persistent identifiers—commonly known as cookies—to deliver targeted ads to viewers, and not data such as name, address, email address, or Social Security number that we typically think of as personal information. This settlement pushed the boundaries of what constitutes personal information and a COPPA violation with that definition." The FTC is currently considering updates to COPPA, and those revisions could reflect this broadened view of cookies and other online privacy issues.

On the consumer privacy front, the FTC imposed a $5 billion penalty against a social media giant last year, saying the company had violated a previous FTC order by misleading consumers about its ability to control its own personal information. The penalty was the largest ever imposed for violating consumers' privacy and one of the largest penalties ever assessed by the U.S. government for any violation, according to the FTC.

In such cases, the requirements of the consent orders issued by the FTC are perhaps more important than the amount of a civil penalty, says Madigan, because they provide insights that can help companies avoid litigation. A recent order, for example, required a social media company to restructure its approach to privacy and establish mechanisms to hold company executives accountable for their privacy-related decisions. "The orders in the FTC's landmark settlements provide a baseline understanding of its evolving expectations. These orders can help educate companies about conduct the FTC views as permissible versus not," says Madigan.

In the coming year, the FTC may temper some of its activities. "We expect the FTC will continue to pursue headline-making cases, particularly involving children's privacy and major data or privacy events that affect many consumers," says Madigan. "In areas where there are close calls or truly novel legal questions, the FTC may revert to the more restrained approach that marked the beginning of the current administration." With that in mind, she says, "states and their attorneys general will be another place to watch for cutting-edge privacy and data security issues."

## Getting Ahead of the Risks

Companies and legal departments can take a number of actions to adapt to this evolving environment:

**Enhance compliance for evolving product liability.** With the very real potential for more product liability lawsuits in the digital age, for example, "compliance and litigation-readiness efforts need to modernize to meet the demands of a much more sophisticated product," says Falvey. "The in-house legal team needs to anticipate, from a design perspective, the potential failure modes of products—and then be able to show that the company thought through those issues prior to launching the product."

Toward that end, Falvey says that the legal department needs to be kept in the loop about product design and maintenance decisions, as well as about the plans that the business has for using product-generated data. The legal team can then help ensure that safety and liability issues are understood and, as much as possible, dealt with up front. That's especially important with AI-enabled products. "The functionality of those products is going to evolve after they are out in the marketplace, based on the inputs and 'learning' of the system. A year down the road, the product will not be the same as it was when it was launched. If the lawyers have a seat at the table, they can help you understand future potential liabilities stemming from those evolving products," she says.

**Take advantage of technology.** On the cybersecurity front, the legal department can work with IT to conduct a risk analysis "and then put together a road map of what technology you need to be using now and in the future in order to better manage your risks," says Gabriel Ramsey, a San Francisco-based partner in Crowell and Moring's Privacy & Cybersecurity Group.

Ramsey also points to data loss prevention, a combination of technology tools and processes that help protect sensitive data. DLP systems identify sensitive and critical data and then monitor the company's end-user computers, corporate networks, and cloud operations to identify any misuse or unauthorized access to that data. "It's tracking things like what's being emailed, what's going out on USB drives, and what's being uploaded to the cloud, and triggering actions in response to suspicious behavior," says Ramsey.

**Prepare for cybersecurity events.** Companies should develop an incident-response plan that spells out how it will deal with an incident. "It should include a clear governance structure, with clear roles and responsibilities for the response team," says Wolff. A plan should also cover the policies and procedures that will be followed—essentially a playbook for how to respond. "That playbook should then be tested through hypothetical exercises where

## GDPR: Recalibrating the Balance of Rights

In a world of increasing privacy regulations, the implementation of the EU's General Data Protection Regulation in May 2018 was a watershed event that recalibrated the balance of rights between citizens, businesses, and governments. The GDPR includes strict rules governing data protection for individuals in the EU—that is, "data subjects"—and gives individuals more control over how their personal data is used. It also allows individuals to sue to enforce the regulation and provides significant penalties. "Under EU law before GDPR, the maximum fine was £500,000. Now it may be up to 4 percent of worldwide annual turnover or £20 million, whichever is higher, which could run into several hundred million dollars," says Laurence Winston, a partner in Crowell & Moring's London office and co-chair of the firm's International Dispute Resolution Group. "So the gravity of the fines is exponentially higher." In the past year, GDPR enforcement actions included, notably, the intention to levy a $230 million fine on a major British company for a 2018 data breach.

"The maximum fine may now be up to 4 percent of worldwide annual turnover, which could run into several hundred million dollars."
**Laurence Winston**

The GDPR is still relatively new, and some aspects of the regulation are still being worked out. "When data subjects have had their data breached, they are entitled under the GDPR to bring claims for 'material or non-material damage.' The question is, what does non-material damage mean? That's something that's being interpreted by the courts," Winston says. However, he notes, it appears to include loss of control of data regardless of whether plaintiffs suffered actual financial damage or distress that could have huge implications. What's more, even if the individual damages are modest and amount to only a few hundred dollars per claimant, the total damages payable could be enormous in the context of a large class or group action.

In general, Winston says, companies are well aware of the requirements of the GDPR, "but there are still many that are not complying adequately." Often they are struggling with the "unknowns" about the sources and degrees of vulnerability and compliance risk in their systems. "Large companies, especially those that have grown through acquisitions, might have many differently configured systems across many countries," he explains. "Some might be more secure or more compliant than others. A company may even be acquiring systems that have already been compromised and are experiencing a continuing breach. And because companies don't have uniformity of systems, it becomes more difficult to secure data and control the problem."

everyone runs through what they will need to do," he says. "That helps ensure that the organization is ready to respond effectively and efficiently when and if a real incident arises."

Such plans should be overseen and implemented by a cross-functional team that includes representatives from the technology, legal, customer relations, and media relations areas, as well as business units. "A broad team helps bridge the knowledge gap between the technical experts and the senior decision makers and helps employees and executives know what to do," says Rosen. "The team should assess its sensitive data, the technology that's in place to protect that data and prevent attacks, training opportunities for employees, and how to respond if a hack occurs."

**Keep learning.** Companies should also put themselves in the bad actors' shoes. "Ask yourself, what kind of victim are we? How do the cybercriminals see us?" says Ramsey. "Who would be interested in us? Would they be looking for money, or consumer information, or perhaps IP? That can help you understand the risk you face."

It's also important to learn from the experience of others, as well. "Companies should keep up with other breaches that are publicized—particularly in the same industry—and understand how they occurred and what kinds of technologies were involved to better defend against similar attacks," says Poston.

As the digital revolution spawns new innovation and helps companies create powerful connections with their operations and customers, it can also create a complex web of tort, privacy, and cybersecurity litigation risk. A forward-looking legal and compliance strategy that works hand in hand with the business units of the company can be a critical factor in limiting exposure and driving ahead to a company's digital transformation imperative.

# Moving Front and Center

## Antitrust

Over the past year, antitrust has emerged from relative obscurity to enter the political and governmental mainstream. Everyone, from the White House, Congress, and regulatory agencies, to state governments and presidential candidates, has been part of the dialogue. After years of megamergers and increasing consolidation across industries, along with little to no government enforcement of anti-monopolization laws, "antitrust is back, it's evolving, and it's at the center of a lot of public discourse," says Beatrice Nguyen, a partner at Crowell & Moring. "The various discussions that are taking place—and recent actions on the part of federal and state regulators—are creating an evolving landscape in antitrust, and they may point to upcoming fundamental changes in how the antitrust laws are enforced."

The changes in antitrust are taking several forms. For example, regulators are under increasing pressure from members of Congress and influential think tanks to consider the once-unusual step of reassessing and unwinding already-consummated mergers. And while the Department of Justice has been quite willing to pursue horizontal mergers, its 2017 challenge to the AT&T-Time Warner merger was the first time in four decades that the government challenged a vertical merger, in which companies from different stages of a common supply chain come together.

One of the more prominent shifts taking place is an increase in "targeted" antitrust scrutiny on entire industries—as opposed to specific companies—starting with Big Tech. In June 2019, the Department of Justice and the Federal Trade Commission divided up among themselves certain investigations into Google, Apple, Facebook, and Amazon. "I don't think we've seen a situation—at least in the past several decades—where regulators essentially divide up an industry to proactively start investigating it," says Nguyen. That same month, the House Judiciary Committee announced a bipartisan investigation into potentially anticompetitive behavior by prominent tech companies in Silicon Valley. And regulators and politicians alike have been talking about potentially anticompetitive actions of online marketplace operators and whether those operators should be able to both run and participate in their own marketplaces.

Other industries are in the spotlight, as well. With the pharmaceutical industry, politicians on both sides of the aisle have questioned a possible connection between rising drug prices and anticompetitive behavior among drug companies. A bipartisan House bill introduced in November 2019, for example, targets the practice of making minor modifications to a drug to extend its patent and keep generics out of the market. And a number of observers—including one FTC commissioner—have also called for greater scrutiny of health care-industry mergers.

Similarly, in 2018, Sen. Cory Booker introduced legislation that would place an 18-month moratorium on mergers between large agribusinesses, food and beverage manufacturers, and grocery retailers. Likewise, Sen. Bernie Sanders has released

### State AGs: Taking Bold Action

While federal regulators explore potential new approaches to antitrust, state attorneys general are not standing still. "We've seen the states become willing to take bold action," says Crowell & Moring's Beatrice Nguyen.

Traditionally, states have often worked with the DOJ on antitrust investigations and litigation, but now they are increasingly likely to launch their own lawsuits. The year 2019 offered "some really prominent examples" of that trend, Nguyen says. In May, Connecticut and 43 other states filed suit against 20 pharmaceutical companies and 15 individuals for allegedly conspiring to fix prices for generic drugs. In June, a number of states sued to block the T-Mobile-Sprint merger, which was eventually approved by the DOJ. And in September, 48 states announced that they would investigate Big Tech companies for possible antitrust violations. In addition to these lawsuits, Nguyen says, "states are taking action individually. For example, California launched a high-profile antitrust lawsuit against a large hospital system in March 2018 that settled in October 2019. This was a case that the DOJ or the FTC might not have pursued."

For companies, it used to be that getting federal antitrust approval for a deal more or less meant the company was in the clear. But now "you can't really assume that anymore," says Nguyen. "The states may be waiting in the wings with a complaint even after the federal government gives its approval."

"Companies in concentrated markets need to be more mindful of potential antitrust implications when conducting business." **Beatrice Nguyen**

a detailed policy proposal that calls for, among other things, a moratorium on corporate consolidation in the agricultural industry, as well as the unwinding of prior mergers in that industry.

With the growing focus on entire industries, says Nguyen, "companies in concentrated markets need to be more mindful of potential antitrust implications when conducting business or considering acquisitions or mergers. Otherwise, they could find themselves in the crosshairs of regulators, embroiled in private litigation, or both."

## Talking About Tomorrow

Regulators and politicians are also reconsidering how they should define "competition" in conducting antitrust analyses. While these discussions have not yet materialized into new laws, regulations, or enforcement action, they have gained traction and provide insight into how antitrust decision making is likely to evolve in the next few years.

Most notably, since the late 1970s, evaluations of mergers have analyzed whether the deal is good for consumers and consumer prices. But, says Nguyen, "we're starting to see more nontraditional considerations being included in antitrust discussions."

For example, as data plays a larger role in business, regulators appear to be more interested in factoring it into their analyses. "They are starting to consider questions such as, If a merger is going to result in one company getting an enormous amount of data, does that raise competition issues?" says Nguyen. Data privacy, too, is an increasing concern: If one company acquires another company and its data, what does that mean for consumers' personal information when they did not consent to giving their data to the acquiring company? As DOJ Antitrust Division Assistant Attorney General Makan Delrahim explained in November 2019, "Without competition, a dominant firm can more easily reduce quality, such as by decreasing privacy protection, without losing a significant number of users." He went on to add that "non-price dimensions of competition deserve our attention and renewed focus in the digital marketplace."

A variety of non-price dimensions is being discussed in various quarters. For example, says Nguyen, "there is a growing concern about labor-market concentration and the potential for companies and industries to have monopoly power over labor, resulting in lower wages." And enforcers' focus on labor is not limited to the merger context: No-poach agreements, in which companies agree not to hire each other's employees, are being scrutinized by regulators. Since the introduction of the DOJ and FTC guidelines for HR professionals in 2016, these agreements are also being investigated as criminal offenses in certain circumstances. The regulators' enhanced focus on labor has also led to an increasing number of labor-focused antitrust class actions.

This broadening discussion is showing up in Congress, too. In 2019, Sen. Richard Blumenthal, along with several other senators, wrote a letter to the DOJ and the Federal Communications Commission opposing the proposed merger between T-Mobile and Sprint because it would not only raise prices but also "harm workers, stifle competition, exacerbate the digital divide, and undermine innovation." And Sen. Amy Klobuchar has introduced several pieces of antitrust legislation, including the Consolidation Prevention and Competition Promotion Act, which would clarify that existing law prohibits mergers that result in lower product quality, decreased choice, and reduced innovation—more non-price criteria.

"In the past, many of these factors were not the driving forces behind regulators' merger investigations and analyses," says Nguyen. But if such ideas become part of the regulatory regime, she adds, "companies will need to pay attention to these considerations not only as part of their transactional review but also in the way they go about doing business."

In this environment, companies wanting to avoid antitrust troubles will need to take a more wide-ranging view of their actions and broaden their focus beyond the question of whether certain conduct will lower consumer prices. "Arguments and analyses are going to have to evolve and address these nontraditional factors," says Nguyen. Even if the laws don't change, she says, "it may be wise from a public-perception perspective to build a narrative that reflects issues beyond consumer prices." At the same time, companies should prepare the organization by ensuring, for example, that HR employees have antitrust training so that they avoid working too closely with other companies on hiring or wages.

As the mix of factors that go into antitrust decision making grows and regulatory scrutiny continues, the result is likely to be increased litigation with the government—and private litigation will not be far behind. And, Nguyen says, "we're not only talking about increased litigation, we're talking about the possibility of litigating new antitrust legal standards. Companies will need to pay attention to what is clearly an evolving antitrust environment."

# *Stare Decisis*: Will Precedent Survive Scrutiny?

## Appellate

The U.S. Supreme Court has been increasingly open to putting aside the *stare decisis* doctrine—that is, the idea that it should respect prior precedent of the Court—and more frequently overturning its own precedents. The question is, how far will this trend go?

"With the Court's new conservative majority, we've seen a debate in the Court over how much weight to give to *stare decisis*, and how reluctant the Court should be to overturning long-standing precedents based purely on the fact that the current Court disagrees with the precedent set by a previous Court," says Tom Lorenzen, a partner in the Appellate Practice at Crowell & Moring and vice-chair of the firm's Environment & Natural Resources Group. Traditionally, the Court has developed careful justifications when overturning precedents.

That debate played out in several recent cases at the Court. The first of these, *Franchise Tax Board of California v. Hyatt* (May 2019), involved a long-running tax dispute between Gilbert Hyatt and California. In a 5-4 decision, the Court ruled in favor of the tax board, saying that states have sovereign immunity from private lawsuits filed against them in the courts of other states. This overruled the precedent set in *Nevada v. Hall*, a 1979 Supreme Court case that said states did not have such immunity. In a dissenting opinion in *Hyatt*, Justice Stephen Breyer wrote that "today's decision can only cause one to wonder which cases the Court will overrule next."

Shortly after that, the Court ruled in *Knick v. Township of Scott, Pennsylvania* (June 2019). In this case, Mary Rose Knick challenged a township ordinance, saying that it violated the Takings Clause of the Fifth Amendment, which requires compensation to be paid for private property taken for public use. A federal district court dismissed Knick's lawsuit, based on the Supreme Court's 1985 ruling in *Williamson County Regional Planning Commission v. Hamilton Bank,* which said that plaintiffs had to exhaust all state court remedies before taking a claim to federal court. In *Knick*, the Supreme Court overruled *Williamson*, essentially saying that a person can sue a local government in federal court without having to go through the state courts first, and then remanded the case to the lower court. "Here again, the dissenting justices said that the decisions were likely to unsettle long-established expectations about how the law worked," says Lorenzen.

Then, later in June 2019, the Court ruled in *Kisor v. Wilkie*, a case involving the denial of benefits by the U.S. Department of Veterans Affairs, an action based on the department's interpretations of its regulations. The case challenged the *Auer* deference doctrine, which was established in 1997 in *Auer v. Robins*. "The *Auer* doctrine says that unless the interpretation of the law by an agency cannot be squared with the plain language of the regulation, the courts must defer to the agency," says Lorenzen. When the Court decided to hear *Kisor*, he says, "many observers thought it was poised to overturn *Auer*." This time, however, the Court upheld *Auer,* based largely on the *stare decisis* principle. "But it also said that there are clear limitations on when *Auer* may be applied—that the courts should avail themselves of all the possible interpreting tools to determine whether the regulation is clear," he says. "If it's clear, there is no room for interpretation."

These cases, and the writings and comments of the conservative Supreme Court justices, have prompted many observers to wonder whether the doctrine of *stare decisis* is still in full effect at the Court. "People are hearing this debate and asking, how much existing law is this going to unsettle?" Lorenzen says.

That's a fair question, but the answer may ultimately be that this potentially changing view of *stare decisis* will have a

"The impact may actually end up being somewhat limited because of the way the court system is structured."

**Tom Lorenzen**

relatively narrow impact. "The impact may actually end up being somewhat limited because of the way the court system is structured," Lorenzen says.

"As the highest court in the United States, the Supreme Court can revisit prior precedents and declare them wrongly reasoned and abandon them in favor of a new construction," Lorenzen continues. But the lower courts don't have that kind of leeway. District Courts are bound by the decisions of the governing Circuit Court of Appeals—they cannot simply invoke *stare decisis* and overturn the precedent set by the Circuit Court. The same thing applies at the Court of Appeals level, where cases are typically heard by a three-judge panel, which is bound by the decisions of prior panels of that court and the decisions that were issued by the court sitting *en banc*. "The only mechanism for the Courts of Appeals to change their minds about what the law means is the *en banc* review process, and the impact there is limited by the extraordinarily few cases that are heard *en banc* each year," Lorenzen says. "They are far and away the exception rather than the rule."

Overall, he says, "there are several structural impediments to the wholesale abandonment of prior precedent in favor of new judicial doctrine." The Supreme Court's workloads are a limiting factor, as well, he points out: "The Court decides only a relative handful of cases each year—perhaps 70 or so. And most of those cases are on issues of very limited applicability."

Nevertheless, there will be changes. "It's very likely that we will see cases in which the Court does resolve issues in ways that are contrary to prior precedent," Lorenzen says. Several justices have made it clear that they are focused on aspects of administrative law, especially around the doctrines that govern the review of executive agency actions. "The Court appears to be interested in a reallocation of power from the federal executive back to the judiciary—so that is something that we can expect to see more of," he says.

For example, Lorenzen says, the Court is likely to eventually revisit the *Chevron* deference doctrine, in place since 1984, which says that federal courts should defer not just to an agency's interpretation of its own regulations, as with *Auer*, but also to an agency's interpretation of statutes that are unclear. "We're not there yet—the Court has not abandoned or revised *Chevron*," he says. "But it is arguably working its way there."

## Deregulation by Appeal?

In 2016, the EPA reaffirmed that the MATS standard regulating power-plant emissions of mercury and other hazardous air pollutants (HAP) was "necessary and appropriate," as required by the Clean Air Act. That assessment was based not only on the direct benefit of reducing HAP emissions but also on the collateral benefit of cutting particulate emissions. Now the EPA plans to reverse the 2016 rule, saying that collateral benefits should not have factored into it. The immediate impact will likely be limited by the D.C. Circuit Court's 2008 decision in *New Jersey v. EPA*, which "said that once a category of sources has been listed for regulation, the agency can't stop regulating it without going through a complicated delisting process," says Crowell & Moring's Tom Lorenzen.

Having largely complied with MATS, much of the utility industry opposes this move. But other parties, such as coal companies, may urge the EPA to go even further. "We can expect challenges to the EPA's decision reversing the appropriate-and-necessary finding without also rescinding the MATS standard itself," says Lorenzen. Those challengers would do so knowing they will lose under the *New Jersey* decision, at least at the panel level. Their goal, however, would be to create an appeals path to the Supreme Court, where the majority is more likely to be open to overturning *New Jersey* to further reduce environmental regulations.

This focus on administrative law and agency decision-making powers will be especially important to business. "These cases are likely to have far-reaching consequences for regulated industries, and they may give those regulated communities more power to successfully question the agencies' policy choices," Lorenzen says.

Meanwhile, the Supreme Court's actions on that front will, as always, play out in various federal courts. For example, while the *Kisor* decision left the *Auer* doctrine in place, it also seems to have narrowed it by more closely defining when it can be applied and clearly requiring courts to use "all the traditional tools of statutory construction" before allowing *Auer* deference. "How much the doctrine has been narrowed probably depends on whom you ask, and there is a lot of debate about whether the doctrine is really viable with those limitations," says Lorenzen. As a result, agencies and regulated businesses can be expected to litigate those questions in court. As Lorenzen says, "Only time will tell what the lower courts will make of *Kisor*—and how *Auer* deference will work in the future. And only time will tell how far from *stare decisis* the Supreme Court will be willing to stray to recraft settled law to fit its own principles of legal construction."

# The Multifront Battle of Chemical Regulation and Litigation

## Environment & Natural Resources

State governments and private environmental plaintiffs are playing a more prominent role in shaping the contours of what will be acceptable in the marketing and sale of products containing chemicals. As a result, the associated risk of litigation is expanding far beyond traditional enforcement actions.

State legislatures, attorneys general, regulators, and private litigants have been increasingly active in bringing litigation involving chemicals present in commercial products, including food items. At the same time, several state attorneys general have filed groundwater investigation and remediation lawsuits against potentially responsible parties for allegedly failing to comply with environmental regulations involving chemicals that have migrated into subterranean water sources. Some are working with plaintiffs' lawyers, sometimes hired on a contingency basis, seeking significant damages for environmental claims on behalf of citizens.

Legislators are weighing in, too. In 2019, Washington state enacted legislation that strictly regulates PCBs and other chemicals, and the New York state legislature passed a law requiring companies to report on various chemicals used in toys, car seats, and other children's products and will eventually ban certain chemicals, such as benzene and mercury, in those products. Local governments are getting in on the action. For example, Key West banned sunscreen containing oxybenzone and octinoxate, which may harm coral reefs, while San Francisco banned certain chemicals used in the food service plasticware sector.

This fragmented landscape, combined with increasing state, local, and private enforcement activity, significantly complicates a company's ability to forecast and manage compliance and avoid or minimize litigation. As a practical matter, rather than coming up with multiple compliance schemes for different markets, companies typically try to meet the requirements applicable in the most rigorous regimes. "California, which tends to have stricter environmental regulations than many other states, is also something like the world's fifth-largest economy," says Rick McNeil, a partner in Crowell & Moring's Environment & Natural Resources Group. "So it often just doesn't make commercial or practical sense not to do business in California if you have a national or international product."

The regulatory patchwork can also create a gray market in products, and that can spawn its own concerns. For example, the South Coast Air Quality Management District, which regulates air quality in Orange County and Los Angeles and elsewhere in Southern California, limits the concentration of volatile organic compounds in a variety of products, such as marine paints and solvents. However, says McNeil, "ship and boat maintenance is still a large part of the economy, so when the district limited the use and sale of these products, a lot of businesses selling them sprung up in the areas beyond the district's geographical jurisdiction." For companies using banned materials in boat repair operations—or for food packaging makers whose

### Proposition 65: An Expanding Risk

Proposition 65, the California law that requires businesses to provide warnings about potentially harmful chemicals in their products, now covers 1,000 or more substances—and is proving to be fertile ground for plaintiffs alleging damages from exposure to chemicals.

Proposition 65 includes a private action "bounty hunter" provision, which makes the law attractive to plaintiffs' lawyers. From 2009 to 2018, the number of annual private actions against businesses under the law grew from 604 to 2,364, according to *The National Law Review*. "Those cases can be challenging to defend," says Crowell & Moring's Rick McNeil, in part because if a plaintiff establishes a *prima facie* case, the burden shifts to the defendant to establish that exposure did not present a "significant risk," which often corresponds to very low concentrations. The difference in which party carries the burden could determine the outcome in some cases.

Plaintiffs have been focusing in particular on substances such as lead and phthalates. But with growing public awareness of the health risks that may be associated with other chemicals listed under Proposition 65, litigation is starting to increase in those areas.

The Proposition 65 list of harmful chemicals changes frequently, with some being added and some removed. But overall, says McNeil, "it tends to be growing."

"You're talking about orders of magnitude differences in damages, especially with class actions—and things are much more unpredictable." **Rick McNeil**

products end up in San Francisco—this kind of gray market "could lead to people bringing private attorney general types of complaints," says McNeil.

The growing activity at the state and local levels stems in part from a feeling among some that there is a need to compensate for a perceived EPA regulatory and enforcement rollback. But the trend has actually been going on for a while and is a reflection of deeper shifts in society's attitudes and culture, says McNeil. For example, polls show increasing public support for environmental protection, and state actions reflect that. State attorneys general are also charged with consumer protection, and many see environmental issues falling under that mandate.

McNeil also points to a growing expectation for companies in general to "not only do no harm, but to proactively be good corporate citizens." At the same time, he cites a growing sense that private citizens should or need to play a role in environmental enforcement. "There's a kind of 'individualization' in which people are starting to take ownership of these issues, and that manifests itself in their going to their state regulators and public interest groups—and to plaintiffs' lawyers," he says.

More and more people are doing just that, driving a trend that is closely related to increased state activity on the chemicals front. "With these environmental chemicals that historically have been regulated as hazardous substances, we are now seeing more private litigants asserting tort claims," says McNeil. "The wall between the traditional environmental regulatory enforcement lawsuits and the private tort lawsuits is breaking down."

That risk is underscored by several trials over the past year or so in which companies were sued for damages allegedly caused by chemicals or pesticides. "We've seen more lawsuits involving chemicals used for industrial purposes or even everyday consumer usage. We've also seen some pretty significant jury verdicts for exposure that were surprising to many observers—some in the tens of millions or even hundreds of millions of dollars," says McNeil. "And we are seeing early signs that the courts are not going to shut these types of claims down, at least in California." Often the science behind the claims of health risks from chemicals is far from settled. But, as always, scientific data is just one of many factors that go into the jury decision-making process. "If the class of plaintiffs is large, it can be hard to find a jury that's not going to be in some way sympathetic," McNeil says.

Indeed, more chemical class actions can be expected. "Plaintiffs' attorneys are advertising online and on television to find people who have used chemicals and may have associated health problems," McNeil says. What's more, there has been a fair amount of media coverage about relatively small concentrations of various chemicals being found in food products. While this has led to food-labeling lawsuits under California's Proposition 65 (see sidebar, page 16), McNeil says that it is not hard to imagine plaintiffs eventually considering trying to pursue class action personal injury claims stemming from the consumption of such foods.

## Litigation: Faster and Less Predictable

In the past, there were relatively lengthy timelines associated with chemicals enforcement and litigation. Under the federal Superfund law, such lawsuits generally were put on hold until EPA action was complete—which in many cases meant a decade or even decades. But in 2018, a three-judge panel of the 3rd Circuit Court of Appeals ruled that a private lawsuit involving groundwater contamination could proceed without waiting for the completion of the EPA action, thus heralding a potential new type of litigation that may well shorten the timeline for companies facing such litigation.

"The timing of these things is changing, and so is the exposure," says McNeil. "It used to be a fairly straightforward exercise to determine your exposure in a lawsuit and plan your resources to match the expected exposure. But now you're talking about orders of magnitude differences in damages, especially with class actions—and things are much more unpredictable."

For companies, this "new normal" might well argue in favor of organizational shifts. "You may no longer have the luxury of parsing out work across your environmental lawyers, your government affairs group, and your litigation teams," says McNeil. "With the increasing speed and potential exposure associated with such litigation, it may take all three of these groups working together to manage risk exposure and litigation."

With states, regulators, and plaintiffs all focusing on chemicals across the stream of commerce, legal departments will want to stay alert to changes and evolving threats. "If I were a GC of a company that manufactures any sort of chemical that is used by consumers and could be linked to health conditions," says McNeil, "I would be planning now how to limit the company's liability as this litigation expands."

# Jurisdictional Analysis

## Understanding the Data Behind the Litigation Trends

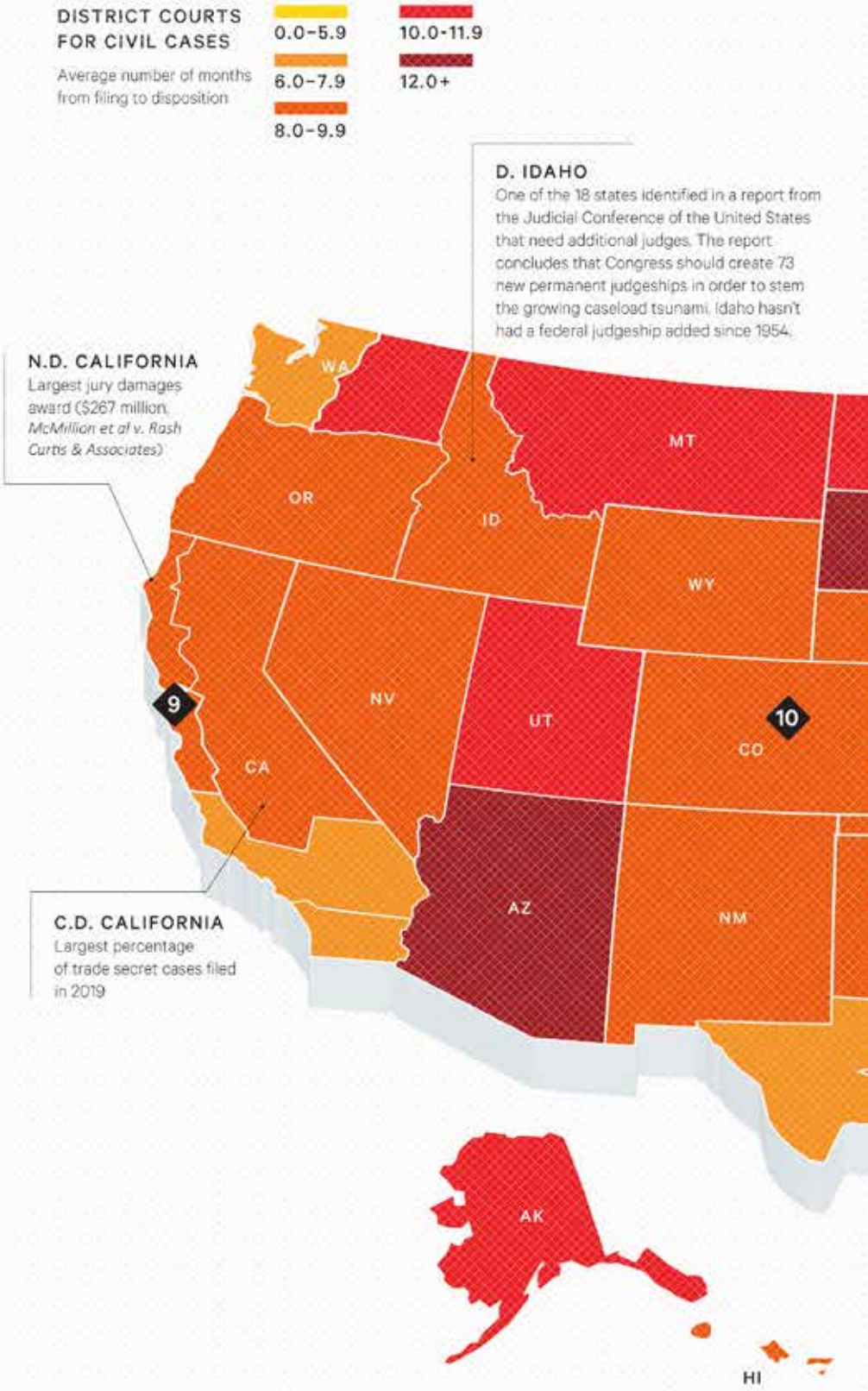
Over the past year, competition in the market for legal data analytics has continued to heat up, providing law firms with increasingly powerful tools to mine ever-more robust data sets from courts across the country. These sophisticated platforms enable attorneys to develop case strategies based on jurisdiction-specific insights into case timelines, outcomes, damages, and more.

But to provide *reliable* insights, it is critical that attorneys using these tools understand how they work and how to parse the underlying data. It is easy to make a broad generalization that the *average* case resolved in 2019 in the District of Massachusetts took nearly three years from filing to disposition. But this generalization papers over radical discrepancies between the speed of different judges' dockets and different types of cases.

In the District of Massachusetts, the average time to termination falls from nearly three years to nine months if you exclude product liability cases. In the Eastern District of Louisiana, the average time to termination falls from 22 months to eight months if you exclude environmental cases. And in the District of Kansas, the average time to termination falls from 40 months to eight months if you exclude trademark cases.

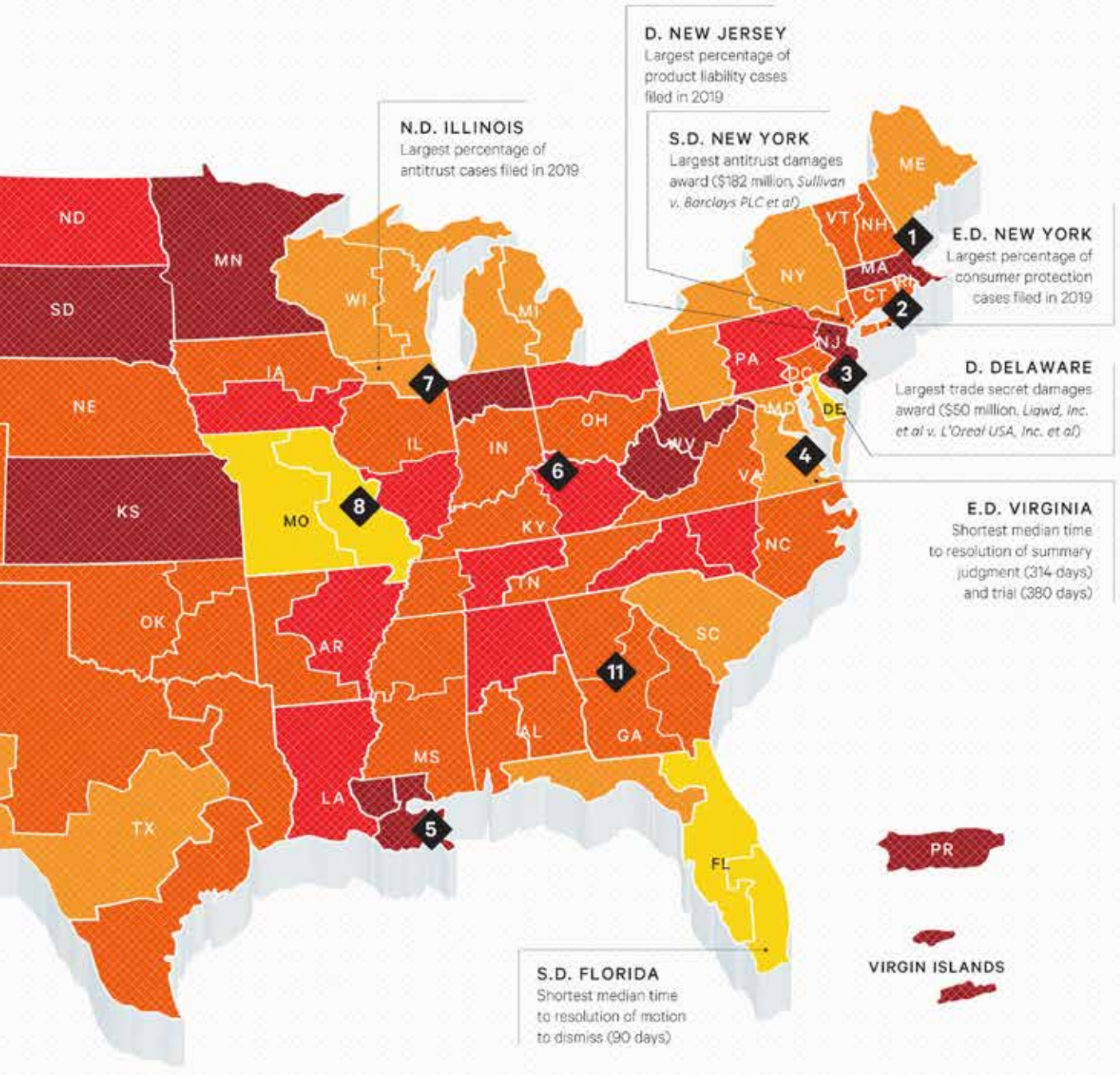
The failure to understand and appreciate the nuances of data can easily lead counsel to draw inaccurate conclusions and provide inaccurate advice. The role of analytics tools will continue to grow in the coming year. But as always, these tools are only as good as the attorneys who use them.

**Keith Harrison,** Partner, Crowell & Moring



## UNITED STATES COURTS OF APPEALS

| Circuit | Notice of Appeal to Disposition (in Months) | S. Ct. Reversal Record |
|---|---|---|
| 1st | 13.6 | 1 of 2 |
| 2nd | 11.4 | 3 of 5 |
| 3rd | 8.3 | 2 of 3 |
| 4th | 5.5 | 2 of 4 |
| 5th | 9.1 | 2 of 4 |
| 6th | 7.3 | 3 of 7 |
| 7th | 8.5 | 1 of 1 |
| 8th | 7.5 | 3 of 4 |
| 9th | 10.9 | 12 of 14 |
| 10th | 9.0 | 1 of 2 |
| 11th | 7.8 | 3 of 7 |
| DC | 10.6 | 1 of 3 |
| FED. | 15.0 | 2 of 4 |




*The map above reflects select data from 2019 federal court dockets for key civil practice areas.*

# Government and Industry Tensions Around Intellectual Property

## Government Contracts

Government agencies continue to require contractors to provide more technical data and computer software to the government, along with greater license rights in that data. That means that contractors should expect to see more IP-related litigation.

"When it comes to IP in government contracting, the rules are quite different than in the commercial space—and there are different rules for civilian agencies and the DoD," says Nicole Owren-Wiest, a partner in Crowell & Moring's Government Contracts Group. When a government contract requires technical data and computer software to be delivered to the government, the government acquires a license in the data that is referred to as "data rights." With Department of Defense contracts, the scope of the government's license generally depends on the source of funding for development (government, private, or mixed), the nature of the item or software (commercial or noncommercial), and any negotiated terms of the contract. If the development is government-funded, the government is entitled to an unlimited rights license, which means that it may disclose (i.e., sublicense) the data outside the government for any purpose. If the development is funded exclusively by the contractor, the government is entitled to a limited or restricted rights license, meaning the data can only be disclosed within the government and not, for example, to other contractors, subject to certain exceptions. If the development funding is mixed, the government may be entitled to government purpose rights, which allows the government to disclose the data outside the government, including to other contractors, for government purposes, such as competing for and performing a government contract.

There are also subsets of technical data, such as "form, fit, and function" data and data that is "necessary for operation, maintenance, installation, and training purposes." With this technical data, the government is entitled to an unlimited rights license regardless of the source of funding. Contractors must assert the applicable data rights in their proposals and mark the data they claim is subject to rights restrictions. The government can challenge contractors' assertions for up to several years after final payment under the contract.

For the past few years, government agencies have increased their focus on both acquiring more contractor technical data and software under its contracts and gaining greater rights in that data, even when the items or software being acquired have been developed exclusively at private expense. This has been particularly true for DoD agencies, which tend to view such data as critical to their ability to enhance competition and sustain systems and subsystems over their life cycle. For example, says Owren-Wiest, "we are seeing more solicitations requesting the contractor deliver detailed manufacturing or process data and computer software, including source code, with at least govern-

### Contractor vs. Contractor—and the Government

In a competitive market, some contractors are looking to recoup losses through IP infringement lawsuits that can bring them up against contracting agencies. "We have been seeing more claims against the government for breach of a contractor's software license, and claims for copyright infringement under 28 U.S.C. 1498(b), and patent infringement under 28 U.S.C. 1498(a)," says Crowell & Moring's Nicole Owren-Wiest. Under that law, when a company believes that the government or another company working for the government with the government's authorization and consent has infringed its copyright or patent, its exclusive right of action is against the government, rather than the other company, in the Court of Federal Claims for its "reasonable and entire compensation."

In March 2019, a key development took place on that front, when the court awarded a patent owner nearly $4.4 million for attorney costs and fees—about 20 times higher than its $200,000 damages award. This was the first time such an award has been granted under 1498(a)'s fee-shifting provision, which is limited to certain plaintiffs and when the court finds the government's position not "substantially justified." With a tighter, more competitive market, and the potential opportunities for recovery, Owren-Wiest says, "we are seeing more 1498 cases related to both patents and copyrights at the court and are hearing more from companies that are thinking about affirmatively pursuing such cases."

"We are seeing more formal challenges to contractors' assertions and markings during contract performance, resulting in more formal disputes." **Nicole Owren-Wiest**

ment purpose rights, even when development was accomplished exclusively at private expense, because the government asserts the data are necessary for its sustainment objectives and to avoid vendor lock-in." These requests are directly at odds with the contractor's objective to protect its IP.

This tension is resulting in an increased number of data-rights disputes between contractors and the government. Owren-Wiest notes that in 2018, a contractor filed a pre-award bid protest challenging the terms of an Air Force solicitation that required the delivery of an additional broad category of data, including software, for enabling the installation and maintenance of the system, including installation, de-installation, disassembly, and reassembly activities, with at least government purpose rights. "The company challenged the terms that it believed were overreaching, including the requirement to deliver software developed exclusively at private expense with government purpose rights," she says. That issue was not addressed by the Government Accountability Office because, during the protest, the Air Force clarified that offerors would not be required to sell or otherwise relinquish to the government any rights in software developed exclusively at private expense (except for certain identified exceptions not at issue in the protest), either as a condition of being responsive to the solicitation or as a condition for award. Similar pre-award protests are likely in the near future. "In talking with companies, we find that more are considering filing pre-award bid protests around far-reaching data-rights terms and requirements for delivery of technical data and software," she says.

## A Range of Disputes

The government can negotiate with offerors to purchase technical data and software that it has determined are necessary to satisfy its needs, as well as to evaluate the license rights an offeror is willing to grant the government as part of the government's source selection. However, some government solicitations have included fairly aggressive data-rights requirements, Owren-Wiest notes. "The question is, at what point do these requirements cross the line? The statute 10 U.S.C. 2320 says that the government cannot require a contractor to relinquish greater rights in technical data as a condition of being responsive to the solicitation or eligible for award. Also, the government cannot prohibit or 'discourage' contractors from proposing to deliver a solution that was developed exclusively at private expense solely because the government's rights in the data related to that solution may be restricted. Those two restrictions have never been tested. What does it mean to be 'discouraging'? In the next year or so, we will probably see contractors testing those prohibitions."

Government agencies are also being more proactive about questioning contractors' data-rights assertions. "We are seeing more formal challenges to contractors' assertions and markings by the government during contract performance, resulting in more formal disputes," Owren-Wiest says. For example, the contractor may deliver noncommercial technical data or software with limited or restricted rights because they were funded exclusively at private expense. Nevertheless, the government may question the contractor's markings and rights assertions if it believes that some portion of the development was funded by the government. The government is increasingly likely to issue such challenges when the contractor's solution was tested or modified at some point under a government contract. "If these challenges can't be resolved by the parties, they lead to contractor-government litigation at the Civilian or Armed Services Board of Contractor Appeals or the Court of Federal Claims," she says.

Heightened competition in the federal market appears to be another factor prompting disputes—here, in the form of more misappropriation claims by and between contractors. Increasingly, losing contract bidders are claiming the theft of trade secrets or violations of nondisclosure or proprietary information agreements against the winning bidder. This typically happens when an employee leaves one company for another or when a teaming agreement falls apart—and the issue may well end up in court. "Those claims are not necessarily a new thing, but we're seeing more of that litigation because the marketplace is getting so much tighter," says Owren-Wiest.

In light of this evolving approach to data rights, companies doing business with the government—especially companies that do not have much government contracting experience—need to reassess and perhaps rethink some of their approaches to IP. "Companies need to understand the government's very different, complex, and nuanced rules around IP and how they could affect your IP," says Owren-Wiest. "And given the government's interest in wanting more in terms of data and data rights, companies should consider ways to rethink their business model and product and service offerings to adapt. What can you do to protect your core IP? How do you build the flexibility that will let you give the government what it wants without getting into your secret sauce? Because going forward, you may need to do things differently."

# The Growing Risk of Disability Litigation

## Health Care

Federal agencies and private plaintiffs are increasingly focused on disability issues with businesses—and that could have a broader ripple effect across health care and other industries.

"As cultural attitudes and norms have evolved to more accurately, and rightfully, view individuals with disabilities as fully enfranchised members of society, the litigation landscape has evolved as well," says Brian McGovern, a partner at Crowell & Moring. "Increasingly, individuals with disabilities and the government agencies charged with enforcement of disability laws have sued in federal courts to vindicate alleged violations."

The number of disability lawsuits against businesses has been growing for a decade or more. Plaintiffs have brought Americans with Disabilities Act suits on many fronts, from inadequate wheelchair access at offices to a lack of sign-language interpreters for hearing-impaired children. Some suits have claimed that websites are essentially places of business that fail to accommodate those with hearing or vision problems—an argument that is likely to continue, since the Supreme Court in June 2019 declined to hear a case that could have clarified requirements for online access. And in many cases, plaintiffs have employed "drive-by lawsuits," a dubious tactic in which plaintiffs' attorneys look at photographs and aerial views of businesses—often small local operations—to find ADA violations.

These trends are now playing out in segments of the health care industry. Recently, there has been increased discrimination litigation targeting medical and senior living communities for allegedly failing to accommodate a resident's or a patient's disability. There are various laws against discriminating against the disabled, but "chief among the arsenal of statutes invoked by disabled and government litigants is the ADA," says McGovern. He notes that the ADA's reach extends beyond employment discrimination to the provision of services and amenities offered by "public accommodations," which can include such living facilities.

The ADA also covers a broad range of disabilities, including physical disabilities such as sight and hearing problems and behavioral or mental health disabilities. In 2019, the Department of Justice settled ADA actions against a Massachusetts operator of a chain of nursing homes and a Virginia care facility that had denied admission to patients who were being treated for opioid-use disorders.

### Ties Tighten Between Federal and State Investigations

The DOJ has been increasing its collaboration with state enforcement agencies on various fronts—and that now includes a more formal approach to cooperating in Medicaid fraud investigations.

At the federal level, the DOJ is the chief enforcement agency for Medicaid fraud, aided by the Office of Inspector General in the Department of Health and Human Services. At the state level, the Medicaid Fraud Control Unit is the primary enforcer. These agencies are charged with the prosecution of providers that claim improper Medicaid payments involving federal and state dollars. "It has become increasingly common for the two groups to work in tandem on investigations and prosecutions, as they have taken advantage of technology to share claims data and pursue their common goals," says Crowell & Moring's Brian McGovern.

In 2019, the OIG and the Centers for Medicare and Medicaid Services strengthened the required level of cooperation between federal and state authorities with new rules. For example, these rules direct Medicaid Fraud Control Units to share information on investigations and prosecutions with federal investigators, to set up regular communication with OIG investigators and federal prosecutors, and to coordinate with federal agencies on similar investigations or prosecutions that involve the same suspects or allegations.

"This cooperation can increase the risk of a provider's exposure, particularly when the billing practice implicates both Medicare and Medicaid," McGovern says. "And any individual or entity that is the subject or target of a Medicaid and/or Medicare fraud investigation by either state or federal enforcement authorities should be prepared to interface with both authorities. Being able to deal with both sets of prosecutors may be crucial to minimizing legal jeopardy for a Medicaid health care provider caught up in such an investigation."

"The reach of some statutes goes beyond the health care and senior care sectors and extends to hotels and other public accommodations." **Brian McGovern**

Care facilities are also seeing enforcement actions taken under the Fair Housing Act, which prohibits discrimination in housing against the disabled. The FHA broadly applies to "any building, structure, or any portion thereat which is occupied as, or designed or intended for occupancy as a residence"—which can include various forms of senior housing, such as nursing homes, long-term care and assisted living facilities, and continuing care retirement communities (CCRC). "In the CCRC context, a complaint that is often raised is the denial of access to the dining room and other amenities to residents in the assisted living level of care, or who are in need of assistance with ambulation, such as the wheelchair-bound," says McGovern.

## New Approaches to Investigations

Private litigation against such senior and group living facilities has become common, and "some public interest groups have brought class actions, particularly against larger systems, to change their policies and practices," says McGovern. In terms of government actions, the ADA can be enforced by the Department of Justice, while both the DOJ and the Department of Housing and Urban Development have the authority to enforce compliance with the FHA. Traditionally, these agencies have worked by receiving complaints or identifying residents of those facilities who feel they have experienced discrimination and then taking action on their behalf. But now agencies are not waiting for issues to be reported and are instead employing a relatively new tactic: proactively looking for problems using cold-calling techniques.

"One of the tools utilized by DOJ, HUD, and other enforcement agencies is deploying a 'tester' who contacts the facility and acts as an individual with a disability to inquire about the availability of services and accommodations for a disabled person," says McGovern. "If the senior housing or congregate-living provider doesn't offer or explain the available services, the agency may take action." From the agency's perspective, these mock calls are highly efficient. "It's a low-cost investigative tool," he says. "It doesn't take much staff time and effort to make a call, record it, and then fashion a case around that."

The repercussions of noncompliance can be significant. Enforcement actions can lead to penalties. These are usually not especially high—very often well below six figures—and in some cases, damages are awarded to individuals who have been affected. But beyond such penalties, the costs of litigating a claim can add up. In addition, many cases are resolved through consent decrees that stipulate the requirements for avoiding liability going forward, such as changing policies and procedures or building or modifying physical structures to accommodate the disabled. On top of that, says McGovern, "there is often the potential for ongoing oversight of a facility's operations." But the biggest potential cost, he says, is harm to a company's reputation. "When a health care provider is accused by a government agency of discriminating against the disabled, it can have a materially adverse impact on the company. The case will be publicized, and it will put the facility in a harsh light," he says.

For senior and long-term care providers, the heightened focus on compliance with disability laws will likely continue, says McGovern. What's more, this scrutiny—and agencies' more aggressive tactics—may be expanded to industries outside of health care. "The reach of some statutes goes beyond the highly regulated health and senior care sectors and extends to hotels and other public accommodations," he says. For example, the ADA's coverage of public accommodations includes hotels, while the FHA applies to a wide range of housing. Section 504 of the federal Rehabilitation Act prohibits disability discrimination by any entity receiving federal funding. And Section 1557 of the Affordable Care Act extends those protections to people participating in the act's health insurance market plans.

With those laws, private plaintiffs and government agencies alike have a lot to work with. To mitigate the risk of litigation or enforcement action, companies should begin by evaluating their physical plant and operations, and assess whether, and how, they can make their offerings accessible to individuals with disabilities. They should also consider proactively revising their policies and practices to help ensure that they are meeting the needs of the disabled. "Equally important, the company—from the governing board to the executive suite to middle management and down to operations staff—must adopt and embrace the company's commitment to nondiscrimination as a corporate value," says McGovern.

Companies also need to pay particular attention to the front lines of the business—the employees who are the face of the company to patients and agencies. "You should educate staff to make sure they know exactly how the company accommodates individuals with disabilities," says McGovern. "That way, when the test caller—or an actual disabled person—comes calling, the marketing or admissions staff will know that information and be able to effectively communicate it, and in doing so, possibly stave off an enforcement action."

# Venue in Patent Cases: The Sea Change Continues

## Intellectual Property

When the Supreme Court issued its landmark *TC Heartland* decision in 2017, it changed the venue calculus for patent plaintiffs and defendants and reshaped the patent litigation landscape. But two years later, some important issues are still being worked out in the lower courts.

Until recently, the Eastern District of Texas was the favored venue for patent owners suing corporations for infringement, and particularly for so-called patent trolls. This was based largely on a perception, generally supported by the statistics, that East Texas juries were more likely to find for a patent plaintiff and award significant damages than juries in other jurisdictions. In addition, the court had established local patent rules that required parties to do a significant amount of work early in a case, "and that put pressure on defendants to settle low-value cases quickly because they would otherwise have to start incurring significant defense costs almost right away," says Mark Supko, a partner in Crowell & Moring's Intellectual Property Group. "The court typically was not receptive to early summary judgment motions to dispose of seemingly weak patent assertions. The Court of Appeals for the Federal Circuit had simultaneously interpreted the patent venue law quite broadly, essentially requiring only that a defendant had sold the infringing product in the district."

In 2017, however, the Supreme Court's *TC Heartland* decision rejected the Federal Circuit's interpretation of the patent venue law, holding that in order to bring a patent lawsuit against a company in a given district, that company must either reside in that district or have a "regular and established place of business" and have committed an act of alleged infringement there. As many expected, the decision led to patent cases shifting to other courts. Most notably, as the number of cases being filed in the Eastern District of Texas has decreased, Delaware—where many corporations are incorporated—has become the top venue for patent cases nationally.

For many defendants, this change sounded like good news. "There is a general perception among many practitioners that the District of Delaware provides a more level playing field for patent defendants," says Supko. "It is generally viewed as a neutral court where parties are going to get a fair shake regardless of which side of the 'v' they're on." For example, the Delaware court does not have local patent rules like those in the Eastern District of Texas. And with so many companies being incorporated in Delaware, the court was a popular venue for patent litigation even before *TC Heartland*. "The judges there know how to handle patent cases and do a good job of keeping them moving," he says. "Many of the judges have developed their own specialized procedures for patent cases, they are very comfortable with patents and technology, and they keep abreast of developments in the patent law. So there is a welcome level of predictability when you are faced with litigation there."

### The End of the Patent Death Squad?

Following creation of the *inter partes* review procedure in 2012, the USPTO's Patent Trial and Appeal Board quickly gained a reputation as a "patent death squad," as the board invalidated a high percentage of challenged patents. But the PTAB appears to be no longer living up to that reputation. "A higher percentage of patents appear to be surviving IPR challenges," says Crowell & Moring's Mark Supko. That's partly because the PTAB implemented some rule changes that some view as making institution of an IPR more difficult, but also because the quality of patents being asserted in litigation has generally improved as plaintiffs have reacted to changes in the law calling into question the validity of patents directed to business methods and computer software-implemented processes.

This does not mean that the PTAB is not a workable forum for companies that want to challenge patents asserted against them. While it can no longer be considered a relatively surefire defense strategy, the PTAB is still more likely to invalidate a patent than is a jury. Moreover, there are potential downsides to factor in when considering whether to pursue an IPR. "In particular, a seemingly expanding statutory estoppel applies when a party attacks a patent through an IPR and loses," Supko says. "So later, in litigation, the party can't assert any prior art that it raised or reasonably *could have raised* in the IPR." Several district courts have grappled with the meaning of the "could have raised" provision of the estoppel law, and a broad interpretation could mean the stakes are even higher if an IPR fails.

"A company may now be able to take advantage of the developing venue law by reconsidering where they incorporate or set up operations." **Mark Supko**

That said, the perceived differences between the two courts may not be that significant. Supko and the Crowell & Moring Intellectual Property Group recently analyzed the outcomes of patent cases and certain types of motions at the two courts over the past two years. "There are certainly procedural advantages that the Eastern District of Texas provides to patent plaintiffs, but once cases get rolling, the two courts are similar in many respects," he says.

For example, the analysis looked at the win rates for motions to transfer based on an inconvenient or improper venue, as well as for motions to stay cases pending resolution of an *inter partes* review or other post-grant validity challenge at the Patent Office. "The percentages were similar for the two courts, and generally in line with national averages," he says. The only real difference this analysis suggested "was that the District of Delaware is significantly more prone to grant motions to dismiss for failure to state a claim than the Eastern District of Texas. That's in keeping with the reputation of the Texas court." Overall, he says, some observers have noted that the pendulum at the Eastern District of Texas had already started to swing toward being less pro-patent plaintiff before *TC Heartland*, and this analysis appears to bear that out.

## Hammering Out the Details

Despite the Supreme Court's effort to bring clarity to the patent venue issue, some of what constitutes a proper venue is still being sorted out in the courts more than two years after *TC Heartland*. "The 'residence' requirement for patent venue is easy to apply and generally only requires looking to where a defendant is incorporated or headquartered," says Supko. "Figuring out what constitutes a 'regular and established place of business' has proven to be far more challenging as plaintiffs try to push the boundaries outward, and that's where the action is today." That's especially true for internet-based businesses, where online and cloud-based operations do not necessarily fit neatly within traditional concepts about the location of a business.

For example, in 2017, the Eastern District of Texas ruled that Google content servers housed in a third-party data center qualified as an established place of business for Google for venue purposes (*Seven Networks LLC v. Google LLC*). While some viewed that decision as an effort by the Eastern District of Texas to push the venue envelope in order to keep more cases there, says Supko, the court supported its decision with a detailed analysis of the principles for determining what constitutes a "regular and established place of business" that the Federal Circuit had spelled out in its *In re Cray* decision. More recently, the Northern District of New York ruled that "lockers" that an online retailer installed at third-party business locations for customers to pick up or return ordered goods were its regular and established places of business and therefore supported venue in that district.

The courts haven't heard the last of these issues, says Supko, who expects that patent owners will continue to try to push the boundaries in order to support venue in what they perceive to be a more favorable forum than the defendant's residence. "As cases continue to present new twists on the facts relating to how and where companies are doing business in the digital economy, it's likely that we'll see district courts struggling with these questions, and there will be more case law developing around what constitutes a 'regular and established place of business,'" he says.

As these issues are debated, companies should recognize that patent plaintiffs have nowhere near the level of control and forum-shopping abilities they had before *TC Heartland.* At the same time, they need to weigh the evolving view of just what constitutes a place of business. Recent cases have shown that in addition to traditional offices and manufacturing facilities, various types of physical equipment—including servers and lockers—may qualify as the owner's place of business for venue purposes. "If a company faces a significant risk of patent litigation in what they view as an unfavorable forum, they may now be able to take advantage of the developing venue law by reconsidering where they incorporate or set up operations, and perhaps avoid certain jurisdictions," Supko says.

Some companies may be able to structure their businesses to take advantage of the evolving venue picture. "For companies that find themselves frequent targets of patent trolls, for example, attention should be paid to how business arrangements are structured in undesirable forums," Supko adds. "A company whose business involves the placement of physical equipment away from a traditional brick-and-mortar facility should explore whether it is possible to structure their relationship with the facility owner differently in order to reduce the likelihood that the location will be deemed the equipment owner's place of business. If there's a jurisdiction where you don't want to get sued," he says, "there may be ways to set up your business to reduce the possibility of that jurisdiction being a supportable venue for patent litigation."

# Non-Compete Agreements Get Harder to Enforce

## Labor & Employment

Many businesses have embraced a more aggressive use of non-compete agreements and other post-employment restrictive agreements in recent years. But the broadened use of such agreements has led to increased litigation, and a number of courts are signaling that they are becoming less willing to enforce them.

Companies generally believe that non-compete agreements and other post-employment restrictive covenants are an important tool for protecting their business, including minimizing the leakage of valuable intellectual property. The use of such agreements has evolved. Two decades ago, non-compete agreements were used primarily for senior executives—people who knew the ins and outs of the company's business and could cause real competitive harm by moving to a rival company. But over the years, companies began using the agreements with more and more types of employees. "You started to see it extended to VPs and directors and other mid-level managers," says Tom Gies, a founding member of Crowell & Moring's Labor & Employment Group. "The increased use of stock options and other equity grants also broadened the use of non-competes, as many companies imposed such agreements as a condition of receiving equity."

In addition to non-competes, most companies use some form of post-employment restrictions barring departing employees from soliciting other employees, pursuing customers of their former employer, or disclosing a company's confidential business information. Companies are pursuing more trade secret misappropriation and related business tort claims to address the problem of IP leakage. "This is not just technology companies. Most companies don't want competitors to get valuable information about customers, pricing, profits, and marketing strategy," says Gies. "If an employee leaves and takes that knowledge across the street, it could really hurt a company."

That trend has also been driven by the Defend Trade Secrets Act, enacted by Congress in 2016, which allows companies to bring suit in federal court when they believe that their trade secrets have been misappropriated.

Like many trends, this one may have gone too far. Several years ago, the Jimmy Johns food chain received a lot of negative publicity by requiring most of its employees, including lower-wage delivery drivers and sandwich makers, to sign non-competes. The agreements said that if they left the company, they could not work at nearby companies that earn more than 10 percent of their revenue from sandwiches—for two years. The company settled lawsuits in New York and Illinois over the issue and eventually announced that it would not try to enforce those agreements.

As companies become more aggressive in trying to enforce post-employment restrictive covenants, "there's been a fair amount of pushback by courts that are skeptical of attempts to enforce them and less inclined to grant temporary restraining orders against former employees, particularly medium- and lower-level employees," says Gies. Some courts appear reluctant to enforce

### Mandatory Arbitration: The Battle Continues

Several recent Supreme Court rulings have strengthened the use of mandatory arbitration to resolve disputes with both employees and consumers.

Those rulings have largely been welcomed by business, which sees arbitration as a way to reduce litigation costs. "But there is considerable resistance in other quarters, including several state legislatures, plaintiffs' lawyers, and various advocacy groups," says Crowell & Moring's Tom Gies. The #MeToo movement has brought public attention to the issue by arguing that private arbitration makes it possible to cover up allegations of sexual misconduct. Several states, including California, New York, and New Jersey, have passed laws in the past two years that broadly restrict the use of mandatory arbitration and ban the use of confidentiality provisions in settlement agreements. Last September, the U.S. House of Representatives passed the Forced Arbitration Injustice Repeal Act (FAIR), which prohibits companies from requiring employees to use private arbitration.

These tensions will likely lead to more arbitration-focused litigation—and companies should review their agreements. "The law has moved at light speed," Gies says. "Many agreements that were well crafted a few years ago probably won't get you where you need to be."

"Enforcing non-competes and other restrictive agreements may no longer be the slam dunk case that companies think it is." **Tom Gies**

agreements that could essentially limit a person's right to make a living—especially where the mid- or low-level employee did not have much bargaining power when hired. And in a time when company-employee loyalty has all but disappeared, some courts may view switching jobs as a "new normal," as employees seek to advance their careers through lateral moves.

Non-competes aren't the only agreements being called into question in recent litigation. For three decades, the law in California allowed companies to enforce carefully drafted employee non-solicitation agreements. But in May 2019, the Northern District of California ruled in *WeRide Corp., et al v. Kun Huang, et al* that such agreements were void because they were an invalid restraint on employment. Two previous California cases had produced similar results, but they involved the recruiting business; *WeRide* did not. "A 35-year-old precedent has been knocked on its head a little bit," says Gies.

State statutes reflect the trend of pushing back against the overly aggressive use of post-employment agreements. California has long banned non-competes by statute, and other states have been moving along those lines and limiting the ability to enforce such agreements. Over the past year, Maine, Illinois, New Hampshire, and Maryland passed laws banning non-competes for low-wage workers, while recent Washington state legislation banned them for employees making less than $100,000 annually.

Case law continues to evolve. "A lot of non-compete agreements say that an employee can't go work for a competitor in any capacity—full stop," says Gies. Now a growing number of courts are rejecting those agreements for being too broad, under what has become known as the Janitor Rule. "If you are in IT at a company, why couldn't you go work for someone else as a marketer, a truck driver, or a janitor?" he asks. "Some courts tend to believe there is no real legitimate concern that the former employer would have about that. So there are now half a dozen states that recognize some version of the Janitor Rule."

As a general trend, courts in many jurisdictions are increasingly saying that the existence of restrictive agreements, in and of themselves, is not enough to justify enjoining someone from working elsewhere in the same industry. "This just doesn't sit right with many judges when you're dealing with lower-level employees or where there's no evidence of misconduct," says Gies. All in all, he says, "enforcing non-competes and other restrictive agreements may no longer be the slam dunk case that companies think it is—and that is catching some of them by surprise."

In this environment, enforceability often depends on gathering information showing that the former employee is harming the company. "It's all about getting evidence of skullduggery," says Gies. "Did they take confidential information home or send it to their new employer? Did they start contacting your customers about their move? Have they been soliciting their former co-workers to join them?"

A cornerstone of that effort is, of course, the forensic analysis of computers. "Often people leave tracks that they've sent the company's secret sauce or spreadsheets of customer lists and pricing to their personal email, or downloaded them onto a thumb drive," says Gies. "Then you go to a judge and say, 'This person left in a huff and wouldn't tell us where he went. He downloaded 3,000 documents to his home computer and won't let us look at that.' If you can get that kind of evidence, you have a pretty good case." The importance of taking preventive measures when employees jump ship for a competitor may seem obvious, he adds, but in practice, companies sometimes fail to perform these analyses and simply wipe a departing employee's laptop clean and recycle it for use by others.

Judges are typically open to enforcement lawsuits that feature evidence of wrongdoing, Gies continues. He points to a case in which Waymo, Google's autonomous driving subsidiary, sued a former key engineer for allegedly downloading nearly 10 gigabytes of confidential files before leaving to start his own company and, eventually, joining Uber. He was later fired by Uber for not cooperating in an internal investigation and indicted for taking or attempting to take Waymo's trade secrets.

Companies need to be mindful of the current environment in their recruiting strategies. "As you hire talent, find out if they are party to an agreement and review it. Then write a letter affirmatively disclaiming any interest in information they might have from their former employer. And throughout the onboarding process, make sure that you are minimizing the risk of hiring talent from a competitor and receiving any confidential information," he says. While companies typically have such policies in place, they may want to increase their scrutiny of new employees and include more levels in those processes.

Overall, companies should keep a close eye on the courts' evolving views of restrictive employment agreements and make sure their own agreements—and their expectations about enforcing them—reflect that changing landscape.

# Sharing Supply Chain Risk

## Torts

Legal departments are making recovery—the practice of proactively pursuing the payment of funds owed to them—a regular part of their operations. They have typically focused on recouping funds from other companies over issues such as IP, antitrust, financial services, and health insurance. But now some are using recovery techniques to mitigate losses stemming from product recall and warranty issues. In addition to mitigating losses, a formal recovery program can help to establish clear supplier expectations and drive desired behaviors.

Such "supply chain recovery" efforts are becoming more important largely because of the increasing complexity of products and the consequences of that complexity. "Products and their component parts are becoming more complicated, given, among other things, their connectivity and the increasing number of features they offer," says Rebecca Baden Chaney, a partner at Crowell & Moring.

At the same time, products are more likely to be offered in various, and often custom, configurations. "The need to deal with this complexity will only continue to grow in an increasingly digital world, where component part technologies need to interact seamlessly with one another," Chaney says.

Mastering it all is often more than one company can do on its own—especially at a time when speed to market is key. Thus, manufacturers of both finished parts and complex components have become more and more reliant on ecosystems of suppliers for design, testing, expertise, capacity, and innovation. As suppliers and sub-suppliers play this growing role, the defects that appear in the parts they produce can have a significant impact on their customers' end products. And, says Chaney, "given the sophisticated nature of today's products and the emerging technologies involved, there are simply more things to go wrong."

When product recalls or unacceptable warranty levels emerge, they can create sizable costs for product and component part manufacturers, and being able to identify the point of origin is imperative. "Once one learns where in the supply chain the defect surfaced, there can be an opportunity to use the parties' supply contracts and, if necessary, tort theories, coupled with the possibility of litigation, to recover some of those costs," says Chaney. "Legal departments can use their existing knowledge and experience in defending against traditional product-defect matters with customers to act affirmatively to bring dollars in the door." Such recovery efforts can offset the costs of recall or warranty issues and protect the bottom line while helping the legal department to be seen as more than just a cost center.

### Creating a Recovery Program

"It is less common for companies to pursue recovery from suppliers for recall and warranty costs," says Chaney. "But this proactive approach provides a clear avenue for doing so." For companies at all levels of the supply chain that want to increase recovery efforts

## Product Liability in a Connected Age

Today's products are increasingly connected through the internet, and directly with one another via Bluetooth and wireless technologies—and the interactions between them are guided by software. As a result, says Crowell & Moring's Rebecca Baden Chaney, "manufacturers and their suppliers now have to contemplate and guard against a new species of potential product failures and ensuing tort litigation and consider new questions about which partner is responsible or liable for those failures."

For example, Chaney explains, Internet of Things products require power, and with mobile products, that power usually comes from a battery. Batteries can fail for a variety of reasons, and with connected, complex products, it can be hard to sort those out. "When batteries fail in a product because they don't communicate properly with other product components, is the cause the battery's software or the product's? Determining the root cause and responsible party can be tricky, especially because many parties are likely to have contributed to the design of the product." And as new features and functions are provided, determining who is responsible for such problems only gets more complicated. "Manufacturers need to be alert to these issues," she says, "and they need to account for these potential liabilities in the contracts they develop for supply chain partners."

"A good program can enable an open dialogue setting expectations about what is acceptable in terms of defects and warranty-claim volume." **Rebecca Baden Chaney**

on this front, having a formal program is essential. A program needs to be tailored to the specific company and its situation. But in general, it should include processes for systematically monitoring supplier quality along with product recalls and warranty costs—a capability that manufacturers often have as part of a supplier management program. This provides a foundation for identifying situations where it is appropriate to ask suppliers to pick up some of the product-defect-related costs. "You can establish metrics for the business to follow to evaluate losses, whether you're looking at incidents per thousand parts or a dollar figure of warranty claims," Chaney says. A program can help companies identify more recovery opportunities and, often, do so sooner. This could accelerate the recovery of funds and avoid statute of limitations problems.

In setting up this kind of recovery program, it is important to identify the personnel responsible, act as points of contact with suppliers, and escalate problems as necessary. "Sound contract hygiene needs to be part of the program," she notes. "Even before an issue develops, product and component part manufacturers should review their purchase contracts with recovery issues in mind. Manufacturers should ensure that their contracts have strong warranties running from the suppliers and sub-suppliers and that there are good venue and choice of law provisions in the contracts."

Ultimately, such programs can provide a more holistic view of warranty spending as it relates to component parts, which can uncover opportunities that may not have been clear otherwise. When looking at individual products, for example, a given product may not be hitting the threshold for unacceptable defects. But an effective program will let the company see warranty costs across the full set of different parts being provided by a particular supplier, or across the various suppliers whose components are in a product—providing an aggregated big picture that can help uncover opportunities that are worth exploring. It might also allow companies to pursue in the aggregate claims that would not be economically viable to pursue individually.

When recovery opportunities are identified, Chaney continues, "you can decide on a case-by-case basis how to address them. Should it be a business-to-business conversation? Should it involve counsel? Should you pursue some resolution proceeding or litigation?" The point, she says, is that a program can help companies consider more informal ways to recoup losses and potentially avoid the need for litigation.

When litigation is appropriate, a proactive recovery program can help ensure that the company is prepared. In looking at contracts and products, says Chaney, "you can evaluate whether you need a tolling agreement. When will you need a litigation hold? When do you need to track engineering time that's being spent on a problem? Or when do you need to engage outside counsel to protect the privilege of an investigation?"

## Making Things Easier

Pursuing downstream recovery—and especially taking a key partner to court—can be unpleasant. As a result, companies often avoid recovery actions against their suppliers. But a formal recovery program can provide a foundation and the supporting facts for discussing warranty-claims problems. "Nobody wants to be seen as targeting a partner, and good supplier relationships are an important aspect of business," says Chaney. "However, a good program can actually help address that issue by enabling an open dialogue all along the way and setting expectations with suppliers up front about what is and is not acceptable in terms of defects and warranty-claim volume."

Such discussions can lead to creative solutions that help preserve relationships. For example, rather than getting a large cash payout for recovery, a manufacturer might negotiate future discounts from a supplier. In addition, having a fact-based dialogue and clearly defined expectations might help boost component quality. "If a supplier clearly understands that you are closely monitoring a supplier's return part and warranty rates and are going to seek to recover costs if its parts do not meet a designated threshold, that supplier is probably going to work proactively to make sure it stays below that threshold," says Chaney.

With a formal recovery program, the company replaces the traditional one-off or ad hoc approaches to recovery with an established, repeatable process—a recovery "machine," as Chaney says. "A manufacturer or upstream supplier then has the mechanisms in place to efficiently pursue smaller claims as well as large ones." This docket approach treats groups of claims as a portfolio to optimize recovery efforts and opportunities. "A company can manage the whole docket, so when small recovery opportunities by themselves may not be meaningful, it can pursue them as a group and cumulatively make it worthwhile.

"These matters come in all shapes and sizes," Chaney continues. "They can be very small, but collectively they can reach eight or nine figures. By having a good program in place, manufacturers can look at their supplier-caused losses and understand how much it is adding up—and then make the most of recovery."

# Smarter Phones, Bigger Risk

## White Collar

Smartphones are a universal fact of life in business today, where they help companies increase speed and productivity. But when it comes to potential white collar investigations and litigation, they are raising some difficult questions about preserving and accessing data.

Smartphones have not only proliferated in recent years, they've also become more sophisticated, expanded to encompass a broader range of functions, and added increasingly powerful security, including password protection, biometric access control, and data encryption. And they've become deeply interwoven in people's lives. As a result, "many companies have a 'bring your own device' culture, allowing people to use their own phones for business purposes," says Glen McGorty, a Crowell & Moring partner and a former federal prosecutor in the U.S. Attorney's Office for the Southern District of New York and the Department of Justice in Washington, D.C.

When it comes to accessing data in order to respond to a subpoena, smartphones represent a fundamental change from the past. Decades ago, business records were kept in company file cabinets. Since then, business data has steadily moved to new platforms—mainframes, personal computers, company servers, the cloud. But throughout that evolution, data has still remained under the company's control and been relatively easy for the company to access.

With smartphones, on the other hand, data is often held on the device, not merely on the server to which it has access, and that device, which contains both personal and business information, is not under the company's direct control. "The medium has changed, but the company's obligation to be able to look through and provide data for investigations and litigation has not—even if the phones are not owned by the company," says McGorty. "And the phone can be a much harder 'file cabinet' to search than computers and servers."

For example, McGorty continues, "search warrants cannot compel an owner to provide a password in light of Fifth Amendment protections, and even the government has a hard time collecting material from smart devices." That point was underscored in 2016, when the FBI tried to compel Apple to create software to unlock an iPhone belonging to one of the attackers in the San Bernardino, California, terrorist shootings. Apple refused and the case went to court. However, the day before the trial, the FBI announced that it had found a third party that could unlock the phone without deleting its data.

To avoid such problems—and potential litigation and compliance issues—companies need to have rigorous policies that clearly address the question. "They need to carefully establish how their data will be stored and how it will be accessible," says McGorty. "Make it clear that by consenting to the use of their own personal devices for business, employees can't deny an employer access to the business-related data on that phone if the company needs it. And make sure employees are aware of that and sign off on it." At the same time, he says, companies need to make sure that they have a process in place that lets them easily capture and retrieve data from phones if that becomes necessary. "If you're not doing those things up front and it all comes to a head in an investigation," he says, "the government may well decide that you aren't properly preserving data."

### Ephemeral Messages Create Concrete Problems

In addition to managing physical access to smartphones, companies need to think about the growing range of apps running on those devices—in particular, ephemeral messaging apps such as SnapChat, Wicker, and Confide. These typically let

"The medium has changed, but the company's obligation to be able to look through and provide data for investigations and litigation has not." **Glen McGorty**

users send encrypted messages that then self-destruct after they are read. This naturally disrupts the preservation of business-related messages.

The use of ephemeral messaging in business has been increasing over the years. In 2017, the DOJ responded by adjusting its Foreign Corrupt Practices Act enforcement policy to require companies seeking cooperation credit in government FCPA investigations to prohibit their employees from using "software that generates but does not appropriately retain business records or communications."

However, the DOJ changed that policy in March 2019—perhaps in recognition of the widespread use of ephemeral communications in business. Now, instead of prohibiting such apps, the DOJ requires companies to implement "appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations."

That change provides some flexibility in using ephemeral messaging, but it also introduces new complications. By including the term "personal messaging," the DOJ has made it clear that it is interested in other types of messaging apps, such as WhatsApp, that are not ephemeral in nature. These apps are frequently used outside of company IT systems, and employees often use them on multiple devices, such as tablets and home computers—all of which could make it difficult to track data down. And companies still need to preserve business records from both ephemeral and personal messaging apps. Doing so will not only require costly tools and complex rules, but it will also introduce the possibility of inadvertently accessing employees' personal information.

With that in mind, companies may decide that it's easier to simply prohibit employees from using personal and ephemeral communications. But that can bring challenges in its own right. For example, monitoring usage to enforce the prohibition is likely to be intrusive and could lead to data-privacy issues. A blanket prohibition would also mean that employees are unable to access tools that are increasingly important in business.

Here again, putting the right policies in place will be key. "You need to explicitly spell out how information will be preserved and how you'll govern these types of communications, and absolutely dictate the circumstances where you believe that it's appropriate to permit the use of this sort of communications," says McGorty. "The more specific and articulate you are, the better.

"Under DOJ guidance, you really need to be able to articulate how and why you're using these apps—the real business reasons," he continues. Often, there are good reasons for doing so, such as the immediacy of the communication, an improved ability to do business in industries and regions where these apps are widely used, and, of course, security. "Certainly, the less data that's out there, the less likely you are to have data stolen," he says.

However, by asking businesses to explain their reasons for using these apps, the DOJ guidance is opening the door to more litigation. "Companies will be coming up with arguments rationalizing why they are using these communications for business purposes," McGorty says. "So by removing the absolute prohibition against ephemeral communication, they're creating a window for subjective interpretations—and it's very likely that litigation will be arising from that."

## The Growing Reach of RICO

When Congress passed the Racketeer Influenced and Corrupt Organizations Act in 1970, it became a well-known tool for fighting organized crime. "But the law also allowed civil remedies, and a growing number of plaintiffs have been using RICO to move fairly ordinary business disputes into federal courts," says Crowell & Moring's Glen McGorty.

In recent years, companies in the pharmaceutical, social media, automotive, entertainment, medical marijuana, and finance industries have been the focus of private RICO lawsuits. In general, these claim that a company or class has been wronged by the alleged corrupt actions of a company, and that those actions are part of running a criminal enterprise.

RICO cases can be hard for a private plaintiff to win. But many are motivated by the possibility of winning treble damages and attorneys' fees under the law, and they are likely to keep looking for new ways to use the RICO statute. As a result, says McGorty, "general counsel should keep an eye on this trend, factor it into their risk assessments, and consider whether to implement a RICO compliance program."

# Class Actions: A New Era in the UK?

## UK Litigation

In the UK, regulatory scrutiny of data breaches has resulted in significant fines. But the repercussions of those actions are highlighting broader changes in the nature of collective actions that are starting to take root in the country.

In July 2019, the UK Information Commissioner's Office (ICO), the country's data protection and information rights regulator, announced that it planned to fine British Airways £183 million—about 1.5 percent of the airline's annual revenue—for a 2018 data breach incident. It was by far the largest fine levied to date under the EU's General Data Protection Regulation, which went into effect in May 2018. And many observers noted that the "mega-fine" marked a new, aggressive approach to data-privacy enforcement on the part of UK regulators.

But the British Airways case also points to another, and perhaps more significant, development—the potential rise of class action litigation in the UK. Not long after the ICO announced the fine, a group of UK plaintiffs launched a class action lawsuit against the airline under the GDPR, which provides a private right of action, and UK legislation makes such claims fertile ground for a class action. In October 2019, the High Court in London said that the lawsuit, involving some 500,000 plaintiffs, could proceed. That same month, another group of plaintiffs filed a class action lawsuit against Equifax for its 2017 data breach, seeking £100 million in compensation for the 15 million affected UK consumers. That lawsuit followed a £500,000 fine imposed on the consumer credit-rating company in 2018 for the breach—the maximum fine then allowable under pre-GDPR law in the UK.

Such high-profile group actions have been fairly rare in the UK, in large part because the country's laws around collective actions—its approach to class actions—have limited the use of such lawsuits. "Over the years, there have been just a couple of notable cases, and they have tended to be primarily personal injury claims," says Robert Weekes, a London-based partner in Crowell & Moring's International Dispute Resolution practice. "The mining industry, for example, faced some personal injury group actions due to health issues with coal dust. But that's about it."

The situation has clearly changed following the GDPR. "It appears to be developing into more of a U.S.-style model here, with the ability for numerous claimants either to join or to be part of the same action," says Weekes. "So corporations are now facing the possibility of having thousands and even millions of claimants against them in one particular action, which breaks new ground here in the UK."

Regulators are clearly focused on data breaches, and in this emerging environment, their actions are likely to have a ripple effect across the UK legal landscape—creating a pattern of litigation that is only too familiar to U.S. companies. For example, when the ICO determines that a company is liable for a data breach and issues a penalty, plaintiffs' attorneys are likely to move quickly to file follow-on class action claims. "There will be data subjects who have had their data breached, and they will be entitled under the GDPR to bring claims," says Weekes.

As costs of that litigation grow, he says, "there will inevitably be attempts to share the blame, and companies will be looking down the contractual chain to attempt to pass at least some of the liability on to suppliers and vendors. We can expect arguments about who the controller of data is, who the processor of data is, and so forth." And finally, he says, "there eventually will be insurance-led claims. Cyber insurance is becoming an extremely important component of company insurance. So there will undoubtedly be claims against insurers around coverage issues."

"It appears to be developing into more of a U.S.-style model here, with the ability for numerous claimants to join the same action." **Robert Weekes**

Data breaches are not going away, and neither are regulators that are willing to scrutinize those breaches. As a result, says Weekes, corporate legal departments in the UK "should be preparing for a knock on the door from the regulators, because those regulators are more active and their powers are very wide-ranging." And increasingly, class action lawsuits are not likely to be far behind.

## The Potential Spread of Class Actions

The GDPR is certainly a significant driver of class action litigation in the UK, but it is not the only factor changing the legal landscape. When the country's Consumer Rights Act of 2015 became law, it provided England and Wales with class action-type options, saying consumers could, as a group, sue companies that had violated competition laws. What's more, claimants do not have to be from the UK, meaning online companies and companies based in other countries could find themselves being taken to court in the UK by groups of claimants.

The act opened the door to more class actions in other ways, as well. In the past, when consumers had a complaint against a company, they had to opt in to a group action—that is, actively sign on to participate. The 2015 law changed that with an opt-out option, which essentially meant that any UK citizen affected by a company's alleged action can be automatically included in the group action, unless they have proactively opted out of it. Overall, this tends to increase the size of groups of plaintiffs involved in a class action, making potential awards much larger. What's more, as some claimants opt out to pursue their own individual lawsuits, companies may find themselves facing litigation over an issue on multiple fronts.

As such trends alter the view of collective actions, "class action lawsuits could be applied to other types of consumer actions beyond data breaches," says Weekes. Already, he says, there is legislation being proposed that would in fact extend class actions to consumers' claims in general. The courts are also moving the class action concept forward. Weekes notes, for example, an October 2019 decision by the UK Court of Appeals that said that a law firm could bring a claim for just one plaintiff who had allegedly been harmed by a company's actions, but be awarded compensation for the entire population that had been affected by those actions.

At the same time, continues Weekes, "we're seeing a significant growth in third-party-funded litigation in the UK—and over the past year, it's exploded. There's plenty of liquidity around in hedge funds and other financial vehicles to provide that funding." Class actions, with their potentially large payouts, are of growing interest to these funders. "They're becoming very much involved in helping claimants fund their lawyers and expert fees," he says. "That will make it possible for claimants to file more class action claims, and those claims will be better resourced as a result of access to funding."

The UK is probably not going to see an abrupt total shift to U.S.-style class action litigation, thanks to some key differences. For example, unlike the U.S. approach, parties that lose lawsuits in the UK pay the other side's legal costs, and judges are not able to award treble damages; these are factors that tend to make a rush to court appear less attractive. Nevertheless, says Weekes, there does seem to be a cultural change among legislators, regulators, and the broader legal community that is making the environment more open to an extended use of class actions—and legal departments should keep an eye on how those changing attitudes are affecting the risk of litigation.

## More Transatlantic Cooperation?

In September 2018, officials from the U.S. Department of the Treasury and the UK's HM Treasury, along with various regulatory agencies from both countries, came together in London for the first meeting of the U.S.-UK Financial Regulatory Working Group, which was formed "to deepen our bilateral regulatory cooperation" to support financial stability and investor protection in both countries. A second meeting was held in May 2019 in Washington, D.C. "And it looks like those meetings might be starting to create some cross-border synergies," says Crowell & Moring's Robert Weekes.

For example, Weekes says, the UK Serious Fraud Office announced a bribery investigation into the Glencore mining company, which is also facing a corruption investigation by the U.S. Commodity Futures Trading Commission. "Whether by coincidence or design, this could signal that U.S. and UK authorities are positioning themselves to work together to investigate and prosecute cross-border wrongdoing," he says. "It will be important for legal departments to think about how to work on both sides of the Atlantic and to balance their approach to ensure compliance with the distinct rules of each regulator."

# False Advertising Claims: Opting for Court

## Advertising

For years, many companies that have taken issue with their competitors' advertising claims have relied on the self-regulation process to sort out their concerns. But lately, some seem increasingly ready to take a different avenue—and head instead to federal court.

The National Advertising Division, part of the Council of Better Business Bureaus, is a voluntary forum in which companies can challenge competitors' advertising. Traditionally, many companies preferred to bring false advertising disputes before the NAD as a matter of course. They viewed the NAD process as fast and inexpensive compared to litigation on the merits. Unlike a court trial, there is no formal discovery at the NAD, and the burden of proving that claims are substantiated falls on the advertiser that is challenged, rather than the challenger. And the process is relatively straightforward: "You initiate a challenge by writing a brief," says Holly Melton, a partner at Crowell & Moring and vice-chair of the firm's Advertising & Media Group. "Each side has the opportunity to provide two written submissions, unless the challenge is expedited, in which case each side submits one written submission. Each side then meets separately with the NAD, after which the NAD issues a written decision with recommendations."

The advantages of the self-regulation process seem clear enough. But recently, some companies have been willing to forgo the NAD process and instead take their competitors to federal court. "In the past year or so, we've seen an uptick in Lanham Act false advertising litigation," says Melton. "Many advertisers have elected to pursue claims in federal court, even when the advertising at issue is not necessarily expressly false but only impliedly so, which carries the additional evidentiary burden of proving consumer deception." Recent Lanham Act cases have involved companies in the telecommunications, consumer goods, and food and beverage industries.

There has also been an increase in the number of companies that, when challenged, either decline to participate in the NAD process or refuse to comply with its written decision. In those instances, the NAD automatically refers the matter to the Federal Trade Commission, a move that carries the risk of a government investigation and litigation by the agency.

The reason for companies' increased willingness to fight it out in federal court seems to stem from a combination of factors.

"We've seen an uptick in false advertising litigation. Many have pursued claims in federal court." **Holly Melton**

For one, some companies say they have perceived a shift at the NAD. "Companies used to report that the NAD's approach to cases was somewhat predictable, and a decision that split the baby to give each side a win on at least one issue was commonplace," Melton says. "Today what I more often hear from advertisers is that they view the NAD process as less predictable, and we are seeing more decisions with a clear winner and a clear loser." With this in mind, some companies may be making the calculation that they might be just as well off in court.

Melton says that the stronger appetite for litigation may also be the natural result of more aggressive marketing strategies and the increased use of expressly comparative claims, as well as increased competition overall. In that kind of environment, an aggrieved company "might feel the need to litigate to send a stronger message," she points out. In addition, federal court offers the possibility of monetary damages, which the NAD proceedings do not. NAD rulings are often prescriptive and call for modifications to advertising. "A federal judge is going to be less inclined to give specifics about how to change the ads," she says. "So some companies may be less interested in receiving, and being required to implement, specific feedback regarding how to shape their advertising."

General counsel need to understand these changes. "It used to be that if your advertising was literally truthful but subject to being construed as misleading, companies could rest easy that the most likely avenue for a challenge would come through NAD. Companies were less likely to be challenged in court because of the higher evidentiary burden relating to impliedly false advertising claims," says Melton. "I don't think companies can rest so easy these days. They should be aware of the increased appetite for filing false advertising cases in court."

# Importing: Risky Business

## Trade

For companies that import goods into the United States, increased tariffs have made business much more complicated and expensive. They are also bringing risk on the legal front.

Such risks came to the fore in May 2019 when, following a whistleblower's lawsuit, the U.S. Attorney's Office for the Southern District of New York filed a civil fraud lawsuit against Stargate Apparel and Rivstar Apparel and their CEO. The suit alleged that they had violated the False Claims Act by understating the value of goods they were importing to avoid duties, costing the government more than $1 million in revenue. There have been a growing number of such cases recently—and there are likely to be significantly more in the near future, says David Stepp, a partner at Crowell & Moring.

"With the Trump administration's Section 301 tariffs against China and other countries, there's a lot of pressure on companies that import finished goods and components to reduce the value of their goods coming into the U.S., because the duties are a percentage of the value," says Stepp. He notes that FCA cases can also be filed against companies that declare the incorrect country of origin of the goods—claiming, for example, that goods made in China were actually made in Vietnam.

"With the administration's protectionist policies and increased scrutiny on making sure duties are paid, we anticipate seeing the government taking up more of these FCA cases," says Stepp. That trend will only be accelerated by the incentives given to whistleblowers to report problems, and by the Supreme Court's 2019 ruling in *U.S. ex rel Hunt v. Cochise Consultancy,* which extended the statute of limitations to allow whistleblowers to file lawsuits up to 10 years after a false statement was made if the government has not learned of the violation. And, says Stepp, "there are plenty of plaintiffs' attorneys out there who are willing to file on those whistleblowers' behalf."

Even if the tariff issue recedes over time, importers face other sources of increased risk. For example, misrepresentations of the same factors used in FCA cases—the value of goods, country of origin, classification, and antidumping duties—can also lead to penalties from U.S. Customs and Border Protection under Section 592 of the Tariff Act. What's more, the Department of Justice is reportedly bringing additional attorneys onboard for the International Trade Office in Washington, D.C., which typically handles trade penalty cases. "This likely means that CBP has already determined that a significant amount of penalty cases are not going to be resolved administratively and will proceed to litigation," says Stepp.

"With the administration's protectionist policies and increased scrutiny on making sure duties are paid, we anticipate seeing the government taking up more of these FCA cases." **David Stepp**

On a different front, there is increased scrutiny on incoming goods produced with forced or child labor, contrary to U.S. laws. "That's really a top priority right now for CBP, the Department of Labor, and other government agencies," says Stepp. However, he says, "it's a relatively new area for them from an enforcement standpoint, so they are trying to determine what the base standard is for each industry, and what their obligations are. And even the definition of forced labor is pretty murky under the current guidelines." In the fall of 2019, CBP issued a number of withhold release orders (WROs) covering a range of products, such as apparel, gloves, and minerals, from at least five different countries. The result is likely to be more litigation from companies that have had their goods excluded, seized, or forfeited as a result of WROs issued by CBP.

In this environment, it is more important than ever for general counsel to work in sync with the business and its global supply chain. "They need to make sure that they have processes in place that let the company make accurate declarations about valuing and classifying imported goods and their country of origin," says Stepp. In general, he says "they really have to do their homework to navigate through the turmoil that's currently out there in the international trade world."

crowell moring

For more information, contact:
Mark Klapow
mklapow@crowell.com
Phone: 202.624.2975
1001 Pennsylvania Avenue NW
Washington, DC 20004-2595

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

## Making the Connections

At its heart, the digital revolution is about connectivity. Connections between companies and consumers, between manufacturers and their supply chains, even between companies and the products they create. While this new era ushers in tremendous opportunities for companies and consumers alike, it also comes with challenges. Products break, connections are lost, IT systems are breached, data is stolen, privacy is compromised. In-house counsel face a dilemma in the new digital age. They must pave the way for innovation while simultaneously minimizing risk in an environment where both the products and the law are often without precedent.

Meanwhile, developments on the regulatory and litigation fronts are moving swiftly. Government regulators are at work, striving to make sure that both technology and the law serve to protect all parties that technology touches: individuals as well as companies up and down the supply chain. And new litigation threats loom, as government enforcers and plaintiffs' lawyers employ new rights of action to pursue companies for the breaks and breaches that arise as new products are brought to market.

Our goal—as a firm and through this *Litigation Forecast*—is to help our clients navigate the increasingly complex connections between litigation and regulation, between technology and all the parties that depend on it. As our lawyers explain throughout this volume, digital transformation has changed the way business is done and enhanced connectivity for a better future. This *Forecast* is designed to help you, our clients, navigate the risks that will arise along the way, so that your business and legal strategies will work in lockstep with one another and stay connected as the new digital economy matures. We look forward to hearing from you and to continuing the conversation.

**Philip Inglima**
Chair, Crowell & Moring