STATE OF PLAY

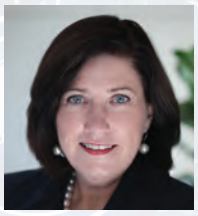
DIGITAL TRANSFORMATION: THE SKY'S THE LIMIT

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

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

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

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



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

—CHERYL FALVEY

GETTY IMAGES

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

—SCOTT WINKELMAN

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

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

THE REGULATORY CHALLENGE

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

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

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

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

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

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

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

and ultimately leave consumers worse off."

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

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

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

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

INTERNATIONAL DATA FLOWS: OPEN OR CLOSED?

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

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

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

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

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

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

—ROBERT HOLLEYMAN

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

—KATE GROWLEY

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

—JODI DANIEL

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

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

DIGITAL HEALTH: REGULATING FOR INNOVATION

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

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

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

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

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

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

CYBERSECURITY: A YEAR OF COMPLEX RISK

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

Companies have a growing, increasingly interconnected digital footprint. Protection of those systems and their data, once a sleepy back-office matter, has taken center stage. Digital-related laws and regulations increasingly contain cybersecurity elements—meaning companies face a growing regulatory burden. "2018 will be a year of complex cybersecurity risk and, especially, regulatory risk," says Evan Wolff, a Crowell & Moring partner and co-chair of the firm's Privacy & Cybersecurity Group, who formerly served as an advisor to the senior leadership at the

Department of Homeland Security.

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

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

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

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

SHAPING THE FUTURE

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

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

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

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

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

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

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

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

—JEFFREY SELMAN

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

—EVAN WOLFF