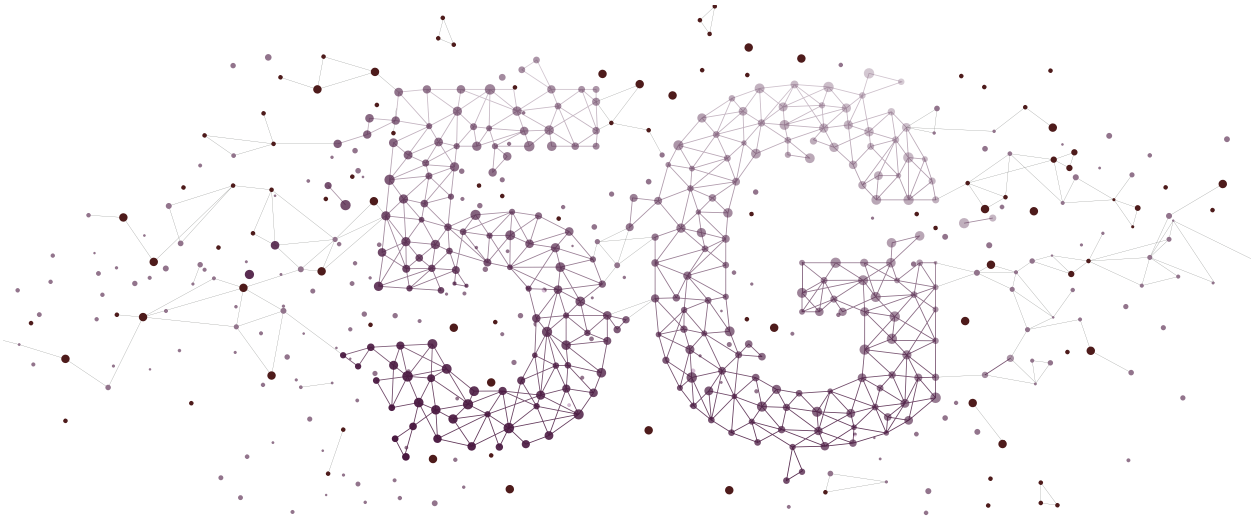
wiley

5G and Government: A Regulator Roadmap



5G and Government: A Regulatory Roadmap

The future of advanced communication is here with the rollout of 5G. A quantum leap in wireless capability, offering incredible speeds, low latency, and the ability to connect far more devices than 4G, 5G will enable the most powerful and dynamic wireless communications network deployed to date. Ubiquitous 5G coverage will proliferate new services and will be necessary to accommodate the growing Internet of Things (IoT), which provides constant broadband connections to a variety of new devices and applications.

- What is 5G?
- How will 5G affect my business?
- How will new technologies and services be regulated?
- What privacy and security issues are raised by 5G?
- What international issues are emerging?

5G will not be a niche regulatory issue—all parts of the global economy will be affected. From telecommunications carriers and ISPs to startups in connected health solutions and retailers deploying machine learning, business models and operations will be changed by a new era of ultra-fast connectivity, distributed networking, and an explosion of devices. Investors around the world are looking to capitalize on the benefits of a truly connected future, while navigating a complicated global trade and security landscape. Likewise, governments around the world are taking action—to spur deployment while also looking at regulatory solutions to privacy, security, and safety concerns.

The "race to 5G" is underway domestically and abroad. 5G will impact law and policy at all levels of government and among a diverse array of agencies in the United States and around the world. Anyone who plans to innovate and take advantage of 5G should consider a variety of issues, opportunities, and risks.

Wiley's 5G team has been helping clients and policymakers shape the future of 5G and beyond, on issues from device regulation to spectrum policy to national security and supply chain concerns.

This primer lays out some of the most important practical, legal, and policy issues arising from 5G, and identifies key players in government. We hope it helps break down cross-cutting issues and identify challenges and opportunities for the diverse set of participants in a global 5G future.

What Is 5G?

The fifth generation of wireless, 5G for short, is the latest step in the evolution of wireless technology and network design. 5G will feature ultra-fast speeds (up to 100x faster than 4G LTE) and highly reliable, low-latency networks, which will enable real-time connections and support innovative services, new applications, and IoT devices.

5G will bring seismic shifts to industries and business:

- ***Industrial uses.*** The connectivity of 5G will support smarter factory equipment and enable companies to conduct remote operations such as production monitoring in real time.
- ***Agricultural uses.*** Farmers can transmit information from sensors and drones. 5G will enable farming processes from planting to crop spraying to be automated and data-enhanced.
- ***Enterprise uses.*** Enterprise uses. 5G's speed, latency, and capacity will foster industrial digitalization through improvements in robotics, automation, and agile, segmented networks.
- ***Health care.*** 5G will enable remote patient monitoring and surgery.
- ***Autonomous Vehicles.*** 5G technologies and networks will be critical for supporting autonomous vehicles' ability to gather, process, and respond to information.
- ***Virtual Reality/Augmented Reality.*** 5G's low latency will create a seamless AR/VR experience.
- ***Drones.*** 5G will help unlock the commercial potential of drones, supporting autonomous flights of multiple drones at once.

Indeed, a recent study across industry sectors found that 74 percent of respondents planned to invest in order to take advantage of 5G technologies in creating value for customers.[1]

Other beneficial uses are on the horizon. IoT technologies enabled by 5G "will enhance supply chain management using identity chips, sensors, communication devices, cloud computing networks, and data analytics engines all working together to fuel automation, continuous feedback, and better decision-making."[2]

American Express expects that the payment industry will get a major boost from 5G, which is the only way to make mobile banking ubiquitous. Likewise, 5G IoT and blockchain can smooth transportation of goods with digital bills of lading.

All told, 5G is expected to add 3 million new jobs, result in $275 billion in new investment, and create $500 billion in economic growth[3] touching every sector of the economy and businesses of all sizes.

Spectrum Access Is Critical to 5G

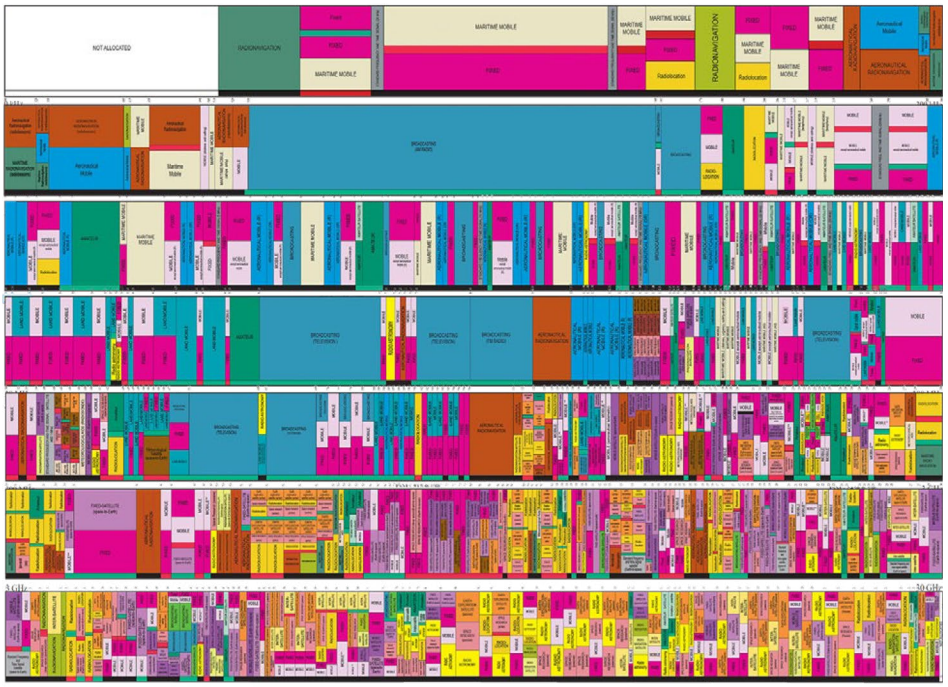
Who should care? **Internet and telecom service providers, and innovators who rely on spectrum access to propel the offering of new services and devices.**

Who are the players? **The FCC, the National Telecommunications and Information Administration in the U.S. Department of Commerce, and the U.S. Department of Defense.**

A robust pipeline of low-, mid-, and high-band spectrum will be required to ensure that 5G reaches its full potential in the United States. The Federal Communications Commission (FCC or Commission) has been aggressive in freeing additional spectrum for wireless use, but more work is left to be done. Companies are engaging with the FCC and the National Telecommunications and Information Administration (NTIA) to promote flexible spectrum policies and continue the effort to identify and unleash much-needed spectrum for 5G use.

Over the past few years, the U.S. government has made 5G spectrum access a top priority, launching numerous proceedings to free additional spectrum and propel 5G deployments forward.

On the low-band front, the FCC repurposed 70 MHz of 600 MHz spectrum for mobile use through the broadcast incentive auction. Mid-band spectrum has also been a key focus. The FCC aims to auction 70 MHz of priority access licenses in the 3.5 GHz band in June 2020, and it continues to weigh options for making the C-band spectrum at 3.7-4.2 GHz available for 5G in the near term. For its part, NTIA has announced that it is studying the feasibility of allowing commercial operations in the 3.45-3.5 GHz band. Finally, on the high-band side, the FCC continues to auction large swaths of millimeter wave spectrum, recently completing two consecutive auctions of the 28 GHz and 24 GHz bands. Future auctions will release more spectrum into the commercial marketplace.



The FCC and NTIA will need to continuously evaluate their spectrum policies to ensure that enough spectrum is available for 5G to deliver the ultra-high speed, low-latency, reliable networks consumers are expecting. Companies can help shape smart spectrum policies from the start by engaging with the agencies early and often. Communicating technological needs and limitations will help policymakers develop better-informed spectrum frameworks for the 5G future.

International Harmonization and Standards Are Critical to 5G Deployment and Interoperability

Who should care? **Internet and telecom service providers, and innovators who want their devices and services to be available in global markets.**

Who are the players? **FCC, NTIA, the UN's International Telecommunication Union, 3GPP, IEEE, CTIA, and GSMA.**

The success of 5G deployment is intertwined with several international activities. Interoperability has long been a hallmark of global telecommunications policy. Global technical standards and spectrum harmonization for wireless services are vital for 5G's success. Regional and national decisions on spectrum band allocations and technical and licensing conditions will affect the ability to fully deploy 5G domestically and abroad. These decisions will also impact the ability of players in the 5G ecosystem to leverage economies of scale.

The 2019 World Radiocommunication Conference (WRC-19), held by the International Telecommunication Union (ITU), will decide the global status of spectrum bands that will be relevant for 5G deployment. The ITU will continue to evaluate 5G issues in study group and working party activities, as well as in regional organizations. It will also begin preparations for the next World Radiocommunication Conference in 2023 (WRC-23), shaping the future for 5G and beyond.

Meanwhile, global standards development organizations (SDOs) such as the 3GPP, the IEEE, and ITU technical working groups are hard at work and will be critical to 5G development. Critical 5G releases have happened to facilitate testing and trials of 5G deployments across the U.S. and around the world.

This is a significant area for engagement by the private sector, directly or through trade associations.

Aside from active advocacy before these standards-setting bodies, working with government officials abroad to ensure that favorable 5G regulatory frameworks are adopted will help facilitate the 5G revolution.

Infrastructure Will Require Government Cooperation with the Private Sector

Who should care? **Internet and telecom service providers, infrastructure owners and operators, and manufacturers of network equipment, as well as businesses and consumers who are hungry for fast, reliable data services.**

Who are the players? **FCC, state and local governments.**

The advent of 5G brings infrastructure needs, and all major U.S. carriers are working to upgrade and deploy needed facilities. This creates regulatory and contractual issues for carriers, infrastructure owners, and the communities that will benefit from connectivity.

> The FCC is "making it easier to install wireless infrastructure. 5G will rely heavily on a web of small antennas. But when I came into office, regulations designed for tall towers threatened to strangle our 5G future in red tape. We've eliminated these rules, because infrastructure the size of a pizza box shouldn't have to jump through the same regulatory hoops as a 200-foot tower."
>
> *– FCC Chairman Ajit Pai, April 2019*

Many initial 5G deployments are occurring on millimeter wave spectrum. The extremely high frequencies of these spectrum bands allow vast amounts of information to be transmitted in the blink of an eye, but the physics of radio propagation dictate that these signals cannot travel far and do not penetrate buildings and other structures as well as the lower frequency signals that have traditionally been used for wireless service. At the same time, as data demands increase, wireless networks are getting more and more crowded, requiring that carriers "densify" their existing networks.

Congress and the FCC have been aggressively addressing infrastructure needed to deploy 5G. Congress has changed the law to promote deployment and streamline review of facilities siting, and the FCC has engaged in rulemakings to tackle regulatory challenges and reduce burdens on construction of these facilities.

But more work remains. The FCC and courts will need to flesh out the permissible scope of regulation under the framework established by the Communications Act and the FCC's previous orders. Most importantly, as technology continues to develop and deployment expands, additional issues will arise. The Commission has signaled its willingness to work with industry and local jurisdictions to make sure issues are addressed so that this transformational technology is not stymied by red tape and obsolete requirements. As such, there is significant opportunity for industry to be engaged at the FCC and in the courts to ensure that infrastructure deployment for 5G can be fully realized.

Data Security and Privacy Risk Management Are Hot Topics in 5G

Who should care? **Manufacturers and sellers of connected devices, applications, and software; internet and telecom service providers; enterprises and end users who will depend on secure connectivity for data.**

Who are the players? **Federal Trade Commission (FTC), FCC, National Institute of Standards and Technology (NIST) in Department of Commerce, state legislatures and Attorneys General.**

Privacy and data security are top of mind for policymakers across the board, including as they look to 5G. There are numerous security and privacy enhancements baked into 5G technologies and networks, including enhanced encryption, increased network virtualization, improved subscriber identity protections, and end-to-end authentication. The result will be a more flexible and secure network.

But nascent and burgeoning 5G use cases, such as IoT, present an increase in attack surfaces, meaning that risk management approaches may need to be adjusted. Agencies across the federal government are weighing in on IoT security: from players that have a long-standing role in cybersecurity issues, such as the Federal Trade Commission and the National Institute of Standards and Technology (NIST), to agencies newer to the field, such as the U.S. Food & Drug Administration (FDA) and the Consumer Product Safety Commission (CPSC).

NIST and the U.S. Department of Defense (DoD) are among many agencies looking at 5G architecture, cybersecurity, and privacy impacts from new 5G use cases. They may develop best practices and models that drive standards of care, or that impose burdens on the private sector.

States are becoming active as well. California and Oregon have adopted IoT security laws that impose security mandates on manufacturers and affect others in the supply and distribution chain. Other states are considering taking similar approaches. Any company involved in the 5G ecosystem should stay abreast of shifting security obligations and best practices.

Companies need to understand what they are making, buying, and using, and have plans for handling vulnerabilities and managing life cycles and support.

5G Supply Chains Are Under Pressure, With Effects Being Felt Around the World

Who should care? **Manufacturers and sellers of network equipment and connected devices, internet and telecom service providers and operators.**

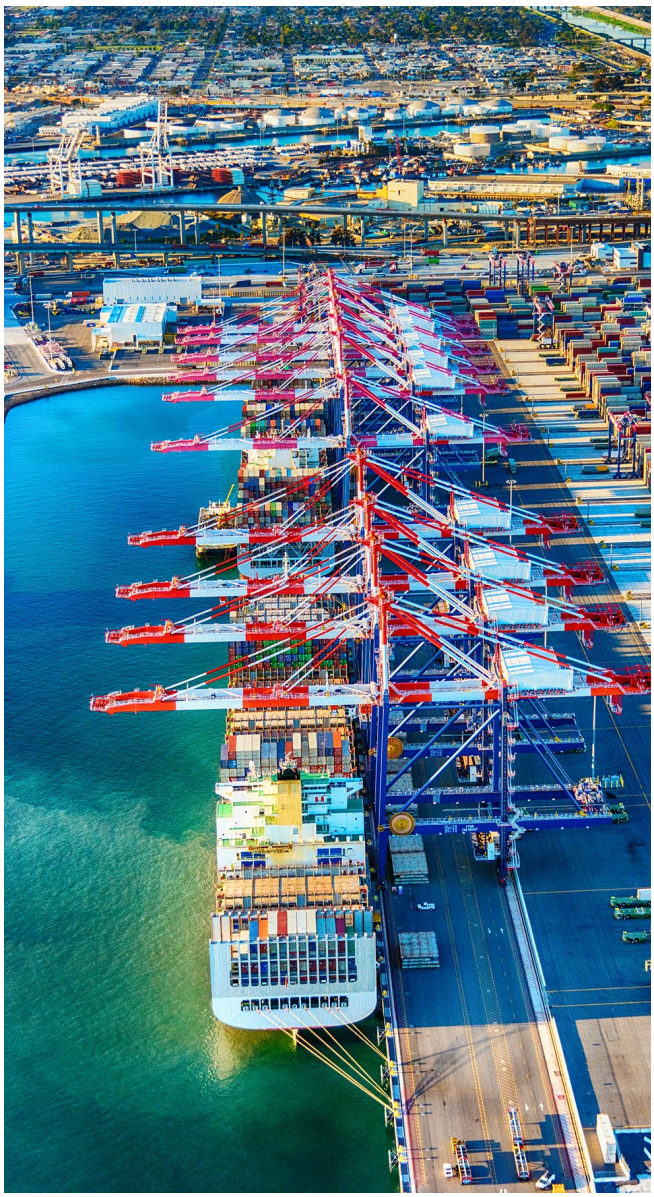
Who are the players? **U.S. Department of Homeland Security (DHS), Bureau of Industry and Security (BIS) at the Department of Commerce, NTIA, NIST, FCC, White House, DoD, and Congress.**

Supply chain integrity with respect to 5G has been a central issue for stakeholders including the White House, the Department of Commerce, the FCC, and Congress. Chinese equipment is a particular area of focus.

This concern has manifested itself across the federal government, including through:

President Trump's 2019 Supply Chain Executive Order, which targets Chinese companies and creates a new regulatory regime for review of certain transactions

- The Commerce Department's addition of Huawei to its Entity List
- The creation of the Federal Acquisition Security Council to help government agencies evaluate supplier security
- The FCC's proceeding to restrict the use of universal service funds by entities with equipment from certain Chinese manufacturers
- DHS work on a 5G security risk assessment, led by the National Risk Management Center (NRMC) in the Cybersecurity and Infrastructure Security Agency (CISA)
- DoD and Defense Innovation Board review of 5G ecosystem for risks and opportunities
- NIST has been looking at supply chain risk management in its Cybersecurity Framework
- An onslaught of federal legislative proposals



Engagement on these issues is advised to ensure that any new regulations or policies strike the proper balance between securing vital networks and enabling innovation.

Innovators Must Understand Equipment and Device Regulation

Who should care? **Manufacturers, importers, and marketers of RF-emitting equipment and connected devices.**

Who are the players? **FCC, Telecommunication Certification Bodies (TCBs)**

5G is poised to introduce a whole new ecosystem of innovative devices and specialized equipment to the market. These devices likely face an array of government requirements, including FCC regulations.

Navigating the FCC's equipment authorization process will be critical to anyone that designs, manufactures, markets, or imports 5G radio frequency devices. Devices that emit radio frequency (RF) radiation are subject to the equipment authorization procedures in the FCC's rules. Understanding the rules and considering them early in the design process can avoid delays in getting to the market and expensive fines if a device does not comply with the Commission's rules.

Any product that emits RF radiation is subject to the FCC's equipment authorization regime. In most cases, FCC equipment authorization must be obtained before an RF device may be marketed (i.e., sold, leased, advertised for sale or lease, or imported). The authorization procedure required may be a rigorous approval process known as certification or a less detailed process known as the Supplier's Declaration of Conformity. Many devices are subject to approval under both approaches. Regardless of the applicable authorization procedure, portable and mobile 5G devices will need to demonstrate compliance with the FCC's RF exposure limitations during testing.

In addition, the FCC's rules also specify detailed labeling and importation requirements. More broadly, non-RF environmental issues and product stewardship issues may be applicable to new 5G devices.

Sellers may also be impacted by federal laws and regulations regarding marketing of noncompliant or unauthorized equipment. The FCC's rules prohibit marketing a radio frequency device unless the device has received its relevant authorization(s). The FCC has brought numerous enforcement actions against individuals marketing unauthorized devices.

Because the FCC's equipment authorization rules are highly technical and can be difficult to apply, we urge entities to seek compliance advice from counsel. Failure to do so can be costly; the FCC has been vigilant in enforcing its equipment rules, levying significant fines against companies who violate the rules.

5G Is Driving Shifts in Government Procurement of Services and Products

Who should care? **Telecom and internet service providers and any contractors whose solutions for government purchasers involve telecom, connectivity, IT solutions, or mobile devices.**

Who are the players? **DoD, OMB, GSA, DHS, Department of Commerce, NIST, DOJ, ODNI.**

Governments around the world will play a role in 5G as market participants. They buy products and services. These activities offer promise and peril for companies in the 5G ecosystem.

Anyone that sells connected devices, IT services, or communications solutions to the United States government should familiarize themselves with a shifting array of obligations and expectations, many of which are focused on 5G. The Defense Department is developing a secure 5G mobile telecommunication network strategy and is developing a 5G requirement set that can shape procurements from ports or airfields or autonomous vehicles.

The United States has implemented several restrictions on telecommunications equipment due to security concerns about the global telecom supply chain. Anyone looking to sell to the government should be aware of these developments and anticipate increased scrutiny of perceived risks. For example:

- Section 889 of the National Defense Authorization Act for Fiscal Year 2019 prohibits U.S. government agencies from procuring or obtaining telecommunications equipment and services from certain Chinese technology companies. A series of restrictions are being developed to implement these and other emerging restrictions. Effective August 13, 2020, Section 889 will prohibit the government from awarding, extending, or renewing a contract to any entity that uses the prohibited technology as a substantial or essential component of, or critical technology to, any system. This additional prohibition will apply to systems that are not used in performance of a government contract.
- Congress established an interagency Federal Acquisition Supply Chain Security Council to assess and mitigate supply chain risks government wide and establish criteria and procedures for exclusion or removal of specific sources of supply for civilian agencies, defense agencies, and/or intelligence community agencies. Congress previously authorized Department of Defense agencies to exclude companies from a procurement competition for a national security system based on the Under Secretary of Defense for Intelligence's assessment of significant supply chain risk.

The Government Is Embarking on Substantial 5G Research and Development Spending

Who should care? **Manufacturers and sellers of network equipment and connected devices, internet and telecom service providers and operators.**

Who are the players? **DoD, NIST, NCCoE, DHS, and others.**

5G also presents opportunities. Currently, the U.S. government is using various non-procurement vehicles to fund 5G research and development (R&D) efforts. These efforts can take many forms, including cooperative agreements, other transaction authorities (OTAs), and cooperative research and development agreements (CRADAs), among others. The White House Office of Science and Technology Policy (OSTP), with the Wireless Spectrum R&D (WSRD) Interagency Working Group, has issued reports on *Research and Development Priorities for American Leadership in Wireless Communications*. OSTP simultaneously released a report on *Emerging Technologies and Their Expected Impact on Non-Federal Spectrum Demand*.

A flurry of activity is underway. For example:

- The Department of Defense is engaging with industry on large-scale experimentation and prototyping of 5G technologies at military installations.
- The National Spectrum Consortium engages in R&D to develop prototypes that support the implementation of 5G, 5G-based technologies, and spectrum awareness, sharing, and use.
- The National Science Foundation, through a public-private partnership, is testing 5G platforms as part of a broader 5G development effort.
- The Defense Advanced Research Projects Agency (DARPA) is using "challenges," a unique method of procurement, to overcome spectrum scarcity—a major issue that will impact the development of 5G networks.
- DHS has announced plans to make 5G-related research grants and pursue partnerships as well.

From a policy perspective, multiple research efforts may overlap or duplicate each other, thereby being less efficient. Some projects identified by government agencies may focus on the wrong use cases or priorities.

From a risk perspective, private-sector participants in government research and development need to consider the obligations that accompany federal research dollars.

Grants are one of the primary ways that the government funds projects. Grants are a significant source of funding for many nonprofit organizations, colleges and universities, research institutions, and for-profit companies, including "traditional" government contractors. Like government contracts, grants are subject to a host of regulatory requirements and compliance obligations, and grant recipients often become the targets of government audits, investigations, and enforcement actions. Participants in government-sponsored research also need to take steps to appropriately protect their intellectual property rights under grant awards, cooperative agreements, and other alternative procurement vehicles.

Many U.S. allies are pursuing similar 5G research efforts, though companies wishing to participate should be aware of additional considerations if they are using foreign assistance to fund 5G research and development efforts.

Law Enforcement and Civil Demands for Electronic Information Require Preparation

Who should care? **Manufacturers and sellers of connected devices, applications, and software; internet and telecom service providers; enterprises and end users who will depend on secure connectivity for data.**

Who are the players? **Federal, state, and local law enforcement agencies.**

5G and the IoT will have implications for access to electronic evidence by law enforcement and others. Vast amounts of personal and business data can be collected and stored by companies through IoT devices, and the government has noticed. We anticipate that law enforcement will follow the data, causing a major shift for companies that previously had minimal contact with criminal investigators.

As the IoT device market develops, companies can expect their relationships with consumers, the public, and law enforcement to become more complicated. Expectations may shift about the collection and availability of data, such that companies accessing or keeping data should be consider how to handle law enforcement and civil litigation requests for electronic evidence.

By way of background, federal, state, and local agencies have the legal authority to intercept and access communications and information pursuant to court orders. But agencies often lack the technical capability to carry out those orders due to the evolution of technology and communications services. The FBI calls this "Going Dark." Policymakers have identified

5G deployment, the move to edge compute power, and the explosion of IoT as exacerbating national security concerns related to "Going Dark."

The FBI and the U.S. Department of Justice have said that investigative agencies face two distinct challenges: (1) real-time court-ordered interception of data in motion, such as phone calls, e-mail, text messages, and chat sessions; and (2) "data at rest"—court-ordered access to data stored on devices, such as e-mail, text messages, photos, and videos. We anticipate that 5G developers will be called upon to support the technical collection efforts of U.S. law enforcement and that the U.S. government may pursue significant regulation to support law enforcement's collection capabilities.

A 2016 Harvard Berkman Center ***report on "Going Dark"*** observed that "the prevalence of network sensors and the Internet of Things raises new and difficult questions about privacy over the long term. This means we should be thinking now about the responsibilities of companies building new technologies, and about new operational procedures and rules to help the law enforcement and intelligence communities navigate the thicket of issues that will surely accompany these trends."[4]

Manufacturers, application developers, service providers, and users of 5G-enabled services should consider their posture with respect to law enforcement requests and demands for electronic evidence.

---

[1] Ericsson, The Industry Impacts of 5G, https://www.ericsson.com/en/networks/trending/insights-and-reports/industry-business impact-of-5g.

[2] American Express, 5G Wireless Technology to Fuel Global Supply Chain Innovation, https://www.americanexpress.com/us/foreign- exchange/articles/5G-supply-chain-technology/.

[3] CTIA, The Race to 5G, https://www.ctia.org/the-wireless-industry/the-race-to-5g.

[4] Harvard Berkman Center, Don't Panic. https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_ Going_Dark_Debate.pdf

Wiley's 5G Team

Wiley has been helping businesses prepare for a 5G future by securing and managing spectrum access, assessing national security risks, shepherding technology investments and transactions, and working on global standards and regulation. Our team handles equipment authorization and regulation facing manufacturers and sellers. We litigate and advise on barriers to infrastructure deployment. We break down regulatory barriers to UAVs, autonomous vehicles, and the IoT generally. We help companies and industries partner with government on research and development. Our team educates regulators, policymakers in Congress and the Executive Branch about the future of 5G and beyond. We draw from many parts of the firm and our ranks include engineering expertise and numerous former senior government officials who drive results. A few of our team members are identified below:

Megan L. Brown
mbrown@wiley.law
202.719.7579
cyber, privacy, national security, supply chain

Scott D. Delacourt
sdelacourt@wiley.law
202.719.7459
spectrum and licensing

David A. Gross
dgross@wiley.law
202.719.7414
cyber, international, privacy, national security, supply chain

Tracye Winfrey Howard
twhoward@wiley.law
202.719.7452
national security and procurement issues

Antonio J. Reynolds
areynolds@wiley.law
202.719.4603
privacy, security, emerging tech

Jacquelynn Ruff
jruff@wiley.law
202.719.3347
spectrum, international

Meredith G. Singer
msinger@wiley.law
202.719.7507
spectrum and licensing, equipment regulation

Joshua S. Turner
jturner@wiley.law
202.719.4807
infrastructure

Brian Walsh
bwalsh@wiley.law
202.719.7469
procurement issues, research grants

wiley.law