

NTIA Rulemaking Seeks Comments on Government Role in IoT

By Aimee Ghosh, Sheila Harvey, Glenn Richards and Brian Wong

The National Telecommunications and Information Administration (NTIA), part of the Department of Commerce, is seeking public comment on the benefits, challenges and potential roles for the government in fostering the advancement of the Internet of Things (IoT). According to NTIA, the Internet of Things describes the connection of physical objects, infrastructure and environments to various identifiers, sensors, networks and/or computing capability. Today, there are an estimated 25 billion connected devices, including connected cars and medical devices, as well as smart cities, refrigerators and heating systems.

While IoT is expected to have an immense impact on the global economy (between \$3.9 and \$11 trillion by 2025), it also presents health, safety and policy concerns for government agencies that have traditional regulatory oversight over the connected devices—such as the Food and Drug Administration (implantable medical devices) and the Department of Transportation (connected cars). To date, according to NTIA, no U.S. government agency has taken a holistic view of IoT that identifies the opportunities and assesses risks. At the same time, other national governments, standards organizations and intergovernmental organization are looking at IoT, creating the possibility of a patchwork of approaches that could increase cost and deter investment.

Businesses participating in the IoT ecosystem would be well-advised to monitor (or participate in) this proceeding, and they can also expect that other federal agencies (and possibly state legislatures and agencies) may begin staking claims to jurisdiction over IoT applications and services. For example, will there be different privacy policies related to information gathering and sharing for smart cities, smart homes and smart cars? What obligations will service providers have in case of data breaches or to share information with law enforcement? What security requirements will be imposed on the manufacturers of wireless industrial devices? Will obligations reflect varying resource levels and risk tolerances of businesses of different sizes and in different industries? Will there be specific restriction or rules and regulations for service providers located outside the United States? Will U.S. policies align with those adopted in other countries or by international standards bodies to provide seamless operations for IoT service providers and developers?

To further its understanding of IoT issues, NTIA is seeking comments on a wide range of issues, including:

1. Are the challenges and opportunities arising from IoT similar to those that governments and societies have previously addressed with existing technologies, or are they different, and if so, how?
2. What definition(s) should we use in examining the IoT landscape, and why?
3. Are there current or planned laws, regulations or policies that foster IoT development or unnecessarily inhibit IoT development?
4. Are there ways to classify the IoT landscape to improve how public policy issues are discussed?
5. What technological issues may hinder the development of IoT?
6. What can government do, if anything, to mitigate technical issues?
7. How will IoT place demands on existing infrastructure architectures, business models or stability?
8. Should the government quantify and measure the IoT sector or economic impact of IoT?
9. How should the government address cybersecurity and privacy concerns about IoT? Are there other consumer protection issues raised by IoT?
10. How should the U.S. government engage with international governments and organizations that are exploring standards, specifications and best practices for IoT?
11. How should government and the private sector collaborate to ensure that infrastructure, policy, technology and investment are working together to best fuel IoT growth and development?

After analyzing the comments, the Department intends to issue a “green paper” that identifies key issues impacting deployment of these technologies, highlights potential benefits and challenges, and identifies possible roles for the federal government in fostering the advancement of IoT technologies in partnership with the private sector.

Comments in this proceeding are due on or before 5 p.m., Eastern Time, on May 23, 2016. Feel free to contact any of the attorneys listed on this Client Alert if you have questions or seek assistance filing comments.

If you have any questions about the content of this alert please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Aimee P. Ghosh [\(bio\)](#)
Washington, DC
+1.202.663.8091
aimee.ghosh@pillsburylaw.com

Sheila McCafferty Harvey [\(bio\)](#)
Washington, DC
+1.202.663.8224
sheila.harvey@pillsburylaw.com

Glenn S. Richards [\(bio\)](#)
Washington, DC
+1.202.663.8215
glenn.richards@pillsburylaw.com

Brian M. Wong [\(bio\)](#)
San Francisco
+1.415.983.6372
brian.wong@pillsburylaw.com

Pillsbury Winthrop Shaw Pittman LLP is a leading international law firm with 18 offices around the world and a particular focus on the energy & natural resources, financial services, real estate & construction, and technology sectors. Recognized by *Financial Times* as one of the most innovative law firms, Pillsbury and its lawyers are highly regarded for their forward-thinking approach, their enthusiasm for collaborating across disciplines and their unsurpassed commercial awareness.

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.

© 2016 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.