than it is of mine, but I am much more excited about the prospect that my car will automatically direct me to a route without a traffic jam or that a wearable health device will detect an impending medical crisis and alert me or my doctor. But maybe that's just me.

So what, exactly, is the Internet of Things? In my view, it means sensors and other types of telemetry embedded in physical objects,

The workshop will examine a variety of issues, such as:

What are the unique privacy and security concerns associated with smart technology and its data?

What steps can companies take to prevent smart devices from becoming targets of or vectors for malware or adware?

How should we weigh privacy risks against potential societal benefits, such as the ability to generate better data to improve health-care decision making or to promote energy efficiency?

arise, consider whether existing laws and regulations are sufficient to address them, before assuming that new rules are required.

For the FTC, I believe we can help ensure that the promise of innovations, like the Internet of Things, is realized by using our unique set of policy and enforcement tools. First and foremost, in a new technology or industry that is rapidly innovating, we should use our policy R&D function to get a better understanding of the technology itself; the new business models it may enable; any existing regulatory structures, including any self-regulation; market dynamics; and the nature and extent of likely consumer and competitive benefits and risks. Second, we should use this learning to educate consumers and businesses on how to avoid or minimize any risks that we may identify. Providing consumer tips and suggesting best practices for business is one of the FTC's most valuable and cost-effective activities. Of course, the FTC is also an enforcement agency and it can and should use its traditional deception and unfairness authority to stop consumer harms that may arise from particular Internet-connected devices. This not only helps consumers but also benefits the companies involved in the Internet of Things by policing actors that may tarnish the technology itself. Likewise, the FTC should use its flexible and fact-intensive approach to antitrust enforcement to investigate and, where appropriate, challenge competitive harms occurring in the Internet sphere.

For the remainder of my remarks, I will touch briefly on the specific issues—data security, mobile privacy, big data, and net neutrality—that have the most relevance to the development of the Internet of Things.

Data Security

As you know, the FTC, as part of its broad focus on consumer privacy, has an active data security program. The importance of this program will only continue to grow with the Internet of Things, which will sometimes involve the transmission of sensitive data such as a consumer's

health status or private activities within the home. A recent FTC case exemplifies the kinds of data security risks that the Internet of Things may present. Last month, the FTC settled a case against TRENDnet, which sold its Internet-connected SecurView cameras for purposes ranging from home security to baby monitoring.[2] Although the company claimed that the cameras were secure, they actually had faulty software that allowed unfettered online viewing by anyone with a camera's Internet address. As a result, hackers posted live feeds of nearly 700 consumer cameras on the Internet, showing activities such

Currently, 47 states have data security laws requiring consumer notification if personal information has been compromised. Although some of the laws are similar, they are not identical and companies thus need to ensure compliance with dozens of statutes and provide varying consumer notifications. A single standard would let companies know what to do and consumers know what to expect when a breach occurs.

Mobile

Mobile has also been a highly disruptive technology that has brought great benefits to consumers and opportunities to businesses. The growth in the use of mobile devices is astronomical. According to the International Telecommunication Union, the number of mobile subscribers globally rose from 5.4 billion in 2010 to 6.8 billion at the end of 2012.[3] Mobile devices play an important role in the Internet of Things as

entitled *Mobile Security: Potential Threats and Solutions*,[5]

Although the ability to collect and analyze large data sets offers benefits in medical, scientific, economic, and other types of knowledge and research, as well as for business innovation, at the same time, the collection of large amounts of data about individual consumers may also raise privacy concerns. In response to these kinds of concerns, the Commission recently began a formal study of the data broker industry. We sent out formal requests for information to nine large data brokers to learn more about their practices, including how they use, share, and secure consumer data. It is vital that we have a good understanding of how data brokers operate because appropriate use of data can greatly benefit consumers through better services and convenience while inappropriate use or insecure maintenance of data could cause significant harm to consumers. We will carefully analyze the submissions from the companies and use the information to decide how to proceed in this area.

Net Neutrality

Another issue with implications for the evolution of the Internet of Things is the debate over how to regulate the flow of information on the Internet. Some market participants, mainly content providers, want the government to impose network neutrality rules on the owners of the Internet's physical infrastructure and require them to treat all users and all transmissions alike. They think such unfettered access to the network is a key driver of the Internet's continued success, as it allows content providers to find their market and the market to find content providers without interference. Network owners disagree and think such regulations are unnecessary and could stifle innovation on the Internet. They believe the freedom to experiment with business models is what sparked the Internet revolution and point to examples, like AOL, where "walled garden" models that arguably could violate network neutrality principles have flourished and then receded based on natural market forces. The FCC has sided mainly with the content providers and issued network neutrality rules which have been challenged repeatedly by

network owners on multiple grounds – indeed, we are all waiting to see what the DC Circuit decides in *Verizon v. FCC*, which could bring some needed clarity to this area.

From my perspective, we do not need another layer of regulati

Second, backbone facilities and regional networks have established numerous additional interconnection points, altering the old three-tiered Internet hierarchy and creating further redundancy in the system. Regional networks now engage in secondary peering and multihoming, by which they can route their traffic

Internet's interconnected architecture and the physical limits of our spectrum and other transmission resources, means congestion management likely will remain an issue for years to come.

As in any other industry, however, free-market price setting should be the default mechanism to allocate resources and incentivize development of congestion solutions. Tiered pricing or pricing flexibility for network operators helps sort out higher priority from lower priority uses of relatively scarce resources. Enforcing a one price, all-you-can-eat approach to network access will distort investment incentives and allow free-riding by heavy users. Even worse, it could also interfere with the prioritization of traffic for Internet-connected devices that provide crucial or time-sensitive monitoring and responses, which may hamper the development of these services and ultimately reduce consumer benefits from the Internet of Things

Fifth, private parties have developed sophisticated and increasingly global multistakeholder organizations (MSOs) to help govern the Internet. Although these organizations are not perfect, they have successfully managed the Internet's complex and thorny problems with bottom up, consensus-based decision making of the most interested and arguably best-situated parties – engineers and businesspeople. The important point about MSOs is that they help mitigate the possibility of concentrated market power with their broad participation, consensus-based organizational structures, and adherence to principles like openness, transparency, and accountability.

There have been relatively few disputes about vertical foreclosure on the Internet, which tells me that the design characteristics and changes to the network's structure, along with increasing use of MSOs, together tend to mitigate the possibility of consumer harm or durable market power. Certainly, we need to be vigilant about vertical restraints and foreclosure, but the limited number of known transgressions to date strongly suggests an enforcement approach

would be more appropriate, and less invasive, than new regulations. We should continue to focus on encouraging businesses to expand network capacity and abide by our existing antitrust and consumer protection laws. We should also think twice before enacting new regulations that could hinder innovation.