

# Policy Implications of the Internet of Things

August 25, 2015 (IN10345)

---

-|

---

-|

---

Linda K. Moore, Specialist in Telecommunications Policy ([lmoore@crs.loc.gov](mailto:lmoore@crs.loc.gov), 7-5853)

---

The [Internet of Things](#) (IoT) is an umbrella term that many policymakers use to refer to the technologies and network structures that interconnect objects, humans, and animals to collect and analyze data and manage processes. IoT appears poised to revolutionize every sector of the economy, creating new business models for every industry, and significantly altering how society and government function. In a June 2015 [report](#), McKinsey Global Institute refers to "the transformative potential for many types of participants and stakeholders" of IoT. In its many manifestations, IoT also has the potential to be an important tool in addressing difficult policy issues of the future, such as [urban congestion](#) and [water resource](#) management.

The [Internet of Everything](#) is a more expansive description that encompasses the vast reach of connected technologies such as integrated sensors, optical recognition, spatial awareness, and cognitive computing, as well as disciplines such as [Cyber-Physical Systems](#) engineering. "Everything" also might describe the vast number of markets and applications and the implications for government agencies at all levels. Policy considerations in areas such as farming, education, transportation, urban planning, and health are similarly numerous. Many departments and agencies of the executive branch—including independent agencies such as the Federal Communications Commission—have or will have regulatory jurisdiction or obligations for some piece within this vast net and will be expected to evolve with the Internet of Things.

## Policy Considerations

Examples of the policy areas in which Congress may have to weigh positive benefits and negative consequences of IoT are:

- *Cybersecurity*: such as balancing privacy rights with data security requirements.
- *Communications*: such as assuring market competition while providing access to spectrum that encourages innovation from new entrants or meets non-commercial social goals, such as public safety.
- *Investment in Infrastructure*: such as identifying public sector and commercial strategies to encourage investment in long-term projects with diversely distributed benefits.
- *Employment and training*: such as anticipating the new skills needed to further the Internet of Things and preparing to offset potential job loss from shifts in employment needs.

These policy considerations touch consumer issues, social change, and industry. The [Industrial Internet](#) is often used to describe the integration of complex physical machinery with networked sensors and software for industrial purposes such as manufacturing, maintenance, and product design. Many of the advances in the Industrial Internet will have significant impacts on consumers, for example through better engineering that leads to lower-cost and safer products, and also in the building of [Smart Cities](#). Smart cities integrate IoT technologies into city management for purposes such as improving services, reducing costs, or enhancing the community.

Economic theory is also likely to evolve as the technology becomes more prevalent. For example, IoT is enabling what is often referred to as the [sharing economy](#). [Theories](#) developed to explain the underpinnings of a sharing economy will likely migrate to economic theories and policies in other areas, such as employment, housing, investment, pricing, and consumer demand. Government also is likely to change in response to how technology is used in society, not just the mechanics of governing, but also the forms of governance and the perception of what is essential in order to govern in a

modern democracy.

## Actions in the 114<sup>th</sup> Congress

Coordinating policy decisions may be essential for addressing the course of expansion of the Internet of Things in the American economy. A congressional [caucus](#) was formed in January 2015 to educate Members on the development of innovative technologies in IoT and public policy. Resolutions introduced in the 114<sup>th</sup> Congress recognize the breadth of technologies and issues that characterize the IoT and call for a development of a national strategy, among other actions. [S.Res. 110](#) was agreed to in March 2015 and a similar resolution, [H.Res. 195](#), was introduced in the House in April.

In support of [S.Res. 110](#), the Government Accountability Office has been [asked to provide](#) information on specific issues with "significant implications for consumers, business, and government" covering current use of IoT in different economic sectors and the federal government; issues for federal agencies; the potential impact on consumer privacy and security; the impact on demand for radio frequency spectrum; and relevant actions by foreign governments.

Hearings in the Senate [Commerce Committee](#), the House [Committee on Energy and Commerce](#) and the [Judiciary Committee](#) have explored the [scope](#) of the Internet of Things, policy issues such as intellectual property rights, and some of its uses, such as [agricultural](#) and [healthcare](#).

## Challenges

In supporting the development of the Internet of Things, Congress has many intersecting issues and policies to consider, not least of these might be the role of the federal government. How much leadership should the federal government offer to industry? To what extent might it play a role in eliminating regulatory barriers to growth? How will federal agencies train and hire a new cadre of skilled workers? What role might the federal government have in shaping education and training for jobs in the fields encompassed by the IoT? What social safety nets might be deployed for workers displaced by new technologies? When federal agencies use the IoT to provide services, how much control might it exert over the networks it uses? How do federal agencies assure access to [public goods](#) provided through IoT without impinging on competition and private-sector innovation?