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
Column Editor

In this Policy and Regulatory Issues column, Professors Berges and Samaras suggest a strategy to help answer two important questions: What would we later regret not regulating now? What good opportunities might certain types of regulation hold back and how can this be mitigated? In answering these questions, they suggest a human-centered utility-like approach to some of the bigger issues facing the deployment of IoT.

A Path Forward for Smart Cities and IoT Devices

by Mario Bergés and Constantine Samaras
Carnegie Mellon University

Abstract

Global urbanization projections suggest that a great majority of human beings will be living in urban areas by the middle of this century. This trend imposes significant strains on urban infrastructure systems and adds additional challenges to achieving environmental, social and economic sustainability goals set by many city governments. Smart city products and services, backed by IoT systems, have been proposed as effective solutions to increase efficiency, reduce costs and improve services. However, as with any technology, IoT solutions for smart cities bring about great opportunities and, at the same time, threats to, among others, governance, security, privacy and community autonomy. As we accumulate experience with these smart city deployments, we must ask ourselves: What would we later regret not regulating now? What good opportunities might certain types of regulation hold back and how can this be mitigated? We offer our perspective on these questions and argue in favor of human-centered IoT systems that are owned, operated and managed much in the same way that other public urban infrastructure systems (e.g., wastewater) are.

Introduction

Increased urbanization throughout the world is one of the defining trends of this century. More than 55 percent of the world's population currently live in urban areas, and forecasts project that this will increase to 68 percent by 2050, adding another 2.5 billion people [1]. Along with this urbanization, digital technologies have proliferated at an exponential rate over the last few decades, quickly becoming a critical intermediator for a wide variety of transactions and exchanges that enable daily life. Already, tens of billions of sensors and actuators that make up the so-called Internet of Things (IoT) landscape have been deployed around the world's urban areas [2], a trend that continues to grow exponentially. These devices can provide real-time information at fine resolutions across a range of applications, which will change how residents experience and interact with cities. The deployment of IoT devices can transform communities and, along the way, introduce new opportunities and threats regarding economic, social, security, and sustainability outcomes. As we accumulate experience addressing these issues, we need policies to ensure that the IoT infrastructure system furthers humanity's needs and aspirations in an urbanizing world.

IoT Devices and Smart Cities

Rapidly growing cities amplify familiar challenges for city managers and residents – concerns about transportation, pollution, food, water, energy, infrastructure, safety, and emergency response, among many other challenges. Cities today are responsible for more than 75 percent of energy-related greenhouse gas (GHG) emissions worldwide [3], and they face a range of new challenges to remain resilient under global climate change. At the same time, social inequality has remained stagnant and may become higher [4], undermining sustainability efforts [5]. City stakeholders and policymakers are thus searching for opportunities to leverage technology to improve the quality of life of their residents, and the promise of IoT devices has featured prominently in discussions around smart cities.

The unprecedented and widespread availability of Information and Communication Technologies (ICT), largely driven by IoT deployments and digitized information, open up new territories in the space of solutions for increasing efficiency, modernizing government services and maintenance, combating climate change and inequality, as well as for improving urban sustainability. The public's view of IoT devices is likely through smart appliances and other consumer products in their home. But IoT devices are also embedded in traffic signals, communication networks, power and water systems, building systems, and other infrastructure that enables urban life. For example, high resolution, connected utility meters (a type of IoT device) enable real-time monitoring and optimization of building energy and mechanical systems. This not only saves costs for building owners, but can enable cost, energy, and GHG savings across an urban system. Similarly, there are tremendous opportunities enabled due to the granular and high-resolution sensing and actuation capabilities brought about by other IoT devices installed in roadways (e.g. traffic cameras, road lighting, structural health monitoring sensors), water, gas, and power distribution systems, food systems, and other enabling infrastructure. IoT devices will also be embedded in new forms of transport and logistics, from connected and automated passenger, transit, and freight vehicles, to package delivery drones and sidewalk droids. All of these devices will collect information about the urban environment that could be used by both public and private stakeholders.

Challenges in IoT Deployment

Yet, experience with IoT solutions deployed in urban systems suggests that they have some considerable practical shortcomings. These include large human capital investments for installation and sustainment, and a reliance on a centralized system architecture that can sometimes hinder their scalability [6]. Moreover, simply deploying connected and autonomous devices without appropriate testing, systems considerations, and cybersecurity safeguards could lead to unintended consequences that would increase risk and life-cycle costs [7]. Furthermore, IoT device deployments are often deployed by private actors, but since these solutions affect the public realm, ensuring and maintaining accountability remains a challenge, and there are societal costs that need to be weighed against their benefits.

The potential benefits of smart cities with near ubiquitous IoT devices will not be realized without the willing support and trust of city residents. A noteworthy example is Sidewalk Labs' project (https://sidewalktoronto.ca) to create an Internet city from the ground up in the city of Toronto, Canada. Though it promises enormous economic opportunities and sustainability achievements, the effort was met with skepticism by many residents due to, among other things, a lack of opportunities for public input on the project, as evidenced in recent community demonstrations against these projects [8]. Furthermore, it is necessary to align commercial interests and governance methods for these IoT-enabled autonomous systems with urban sustainability goals [9], which requires redesigning incentives to encourage positive environmental and social outcomes.

Aligning Incentives

While consumers seem ever-willing to yield privacy in exchange for services, the privacy issues around IoT devices remain largely unaddressed. Caron *et al*. [10] outlined four areas of privacy concerns from IoT proliferation: unauthorized surveillance, uncontrolled data generation and use, inadequate authentication, and information security risks. Every IoT device is a portal between the physical environment around it, and the digital environment (the Internet), through which an agent on one side can effectively monitor and potentially control the other. However, this portal exhibits inherent asymmetries: information moving from the physical to the digital world is only constrained by digital rules (software), whereas information traveling the other way faces stricter, physical constraints. Hence, it is much easier to design an IoT device with a limited scope of action or measurement in the physical world (e.g., limited field of view for a smart doorbell camera), than it is to design one that limits the actions and measurements in the digital environment (e.g., implementing access control policies). Physical laws are immutable, while digital rules are not.

Similarly, measurement and control capabilities provided by these IoT devices can be asymmetrically distributed between users and providers of IoT solutions, largely due to the fact that most of these solutions are currently sold as services. In other words, while customers may purchase a smart thermostat or a smart speaker today, and own the device, its functionality will be severely limited unless it is provisioned with the vendor's services over the Internet. Thus, users control only the physical scope of action/measurement of their IoT devices, while vendors control the digital scope of action/measurement for all of their IoT devices. Though there are technical solutions to reduce these asymmetries (e.g., decentralized network architectures, differential privacy techniques and federated learning algorithms), policies to regulate the digital domain, in our opinion, are still required and are a more effective solution. In particular, in light of these asymmetries and the pace at which these IoT solutions are populating our built environment, we need to ask ourselves: What would we later regret not regulating now? What good opportunities might certain types of regulation hold back and how can this be mitigated? In 2013, the authors in [11] posited that policymakers should develop an environment where IoT is accountable, competitive, ethical, inclusive, interoperable, open and safe. As the year 2020 approaches, these goals remain elusive and performance metrics are largely undefined.

A Path Forward

To make progress on these issues, we might consider the set of IoT devices in an urban area as its own infrastructure system. Just like other infrastructure systems (e.g., the wastewater system), this one consists of the devices and algorithms themselves, the means of collecting, analyzing, and acting on the data collected, and any enabling sustainment systems to monitor performance and replace devices as needed. This IoT infrastructure system to-date has been largely private, established by independent and often competing entities. And just like other private and public infrastructure systems, this new infrastructure system could have well-defined responsibilities, standards, and protocols. There are lessons to be learned from the evolution of the Internet, with its set of regulating institutions, for the continued evolution and proliferation of IoT devices [12]. But beyond ensuring that the IoT infrastructure system has better defined boundaries and responsibility assignments, we must also confront issues regarding ownership and distribution of the raw material this system processes: data and metadata about cities and residents. At the moment these are valued and regulated much like natural resources were at the dawn of the industrial revolution [13]. We likely need to create market structures, incentives, and regulations to encourage the positive aspects while safeguarding public welfare. High-profile examples of bad outcomes might limit the potential good outcomes if not properly addressed.

Maximizing the opportunities with IoT devices requires a complete paradigm-shift in the way we design, test and deploy ICT if we are to balance the goals of autonomy, resilience, sustainability and community governance. This could take the form of an IoT Public Utility Commission, be based off of governmental, non-governmental and private entities structures that underpin the Internet, or a hybrid. If cities want to deploy IoT infrastructure, the city should be able to do so independently with interoperable and open components, so that today's choices do not constrain future stakeholders. What is clear is that a human-centered IoT infrastructure system is needed, and much work remains to make this a reality.

Acknowledgments

This work was supported in part by the National Science Foundation, Awards CNS-1929937 and EEC-1937103, as well as the U.S. Department of Energy, Award DE-EE0008463. The opinions expressed do not represent the views of any organization.

References

[1] UN, "2018 Revision of World Urbanization Prospects," United Nations Department of Economic and Social Affairs, Tech. Rep., 2018, https://population.un.org/wup/Publications/Files/WUP2018Report.pdf.

[2] R. Bogue, "Towards the Trillion Sensors Market," *Sensor Review*, vol. 34, no. 2, 2014, pp. 137–42.

[3] IPCC, *Climate Change 2014: Mitigation of Climate Change (Vol. 3)*, O. Edenhofer, Ed. Cambridge University Press, 2019.

[4] B. Milanovic, "Global Inequality Recalculated and Updated: The Effect of New PPP Estimates on Global Inequality and 2005 Estimates," *J. Economic Inequality*, vol. 10, no. 1, 2012, pp. 1–18.

[5] The National Academies, *Pathways to Urban Sustainability: Challenges and Opportunities for the United States*, National Academies Press, 2016.

[6] W. van Winden and D. van den Buuse, "Smart City Pilot Projects: Exploring the Dimensions and Conditions of Scaling Up," *J. Urban Technology*, vol. 24, no. 4, pp. 51–72, 2017, https://doi.org/10.1080/10630732.2017.1348884.

[7] The National Academies, *Autonomy Research for Civil Aviation: Toward a New Era of Flight*, National Academies Press, 2014.

[8] "The Google City That Has Angered Toronto," https://www.bbc.com/news/technology-47815344, accessed: 201905-29.

[9] T. Yigitcanlar *et al.*, "Can Cities Become Smart Without Being Sustainable? A Systematic Review of the Literature," *Sustainable Cities and Society*, vol. 45, pp. 348–65, 2019, http://www.sciencedirect.com/science/article/pii/S221067071831268X.

[10] X. Caron *et al.*, "The Internet of Things (IoT) and Its Impact on Individual Privacy: An Australian Perspective," *Computer Law Security Review*, vol. 32, no. 1, pp. 4–15, 2016, http://www.sciencedirect.com/science/article/pii/S0267364915001661.

[11] H. R. Schindler *et al.*, "Europe's Policy Options for a Dynamic and Trustworthy Development of the Internet of Things: Smart 2012/0053," RAND Corporation, 2013, https://www.rand.org/pubs/researchreports/RR356.html

[12] R. H. Weber, "Internet of Things Need for a New Legal Environment?" *Computer Law Security Review*, vol. 25, no. 6, pp. 522–27, 2009, http://www.sciencedirect.com/science/article/pii/S0267364909001514.
[13] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for A Human Future at the New Frontier of Power*, Profile Books, 2019.

Mario Bergés is a Professor in the Department of Civil and Environmental Engineering at Carnegie Mellon University (CMU). He is interested in making our built environment more operationally efficient and robust through the use of information and communication technologies, so that it can better deal with future resource constraints and a changing environment. He has led multiple research projects on a wide range of problems related to sensing and data analysis for civil infrastructure systems, particularly in the area of buildings and energy efficiency, with funding from federal agencies (e.g., DOE, NSF, NASA), industry (e.g., Bosch, HP Labs, Samsung) and other sources. He is the faculty director of the Smart Infrastructure Institute at CMU and the Intelligent Infrastructure Research Lab (INFERLab). Among recent awards, he received the Professor of the Year Award by the ASCE Pittsburgh Chapter in 2018, the Outstanding Early Career Researcher award from FIATECH in 2010, and the Dean's Early Career Fellowship from CMU in 2015. He received his B.Sc. in 2004 from the Instituto Tecnológico de Santo Domingo, in the Dominican Republic; and his M.Sc. and Ph.D. in Civil and Environmental Engineering in 2007 and 2010, respectively, both from Carnegie Mellon University.

Constantine Samaras is an Associate Professor in the Department of Civil and Environmental Engineering at Carnegie Mellon University. His research spans energy, vehicle automation, resilience, and defense analysis, and he directs the Center for Engineering and Resilience for Climate Adaptation. He has published studies examining electric and autonomous ground and air vehicles, is a Fellow in Carnegie Mellon's Scott Institute for Energy Innovation, and is an affiliated faculty member in the Traffic21 Research Center. He received the Professor of the Year Award by the ASCE Pittsburgh Chapter in 2019, and the Dean's Early Career Fellowship from CMU in 2018. He is also an Adjunct Senior Researcher at the RAND Corporation. From 2009 to 2014 he was a researcher at the RAND Corporation and from 1999 to 2004 he was megaprojects engineer in New York. He received a joint Ph.D. in Civil and Environmental Engineering and Engineering and Public Policy from Carnegie Mellon, a M.P.A. in Public Policy from New York University, and a B.S. in Civil Engineering from Bucknell University.

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.