POLICY AND REGULATORY ISSUES

Policymakers face a conundrum – promoting the adoption of IoT services to reap its many benefits, while safeguarding societal concerns. This will be a balancing act of oversight and regulation from policymakers to drive investment and consumer adoption while ensuring that safety, security, and privacy frameworks are in place. This column will explore critical national and international IoT policy and regulatory efforts as well as take a deeper dive into specific topics of interest.

Introduction

Douglas C. Sicker

Policymakers face a conundrum: promoting the adoption of IoT services to reap its many benefits, while safeguarding societal concerns. This will be a balancing act of oversight and regulation from policymakers to drive investment and consumer adoption while ensuring that safety, security, and privacy frameworks are in place. Meanwhile, industry must step up to lead and adopt best practices and standards, which will allow policymakers to forbear as appropriate.

In this inaugural issue of *IEEE Internet of Things Magazine* (IoTM), we are fortunate to have the Assistant Secretary of Commerce and Administrator of the National Telecommunications and Information Administration (NTIA), David Redl, as our first contributor to this Regulatory and Policy Column, discussing key findings of NTIA's recent green paper on IoT. In future issues, we will explore critical IoT policy and regulatory issues being considered in other parts of the world as well as take a deeper dive into specific topics of interest. It is difficult to overstate the impact that IoT will have on our society; therefore, getting the policy and regulatory issues right is critical because the policies will guide the ultimate success and direction of this important digital evolution. The breadth and depth of policy and regulatory issues facing IoT are surprisingly vast, ranging from safety, privacy, security and spectrum policies to issues of infrastructure coordination, rights of way and acceptable use.

Perspectives on IoT Policy from the U.S. NTIA

by David J. Redl

Assistant Secretary for Communications and Information and Administrator, National Telecommunications and Information Administration, U.S. Department of Commerce

The Internet of Things (IoT) is not the future — it is the present. From smart home devices that open blinds, brew coffee, and turn on the news in the morning to industrial applications revolutionizing supply chain management, connected devices are changing how we live, work, and play.

At the National Telecommunications and Information Administration (NTIA), we understand the potential benefits of IoT and are dedicated to ensuring that we have the policies and infrastructure in place to support the innovation behind these advances. In depth technical understanding is vital to well-run policy making processes, and it is equally important for the technical community to grapple with the wider impacts of its work. *IEEE IoT Magazine* is therefore a welcome addition to the conversation, and I appreciate the opportunity to contribute to the inaugural edition.

NTIA is the Executive Branch agency located within the U.S. Department of Commerce that is principally responsible for advising the President on telecommunications and information policy issues. NTIA's programs and policymaking focus largely on expanding broadband Internet access and deployment in America, increasing the use of spectrum by all users, and ensuring that the Internet remains an engine for continued innovation and economic growth. This broad mandate includes emerging technologies, such as those powering IoT. Within the Administration's interagency processes, NTIA is a primary voice at the table focused on innovation and economic growth.

Neither the fundamental technologies nor the policy challenges of IoT are novel. IoT differs in the sheer number of devices that will be connected to the Internet and to each other, the variety of industries that are newly integrating connectivity into their products and business processes, and the increased stakes in the benefits and the risks. In other words, IoT brings new challenges to ongoing and longstanding policy debates. For example, IoT raises particular cybersecurity challenges, but it would be counter-productive to consider them outside of the context of broader cybersecurity conversations or to reinvent the wheel where progress has been made elsewhere.

This insight is reflected in the policy paper titled *Fostering the Advancement of the Internet of Things* (**https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf**) that was released by the Department of Commerce's Internet Policy Task Force. Informed by public comments from industry, academia, civil society, individuals and a public workshop, the paper concludes that the United States' policy approach that helped lead to the global success of the Internet continues to be the best way to respond to innovative technologies. It also lays out the following four areas that could help guide the Department's efforts to encourage IoT growth and innovation in a manner that is inclusive and widely accessible, and is within a stable, secure and trustworthy environment:

Enabling Infrastructure Availability and Access: IoT only works so long as there is connectivity, and that connectivity is dependent upon telecommunications infrastructure, both wireline and wireless. NTIA plays important roles, as our Office of Telecommunications and Information Applications works to ensure that unserved communities gain access to the broadband connectivity necessary for IoT applications, and our Office of Spectrum Management both manages Federal spectrum resources and works with the Federal Communications Commission to identify additional spectrum for commercial use. Our contribution to wireless connectivity also includes the work of the Institute for Telecommunication Sciences (ITS), NTIA's research lab, which is exploring what the real spectrum needs are going to be with the onset of IoT. These efforts put us at the forefront of working to help enable access to robust and innovative IoT solutions for everyone.

Crafting Balanced Policy and Building Coalitions: The advancement and adoption of IoT will also be affected by the policies that are in place to help encourage trust while safeguarding innovation. This will require close collaboration across the government with industry and civil society to take on issues, such as privacy, cybersecurity, and intellectual property, among others, that will shape the IoT ecosystem. The United States has a successful track record in achieving this balance, but it will take dedication and cooperation across sectors to ensure

Editor's Note: Text appearing in bold indicates a live link in the online version.

that this continues for IoT and other emerging technologies. NTIA's Office of Policy Analysis and Development and Office of International Affairs are key players in helping to shape these policies.

Promoting Standards and Technology Advancement: The Department of Commerce, through ITS and the National Institute of Science and Technology (NIST), is committed to ensuring that the necessary technical standards are developed and in place to support global IoT interoperability, and that the technical applications and devices to support IoT continue to advance. We remain steadfast in our support of industry-driven, consensus-based, voluntary, global standards. NTIA helps support these efforts in a number of international organizations.

Encouraging Markets: Finally, the Department of Commerce is working to promote IoT through the use of its own IoT devices, iterative enhancement, and novel deployment of the technologies. We will also be working with our global partners to help translate the economic benefits and opportunities of IoT, expanding the market not only domestically but worldwide.

To show how this work is being translated into practice, I want to spend some time drilling down into how NTIA is approaching what commenters on our report cited most frequently as a challenge to the advancement of IoT: cybersecurity. NTIA is taking a multipronged approach to addressing cybersecurity concerns, takings steps to work with stakeholders and within the government to craft balanced solutions that can affect real-world change.

First, NTIA has convened cybersecurity multi-stakeholder processes that have brought together representatives of industry, civil society, academia and the security research community to tackle difficult policy issues. The second of these processes focused on patching and upgrading IoT devices to limit vulnerabilities. This process resulted in three finished work products — a guide for consumers, a technical breakdown of the patching process and a discussion of incentives and barriers to patching — as well as a compendium of standards and best practices, which will be maintained as a living document. These documents, as well as more information about our processes, can be found on our website here: **https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security**.

NTIA has also worked closely with NIST and with the Department of Homeland Security to produce a report on how to combat distributed threats on the Internet, which can be found here: **https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets**. This report benefited greatly from stakeholder input through both comments and a workshop and lays out actionable steps that can be taken to address this abuse of Internet-connected devices.

NTIA is further engaged at the international level on developing cybersecurity policies, working in forums such as the International Telecommunications Union, the Organization for Economic Co-operation and Development, and the Internet Governance Forum. We engage as well on the bilateral and regional level, representing U.S. positions and promoting dialogue. We actively support NIST's Global Cities Challenge work, which has this year added consideration of cybersecurity issues that smart cities face.

While I highlight cybersecurity, this is only one aspect of IoT in which NTIA is engaged. All of our diverse efforts are predicated on stakeholder engagement and reliance on the expertise of practitioners. So we want to hear from you about the challenges that you face and your thoughts on potential solutions. It is only through your active participation and sharing of knowledge that we will be able to craft the informed policy solutions that a vibrant IoT ecosystem requires. NTIA is excited to work with you to ensure that IoT continues to fulfill its extraordinary potential.

David J. Redl was sworn in as Assistant Secretary for Communications and Information at the Department of Commerce in November 2017. He serves as Administrator of the National Telecommunications and Information Administration (NTIA), the Executive Branch agency that is principally responsible for advising the President on telecommunications and information policy. He is a lawyer and communications policy expert with more than a decade of experience in government and the private sector. He was previously the chief counsel at the U.S. House of Representatives Committee on Energy and Commerce. In that role, he served as principal legal advisor to the chairman and members of the Energy and Commerce majority on communications and technology matters. Prior to his time with the committee, he was director of regulatory affairs at CTIA, a trade association that represents the U.S. wireless communications industry. He earned his J.D. from the Catholic University of America with a certificate from the Institute for Communications Law Studies, and he is a graduate of Pennsylvania State University with degrees in journalism and political science. He is admitted to the New York and District of Columbia bars. He lives in Falls Church, Virginia, with his wife, Amy, and their son, Benjamin.

Douglas C. Sicker (sicker@cmu.edu) is currently the Lord Endowed Chair in Engineering, department head of Engineering and Public Policy, director of CyLab Security and Privacy Institute, and a professor of engineering and public policy with a joint appointment in the School of Computer Science and courtesy appointment in the Heinz College at Carnegie Mellon University. He is also the Executive Director of the Broadband Internet Technical Advisory Group (BITAG). Previously, he was the DBC Endowed Professor in the Department of Computer Science at the University of Colorado at Boulder with a joint appointment in, and directorship of, the Interdisciplinary Telecommunications Program. He recently served as the chief technology officer and senior advisor for Spectrum at the National Telecommunications and Information Administration (NTIA). He also served as the chief technology officer of the Federal Communications Commission (FCC), and prior to that he served as a senior advisor on the FCC National Broadband Plan. Earlier he was director of Global Architecture at Level 3 Communications, Inc. In the late 1990s, he served as Chief of the Network Technology Division at the FCC. He is an active member of ACM, AAAS, and the Internet Society. He has served as an advisor to the Department of Justice, the Federal Trade Commission, the FCC, and the Department of State; the Chair of the FCC Network Reliability and Interoperability Council steering committee; an advisor on the Technical Advisory Council of the FCC, and chair of a recent National Academy study on the Boulder Department of Commerce Laboratories. He has chaired numerous conferences as well as served on many program committees and several National Academy studies. He has published extensively in the fields of wireless systems, network security, and network policy, and has received funding from NSF, DARPA, FAA, Cisco, Intel, IBM, and other sources.