Antitrust, Vol. 29, No. 1, Fall 2014.

Connecting Antitrust Standards to the Internet of Things

BY GREGORY G. WROBEL

THE FEDERAL TRADE COMMISSION is engaged in ongoing study and public discourse about the Internet of Things (IOT), which is fitting terrain given the Commission's dual mandate for consumer protection and antitrust enforcement. The IOT is at an early stage of development but evolving rapidly through diverse business initiatives for a wide range of products, and offers great promise to enhance consumer welfare through new products, efficiencies and cost savings for existing products, and vast new databases with wide potential for personal, business, and government applications.[1]

These business initiatives have not faced material impediments from government or private antitrust enforcement, but the contours of markets for IOT products—used here to cover both physical products, data analytics, and related services—are nascent and difficult to discern, and business models and practices used now may provoke antitrust claims and investigations in the future as IOT products grow in importance and perhaps evolve into distinct relevant markets.[2]

The FTC has focused mostly on consumer protection, privacy, and data security concerns rather than how antitrust standards apply to the IOT.[3] The discussion below takes the opposite approach, seeking to connect antitrust standards to the IOT by proceeding from a description of common traits of and business models for emerging IOT products, to a high-level discussion of antitrust standards that impact these business models and strategies to manage antitrust risks that may arise, and closing with comments on the role of the FTC in shaping how antitrust standards apply to the IOT.

Emerging Business Models and Common Traits

FTC Commissioner Maureen Ohlhausen has described the IOT as the "next phase of Internet development [focused] on connecting devices and other objects to the Internet, without the active role of a live person, so that they can collect and communicate information on their own and, in many instances, take action based on the information they send and receive."[4]

A technology website describes the IOT as "the network of physical objects that contain embedded technology to communicate, sense or interact with their internal states or the external environment."[5] A commentator for a recent FTC Workshop traces the emergence of the IOT to a range of advances in sensor technology, investments in wired and mobile broadband networks, wider availability of Bluetooth, Wi-Fi, and similar technologies, and ever-rising use of tablets and smartphones, which make it easier and more cost effective to connect objects to the Internet.[6]

Consumer Products. Commentators see growing consumer demand for IOT products that connect a wide range of devices in the home to the Internet, including thermostats, light bulbs, refrigerators, photo frames, power meters, healthcare and fitness devices, garbage cans, and even cars.[7] Typical early-stage IOT consumer products include small personal sensors that communicate with a smart phone or home WiFi router (e.g., wearable devices that connect to Apple iPhones and input personal health data through the Apple Health App; sensors and control devices for home appliances that communicate with Apple computers or smart phones through apps configured to Apple Home Kit specifications).[8]

Business/Industrial Products. Suppliers of a wide range of business and industrial products are incorporating IOT functionality and providing data analytics services. Data provided by the devices can then be used to avoid unexpected outages, reduce maintenance and service costs, and provide detailed performance analysis that enhances customer satisfaction.[9] Some of these products are designed to improve efficiency for individual customers rather than to provide information for a broader group of customers, so business practices may vary on whether data outputs generated by the installed base of these products will be aggregated and/or shared among customers or with the supplier of the product for broader data analytics services.

Common Traits. Important traits of early-stage IOT products include: direct and indirect network effects in some products; enhancements to existing products; rapid technology development; blurred product markets both for suppli-

Gregory G. Wrobel is a shareholder and head of the Antitrust Practice Group of Vedder Price P.C., Chicago, IL, and is the Articles Editor of ANTITRUST.

ers and customers; close interactions between physical devices and data analytics; mix of open source and proprietary business models; dependence on the Internet, cable, and satellite communications systems; interoperability with computer and cell phone operating systems; active role in product development by leading suppliers of consumer and industrial products, computer hardware and software, microprocessors and sensors, communications devices and services, and information and data analytics services.

Product Enhancement. Many IOT products enhance existing products with sensing and communications technology to generate data and send/receive commands (e.g., household appliances with electronic sensors and control systems for remote operation and monitoring). Over time, entirely new IOT products may emerge to replace older products that lack new functionality (e.g., self-driving vehicles may be viewed as a service or distinct product and product market from driver-operated vehicles).

Autonomous Operation. IOT products may operate automatically and autonomously, without active human control. Once installed, the device may generate data and perform functions of which the consumer or business user is not actively aware. Computers and cell phones now operate primarily with human direction, but may also function as IOT devices when not actively managed (e.g., cell phones transmit geolocation data when turned on but not in active use).[10]

Data Analytics. IOT products generate data that may enhance use of existing products (e.g., by providing early warning signals of component failure in industrial machines). The resulting data may be aggregated and used both to improve the IOT products that generated the data and for unrelated business purposes. Some analysts see data analytics as the key element of business models for IOT products, and posit that "controlling the data value chain from the point of data collection to the point of data analytics is key to unlocking these value creation opportunities."[11]

IOT products may generate data about consumers or customers that are part of the installed base, but data analytics outputs may not be used solely or even primarily by the customers, which may raise important issues in defining relevant markets for the products and/or data outputs they generate.

Interoperability. In an effort to generate network efficiencies, some IOT products are designed to be interoperable with other devices used in a particular location (e.g., home, office, and factory control panels that interact with multiple products used for distinct applications), and use standard data formats to facilitate aggregation into databases for analysis.[12] Other IOT products may be configured to interface with a particular computer or cell phone operating system (e.g., apps for Apple and Android devices). Interoperability may also help to achieve important data security and privacy goals by making a range of IOT products and data outputs compatible with a single data security and privacy system selected by the suppliers and/or individual users.[13]

Potential benefits of interoperability are driving numerous efforts to develop industry standards, but views may vary on whether the desired interoperability is between and among competing IOT products, with communications and control systems for the products, or with data analytics services that use their data outputs. These potentially conflicting goals may give rise to difficulties and disputes in determining the reasonable range of IOT products and suppliers to include in standards programs.[14] For many IOT products, standardization may be necessary to assure interoperability with communications and control systems, but other product features and data analytics services may be differentiated through normal competitive processes.

Communications Networks. Current IOT products for the most part use interfaces with devices connected to the Internet to transmit and receive data and commands; some devices may use cable or satellite services.[15] Over time, specialized communications networks may develop that operate independent of phone and cable services, configured to be cost-effective for the number, size, and (low) power requirements of IOT devices.[16]

The FCC and state agencies may have important roles in determining standards, requirements, and/or terms of service for IOT products to transmit data via broadcast or services of regulated carriers. A range of difficult issues may arise over the intersection of antitrust standards with such federal and state regulation, which are beyond the scope of this discussion.

Open Models and Proprietary Models. Emerging business models for the early-stage IOT reveal a mix of open-source and proprietary strategies. Open models may need standards to configure, communicate, and share data among IOT devices on a common platform to achieve interoperability and consistent datasets.[17] Proprietary models may seek a competitive advantage for the suppliers' IOT products, perhaps driven by proprietary analysis of data generated by products of a particular firm or group of firms.[18]

As with cell phones and some Internet-based services, some proprietary models may seek to achieve network effects by encouraging application software developers to focus on one IOT platform rather than others, and to promote widespread adoption by consumers or business customers of IOT products configured for a particular technology platform. Proprietary models also may give sponsors of IOT platforms and technology standards (e.g., Apple and Android operating system for cell phones), access to data that has independent market value or assists the sponsors to market and provide a range of different IOT products and related services to their customers.

The ability of some IOT products to generate direct network effects among users may be open to question (e.g., Nest thermostats and users of these devices do not communicate with each other through the Internet (at least as of now), or gain greater value from the product as the network of users grows). For other IOT products, the potential for

network effects may be more apparent; for example, traffic monitoring systems may benefit all users by generating real-time data for drivers (or eventually for driverless vehicles), and the benefits of these systems may grow as more vehicles are equipped with sensors, etc. As IOT products gain favor, an important focus of market analysis will be whether a product generates direct or indirect network effects, and if so whether these effects promote and thereby explain consolidation that may occur in markets for these products.

The discussion below includes a general overview of the implications of these common traits and emerging business models for potential antitrust tensions and risk mitigation strategies for early-stage IOT products.

Antitrust Tensions and Risk Mitigation Strategies

Discerning the precise business practices and market dynamics that will spawn future antitrust battles over the IOT is difficult, due in large part to the nascent stage of business initiatives and technology for IOT products.[19] Given this uncertainty, suppliers may be well-served by using long-term risk mitigation strategies that will position the supplier as much as possible to wage these battles within the domain of the full rule of reason, where the procompetitive benefits of emerging IOT products will (and must) be weighed against competitive harm attributed to the supplier's business model.

Key elements of this approach are:

(1) Avoid business practices that provide a colorable basis to apply either a per se or truncated rule of reason standard (i.e., practices that are recognized to have obvious anticompetitive effects based on case law and current economic thinking), given that future plaintiffs may seize on such practices to explain the supplier's commercial success and perhaps the plaintiff's commercial failure.[20]

(2) Engage in objective periodic assessments of evolving market structure and market performance, and adjust business practices that may exclude rivals or unduly limit customer choice, in particular where the supplier's market share in plausible relevant markets for the IOT product could suggest the ability to exercise market power.

These general risk mitigation strategies may serve as general guideposts in evaluating and controlling the particular antitrust risks discussed below.

Open-Source and Proprietary Business Models. Open-source standards and business models for IOT products are less likely to create antitrust risks compared to proprietary models, given that open-source models tend to promote competition among rival device makers and/or service providers by assuring interoperability. Proprietary models may seek to avoid interoperability at some level in order to gain a competitive advantage; these models may give rise to antitrust risks in market settings where the supplier has a significant market share, and risks should be lessened where a sufficient number of competing IOT products are offered under either open-source or proprietary models to avoid market power concerns.

Market structure and dynamics may change—perhaps even rapidly—given that technology, applications, and data analytics for IOT products are evolving rapidly. Network effects may emerge over time for particular IOT products or systems, and these effects may drive a shift toward concentrated market structures.

Some IOT business models reflect a hybrid approach in which a technical standard or platform for software and data analytics is open only to members of an association or joint venture who agree to make products configured to the venture's IOT standards, or where members of an industry adopt a standard that applies only to members of the industry.

Normal market analysis is warranted—with monitoring over time in light of changing market conditions—to evaluate whether proprietary business models and restraints on use of standards are shifting markets for particular IOT products toward a concentrated market structure and, if so, whether the restraints can be justified based on efficiencies and consumer benefits that the restraints promote.

[S]uppliers may be well-served by using long-term risk mitigation strategies that will position the supplier as much as possible to wage these battles within the domain of the full rule of reason, where the procompetitive benefits of emerging IOT products will (and must) be weighed against competitive harm attributed to the supplier's business model.

Mergers. Government merger review has not yet yielded challenges or voluntary termination of transactions involving IOT products. Most mergers related to the IOT have been vertical rather than horizontal (e.g., Google's acquisition of Nest), and antitrust risks have been minimal for early movers in such transactions given the prospect for long-term integrative efficiencies and perhaps due to a lack of clearly ascertainable relevant markets for particular IOT products (i.e., consumer demand remains uncertain or is tied to traditional products that may gain IOT functionality).[21]

Parties to merger transactions in the early-stage IOT may emphasize these difficulties in delineating product markets, as well as potential benefits to consumers from transactions that drive development of new products and services.

Over time, merger transactions may have more horizontal elements, market facts may develop that show distinct consumer demand and/or suppliers of IOT products, and such markets may trend toward greater concentration in response to network effects or other factors. The potential also exists for agency review to focus on competitive effects in innovation markets for IOT products.[22]

For now, however, parties seeking to position themselves through vertical acquisitions for a meaningful role in the IOT do not appear to have faced significant antitrust concerns in agency review of merger transactions.

Joint Ventures. The most visible collaborative efforts emerging in the early-stage IOT appear to focus on technology standards to achieve interoperability for IOT products made by different suppliers (discussed below). Joint venture arrangements may also arise among suppliers of complementary products and services that are combined to make IOT products. As with vertical mergers, these arrangements may give rise to few antitrust risks in the early-stage IOT, where venture participants identify integrative efficiencies that the venture will promote, avoid or carefully justify restraints that foreclose rivals from access to essential technology, and take affirmative steps to prevent spillover collusion unrelated to legitimate goals of the venture.

Joint ventures that include rival suppliers of IOT products may warrant additional precautions to mitigate antitrust risks, including focused market analysis to avoid overinclusive ventures, or nonexclusive participation so members can participate in other IOT ventures, and measures to prevent spillover collusion in the marketing and sale of IOT products.

Rival firms that compete in a given product market may also face antitrust risks if they collaborate in sharing data from IOT products, in particular if the shift to a collaborative model eliminates important elements of commercial rivalry that benefited customers in the past. Even if there is no history of prior competition among suppliers of the specific IOT products at issue, antitrust enforcers may still be skeptical if the companies were rivals in similar pre-IOT products, or if the types of collaboration at issue have reduced competition in other industries or markets. Thus, precautions may be warranted to avoid spillover collusion (e.g., the de-identification of data outputs or the use of a third-party intermediary to prepare aggregate databases), even if data sharing arrangements are likely to produce procompetitive benefits.

Industry Standards. A great deal of activity is now focused on industry standards for early-stage IOT products.[23] The need for standards is apparent to achieve interoperability and consistency in data outputs, among other considerations, so participants should have little difficulty demonstrating expected procompetitive benefits for these efforts. Participants should adopt procedures consistent with existing guidance to mitigate antitrust risk in the standards process (e.g., disclosure of standard-essential IP rights; up-front licensing commitments on reasonable terms). If participants exclude some actual or potential rivals from a standards program, they should be prepared to identify legitimate, procompetitive grounds for doing so.[24]

Complexities may arise beyond the scope of normal industry standards programs, where a diverse range of products and devices must interoperate under a given IOT standard, e.g., where appliances, utility systems, and perhaps even vehicles in a household interact with a common control system or database, or similar applications for industrial equipment made by diverse suppliers and for diverse applications in a plant, etc. Technical considerations of this type may complicate efforts to set a common standard and may necessitate limits on the scope of the standards program in order to achieve agreement. Where such circumstances arise, and the potential exists that excluded product makers may be competitively disadvantaged, the standards body should fully document technical difficulties that arise and the need to restrict participation in order to achieve agreement on a standard.

IP Licensing. Technology used in IOT products is likely to embody a wide range of patents, copyrights, proprietary software, and other intellectual property rights. As discussed above, standards programs for IOT products should address licensing of standard essential IP rights to avoid hold-up on licensing and royalty terms, and preserve competition among suppliers of IOT products that use the standard.

Apart from standard essential IP rights, antitrust risks may arise primarily with overly restrictive IP licensing models, which may exclude rivals from one or more emerging markets for IOT products. A broad approach in which owners of IP rights used in IOT products license those rights freely on reasonable, nonexclusive terms should not raise material antitrust risks.

A range of business considerations may drive decisions on licensing and enforcement of IP rights in the early-stage IOT. Suppliers developing new IOT products may adopt open and favorable licensing strategies for IP rights in order to develop market demand (as well as supply) for new IOT products. Balanced against these concerns may be funding needs to support investments in IP rights. Suppliers that pursue a closed business model (i.e., refusing to license IP rights, or doing so only subject to exclusive dealing or other restraints on licensees) may in theory face potential antitrust risks, but unilateral refusals to license valid IP rights may be presumptively lawful in deference to rights under patent and copyright laws, and such conduct typically has been analyzed under the rule of reason.[25]

Suppliers of IOT products that hold large IP portfolios may seek positions of parity (or avoid costly and long-running IP litigation), by negotiating cross-licensing arrangements with rivals, as seen in existing markets for computers, cell phones, and other products that embody numerous patented components and methods.[26] Over time, strategies of this kind may lead to market consolidation if firms that control large portfolios of IP rights used in IOT products license their IP rights only selectively with other similar firms.

Exclusive Dealing, Bundling, Price Discrimination. Antitrust risks may arise with IOT products sold using restrictive sales and distribution methods, bundled sales policies, price discrimination, and other nonprice restraints that are normally analyzed under the rule of reason (or Section 2 standards where the supplier has a significant market position). As with other products and services, these antitrust risks should be lessened where a number of existing rivals sell,

or are working independently to develop, competing IOT products and the supplier does not account for a dominant share of sales.

A range of factual issues may arise with the early-stage IOT in defining relevant product and geographic markets for rule of reason analysis or in showing direct evidence of anticompetitive effects that may obviate the need for relevant market analysis.[27] For IOT products that are enhancements to existing products (e.g., IOT functionality added to current versions of home appliances, industrial equipment, and related controls), relevant markets and potential competitive effects may be analyzed using historical data in the market for existing products. Over time, data may emerge that show distinct consumer/customer demand and perhaps distinct suppliers for IOT products, which may warrant analysis of competitive restraints and effects in a relevant market limited to the IOT products.

Rivalry may also arise for control of key communications and control platforms that transmit, store, and analyze data from IOT products. Over time, such trends may reveal distinct customer demand and perhaps separate suppliers of IOT communications and control systems, which may warrant analysis of markets limited to these systems distinct from the IOT products that operate on the systems (e.g., numerous apps for a particular end use may compete on Apple, Android, and Microsoft operating system platforms, but competition among suppliers of control systems and some data analytics services that interface with or are enabled by the apps may take shape in a separate and perhaps more concentrated relevant market).

Use of Data Outputs. A key feature of IOT products—and for some applications the key strategic benefit for suppliers—is the feedback effects that data analytics will generate for customer service, marketing, advertising, and product improvement. In fact, some IOT products (e.g., driverless vehicles), may not function at all except through complex real-time interactions with data analytics systems. Thus, rights to access and use data outputs from IOT products and related data analytics systems may be a key driver of competition for IOT products.

Some IOT products may use data outputs primarily to support use of the IOT products themselves (e.g., industrial sensors that monitor component usage, wear, and failure); others may generate data that has value for other applications (e.g., geo-location data generated by cell phones enables new approaches to consumer marketing).

Given the importance of data analytics to many IOT products, antitrust risks may arise if suppliers of IOT products (or communications and control systems) restrict access or use of data (e.g., where product users are required to provide data outputs exclusively to the supplier or prohibited from sharing data with rival providers of data analytics services). The competitive effects of such restraints should be analyzed in the market setting of particular IOT products; open models that share data freely are less likely to present antitrust risks; proprietary or restrictive business models may warrant closer consideration of antitrust risks, but may be justified as a way to drive development and sustain the financial viability of IOT products and systems.

For example, some IOT products may operate in a two-sided market setting where suppliers use free or low-cost pricing to build a network or installed base of IOT products—perhaps at significant cost to the supplier—with the intention of monetizing the network through data analytics that are directed to customers on another side of the market (e.g., free search services via Google and free social media services via Facebook drive demand for advertising services that these firms offer to a separate group of customers). Business models of this type may provide significant value to users on both sides of the market, and may suffer from free-rider problems if the supplier must share data outputs with rivals that do not bear the cost to create an installed base of IOT products.

Antitrust risks may arise from bundling the sale of physical products with control systems and/or data analytics services or from requirements that customers share data outputs with the supplier. For example, a supplier of industrial IOT products may provide data analytics services that customers are required to purchase as a condition to product warranties (or bundled for no additional charge with warranty service). These practices may benefit customers but also may foreclose rival suppliers of data analytics services from engaging in viable competition. Suppliers may also require that customers share data outputs with the supplier, even if only to support the supplier's internal product improvement efforts, or may restrict customers from sharing data outputs with competing suppliers of IOT products or data analytics services. The competitive effects and business justifications for such restraints warrant close consideration as the contours of relevant markets take shape for particular IOT products and data analytics services.

For some IOT products, sharing data outputs that contain sensitive personal or business information with rival suppliers (or among competing firms that use the IOT products), may create unwarranted antitrust risks of horizontal collusion (e.g., industrial sensors may reveal the number of installations and related operating details that are proprietary to the customer and/or supplier). Suppliers may also need to restrict data sharing for IOT products used by consumers, to comply with consumer protection, privacy, and data security rights.

Tensions with Regulation

A range of regulatory programs may apply to particular IOT products. For example, the Federal Communications Comsion (FCC) has jurisdiction over existing communications networks used for IOT products, and may, as well, for specialized communications systems that emerge; the Federal Energy Regulatory Commission (FERC) and state public utility commissions may have jurisdiction over IOT products used with natural gas pipelines and electric transmission

lines; and the Food and Drug Administration (FDA) has jurisdiction over IOT products used as medical devices.[28] These regulatory programs apply to existing products that do not have IOT functionality, so regulations and regulatory actions that apply to these products may show how the agencies will harmonize antitrust standards with regulatory requirements for IOT products.

IOT products may also give rise to new issues about regulatory jurisdiction (e.g., overlapping authority of the FCC and FERC for IOT products used on interstate natural gas pipelines and electric transmission lines). As these issues arise, regulatory agencies and courts can be expected to apply established legal doctrines on preemption, primary jurisdiction, and implied immunity to determine and harmonize the role of regulation and antitrust laws. The FTC and Department of Justice may also be expected to take an active role in advocating for regulatory actions that achieve and preserve competitive markets for IOT products.

Tensions with Consumer Protection, Privacy, and Data Security Rights

FTC commissioners and staff have articulated core principles for suppliers of IOT products to protect consumer protection, privacy, and data security rights of consumers and other users, focused largely on transparency and full disclosure (i.e., prominent and accessible disclosure about data collection and use), consumer control (i.e., let individual consumers decide what data to share), and data security (i.e., use of industry standard technology and methods to protect data from unauthorized disclosure and use).[29] The Commission has refrained from rulemaking that might shape or restrict business models in the early-stage IOT, and the FTC's initial enforcement action involving an IOT product aligns with Commission actions directed at non-IOT products.[30]

IOT products often operate without human interaction, and this functionality may complicate how suppliers and users comply with these enforcement standards and goals (e.g., once a consumer or property owner installs an IOT thermostat in a dwelling, the consumer and future occupants may not be aware that the product supplier is receiving Internet-enabled data about the dwelling and settings on the device, etc.). These tensions may give rise to new or refined enforcement standards for suppliers of IOT products, property owners, and others to comply with consumer protection, privacy, and data security rights.

Importantly, these consumer protection concerns with data from IOT products do not appear to create new conflicts with antitrust standards in the early-stage IOT. The rights in question warrant protection both in fragmented and highly concentrated market settings. Nor do these rights depend on the market position of the IOT products and related data systems, or whether suppliers or users are engaged in conduct that may harm competition. In fact, enforcement efficiencies may arise in concentrated markets where monitoring and enforcement against only one or a small number of key suppliers, platforms, or networks may achieve compliance with consumer protection rights.[31]

Conclusion

The early-stage IOT is evolving rapidly and presents many open questions about the viability of IOT products, the contours of relevant markets, and the benefits and needs for open or closed business models for particular IOT products. These dynamics and uncertainties may mitigate some potential antitrust risks for now, but suppliers should take a cautious approach about business models, IP licensing, and sales and distribution practices used to achieve commercial success with new IOT products.

Antitrust risks may arise at a later stage if the supplier develops a network or installed base using an open model but then shifts to a closed model that unduly restricts customer choice or market access by rivals.[32] Suppliers may evaluate potential antitrust risks for now based on their current position in relevant markets for non-IOT products that they sell, but they should closely monitor industry dynamics and the focus of market analysis as customer demand for IOT products evolves and the contours emerge for distinct relevant markets for particular IOT products or networks.

The FTC has focused largely on consumer protection rather than antitrust concerns with the IOT. The regulatory humility implicit in the Commission's approach to the IOT is even more important from the perspective of antitrust than consumer protection enforcement, so that regulatory oversight or enforcement pressures do not thwart technological innovations and growth in customer acceptance and demand, or pick winners in the competitive struggle among suppliers and business models for IOT products in diverse consumer and business markets.[33]

Tensions between consumer protection and antitrust standards do not appear evident in the early-stage IOT, but technology is advancing rapidly and business models that offer significant procompetitive benefits to customers may confront difficulties in assuring compliance with consumer protection, privacy, and data security rights. Over time, these tensions may present challenges for product suppliers, and the FTC and other antitrust/consumer protection enforcers, in balancing these consumer welfare effects.

With its dual enforcement mandate, the FTC is uniquely positioned as it embarks on its second century—and the Internet passes the quarter-century mark—to provide targeted enforcement and constructive advocacy on how to balance such conflicts, and thereby help connect consumer protection and antitrust standards in a consistent way to the Internet of Things. ■

[1] *See, e.g.*, Pew Research Center, Digital Life in 2025: The Internet of Things Will Thrive by 2025 (May 14, 2014), *available at* http://www.pewinternet.org/2014/05/14/internet-of-things/ (report summarizing responses to opt-in survey of 1,867 technology experts and other stake-

holders, showing consensus view of expected growth and benefits of IOT products despite challenges to personal privacy and control of data).

[2] *See, e.g.*, Phil Milford, *Eaton Avoids $2.4 Billion Damage Claim in Meritor Accord*, Bloomberg (June 23, 2014), http://www.bloomberg.com/news/2014-06-23/eaton-avoids-2-4-billion-damage-claim-in-meritor-accord.html (describing $500 million settlement of private antitrust suit filed in 2006, with $2.4 billion potential exposure at damages trial, challenging use of exclusive dealing, loyalty discounts, and rebate arrangements by leading maker of truck transmissions in the early 2000s to exclude rival transmission maker).

[3] *See, e.g.*, FTC Workshop, *Internet of Things—Privacy and Security in a Connected World* (Nov. 19, 2013) [hereinafter FTC IOT Workshop], http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world (announcements, public comments, and program transcripts for workshop).

[4] Maureen K. Ohlhausen, FTC Commissioner, Remarks to U.S. Chamber of Commerce, The Internet of Things and The FTC: Does Innovation Require Intervention? 1 (Oct. 18, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/internet-things-ftc-does-innovation-require-intervention/131008internetthingsremarks.pdf (discussing data security, mobile privacy, big data, net neutrality, and competition issues arising with IOT products; recommending flexible and fact-intensive approach to antitrust enforcement; analyzing market forces that obviate need for FCC net neutrality rule for Internet data transmission).

[5] *See* Gartner IT Glossary, Internet of Things, http://www.gartner.com/it-glossary/internet-of-things/ (accessed Aug. 11, 2014); *see also* John Rath, *The Internet of Things: Buzzword or Big Business?* (May 31, 2013), http://www.datacenterknowledge.com/archives/2013/05/31/internet-of-things/ (discussing broad scope of business initiatives for IOT products).

[6] FTC IOT Workshop, Comments of U.S. Chamber of Commerce 2 (Jan. 10, 2014), *available at* http://www.ftc.gov/policy/public-comments/comment-00011-51.

[7] Chris O'Brien, *CES 2014: Consumer Electronics Show to Feature "Internet of Things,"* L.A. Times, Jan. 4, 2014, http://www.latimes.com/business/la-fi-ces-internet-things-20140105-story.html#page=1; *see also* Daniel Castro & Jordan Misra, Center for Data Innovation, The Internet of Things, (Nov. 2013), http://www.datainnovation.org/2013/11/the-internet-of-things/ (describing range of applications for IOT products for personal, business, and government uses); Don Clark & Geoffrey A. Fowler, *Seeing the Internet of Things in Action: A Look at Some of the Connected Gear at CES*, Wall St. J., Jan. 8, 2014, http://online.wsj.com/news/articles/SB10001424052702303393804579308642134683098 (same).

[8] *See, e.g.*, Apple iOS8 Preview for Health App, https://www.apple.com/ios/ios8/health/; Apple Developer HomeKit website, https://developer.apple.com/homekit/; *Google's Nest Launches Thread Platform for Smart Homes, Internet of Things* (July 15, 2014), http://na.newshub.org/google_s_nest_launches_thread_platform_for_smart_homes_internet_of_things_2052020.html (describing Google-led Thread networking protocol with security and low-power features for connecting household devices, and Thread Group that includes Samsung, chip companies ARM, Freescale Semiconductor and Silicon Labs, Big Ass Fans, and lock maker Yale).

[9] *See, e.g.*, Castro & Misra, *supra* note 7 (describing personal, business, and government applications for IOT products and data analytics); Efrat Kasznik, *When Big Iron Meets Big Data: Unlocking Value Creation Opportunities in the Internet of Things—Industry Report* (June 25, 2014), http://www.iam-magazine.com/industryreports/Detail.aspx?g=15c9fcef-9313-416a-b79c-76508f84c1f4 (describing GE industrial IOT products, including RailConnect 360 (collects and analyzes performance data during locomotive operations), Grid IQ Insight (provides utilities with advanced analytics of data collected from equipment along the grid to predict, manage, and forecast potential problems and optimize operating performance), and Flight Efficiency Services (collects and analyzes real-time data generated by aircraft to improve fuel management, flight analytics, navigation services, and fleet synchronization); Clint Boulton, *Sensors in Heavy Machinery Signal Need for Better Analytics*, Wall St. J. (July 31, 2014), http://blogs.wsj.com/cio/2014/07/31/sensors-in-heavy-machinery-signal-need-for-better-analytics/ (describing IOT sensors in earth-moving equipment that transmit data for customer download from manufacturer-hosted websites via satellite; noting software difficulties in integrating data from sensors and websites of different equipment makers (Caterpillar, Deere, Hitachi), and separate RFID tag system for maintenance records).

[10] *See, e.g.*, Douglas MacMillan, *Foursquare Now Tracks Users Even When the App Is Closed*, Wall St. J. (Aug. 6, 2014), http://blogs.wsj.com/digits/2014/08/06/foursquare-now-tracks-users-even-when-the-app-is-closed/?mod=WSJ_hpp_MIDDLENexttoWhatsNewsThird (describing change in mobile phone app that tracks user locations via GPS coordinates and generates data stream for app maker whenever the phone is powered on).

[11] *See, e.g.*, Kasznik, *supra* note 9 (commenting that rationale for Google's $3.2 billion acquisition of Nest Labs was that Google augmented its data analytics capabilities by acquiring control of physical objects that collect data, and gained access to home data collection endpoints through Nest's growing inventory of home automation devices); Jeffrey A. Eisenach & Ilene Knable Gotts, *In Search of a Competition Doctrine for Information Technology Markets: Recent Antitrust Developments in the Online Sector*, Comm. & Competition L.: Key Issues in the Telecoms, Media & Tech. Sectors 21 (forthcoming), *available at* http://www.techpolicydaily.com/wp-content/uploads/2014/06/In-Search-of-a-Competition-Doctrine-for-Information-Technology-Markets-Eisenach-Gotts.pdf (describing IOT as "one of the factors (perhaps the most significant factor) driving the related phenomena commonly referred to as "big data": the capacity to collect, synthesize and analyze previously incomprehensible amounts of data," and observing that "access to database information is becoming increasingly important from a competition perspective").

[12] *See, e.g.*, Quentin Hardy, *Intel, Qualcomm and Others Compete for "Internet of Things" Standard*, N.Y. Times (July 8, 2014), http://bits.blogs.nytimes.com/2014/07/08/standard-behavior-in-an-internet-goldrush/?_php=true&_type=blogs&_r=0 (describing formation of Open Interconnect Consortium with Intel, Atmel, Broadcom, Dell, Samsung, and Wind River to create open-source standard to wirelessly connect devices to one another and to the Internet; describing similar effort by AllSeen Alliance, led by Qualcomm with over 50 other companies, including Microsoft and Cisco, and other similar efforts that Google, Apple, and other companies may pursue; noting that communications standards will affect the means for collecting data about the behavior of both devices and people that use them, which will affect future product development and what ads individual consumers are shown); Dan Rowinski, *Intel and Samsung Join Battle over the Internet of Things*, Readwrite (July 8, 2014), http://readwrite.com/2014/07/08/open-internet-consortium-internet-of-things-standards (same; noting similar standards efforts of Industrial Internet Consortium led by AT&T, Cisco, General Electric, IBM, and Intel).

[13] *See, e.g.*, FTC IOT Workshop, Comments of Infineon Technologies North America Corp. (Jan. 10, 2014), http://www.ftc.gov/policy/public-comments/comment-00009-59 (describing security standards programs for IOT products).

[14] Interoperability of IOT products may also be limited by government restraints on the Internet. *See, e.g.*, Anupam Chander & Uyen P. Le, *Breaking the Web: Data Localization vs. the Global Internet*, Emory L.J. (forthcoming) (UC Davis Legal Studies Research Paper No. 378, at 41–42), *available at* http://ssrn.com/abstract=2407858 (discussing country restrictions on information and data flow via the Internet that may result in data localization within countries and thereby limit interoperability and data analytics for some IOT products).

[15] Cost structures for cellular and cable service may not accommodate direct connection for IOT devices, but rather may induce users to route data from IOT devices through cell phones and other devices covered by existing data plans. As the IOT evolves, service providers may change rate structures to include special pricing for IOT devices, which may impact nascent competition from alternative communications networks. *See, e.g.*, Ryan Knutson, *Sprint Will Sell a $12 Wireless Plan that Only Connects to Facebook or Twitter*, Wall St. J. (July 30, 2014), http://blogs.wsj.com/digits/2014/07/30/sprint-tries-a-facebook-only-wireless-plan/?mod=trending_now_1 (describing announcement by Sprint of reduced pricing model for connection only to particular social media sites).

[16] *See, e.g.*, *Internet of Things Network to Launch in UK Next Year* (May 18, 2014), http://phys.org/news/2014-05-internet-network-uk-year.html (describing announced plan of UK-based Arqiva to build and run a national low-power, battery-preserving network to connect smart devices in ten UK cities during 2015 in support of the Internet of Things; noting that low power

consumption allows batteries and equipment to last longer, avoiding the cost and inconvenience of replacing devices); Katherine Noyes, *With Phones in Its Pocket, ARM Eyes the Internet of Things*, FORTUNE (July 22, 2014), http://fortune.com/2014/07/22/with-phones-in-its-pocket-arm-eyes-the-internet-of-things/ (describing ARM Cortex-M microprocessor series directed at IOT products featuring very low energy usage and miniaturization, and ARM work on 6LoWPAN standard for interoperability of networks of low-power devices with current dominant Internet protocol, and on CoAP Internet protocol tailored to simple electronics).

[17] *See, e.g.*, Eva Eanoria, *Open-Source Approaches to Ensure IoT Success* (July 22, 2014), http://m2mworldnews.com/2014/07/22/15424-open-source-approaches-to-ensure-iot-success (describing concerns of advocates who favor open-source models for the IOT, that "Silos of Things" are emerging where nothing works across different silos because first generations of IOT devices are built on different platforms, and users must look for the individual apps that make each device work).

[18] *See, e.g.*, *AFP, Tech Giants Scramble for Lead on "Internet of Things,"* MSN (June 8, 2014), http://news.msn.com/science-technology/tech-giants-scramble-for-lead-on-internet-of-things (describing new IOT platforms by Apple (iOS 8 mobile operating system, HealthKit software to manage personal healthcare, HomeKit for home appliances), and Samsung (Tizen open-source operating system), following Google's announcement of new Android platform for wearable electronics); Clint Boulton, *Stanley Black & Decker Retools Factory for the Internet of Things*, WALL ST. J. (Aug. 1, 2014), http://blogs.wsj.com/cio/2014/08/01/stanley-black-decker-retools-factory-for-the-internet-of-things/ (describing proprietary system using RFID tags to monitor production quality in factories and communicate data and alerts to staff).

[19] *See, e.g.*, Eisenach & Gotts, *supra* note 11, at 21 (declining to predict precise course technology for the IOT will follow or the exact implications for competition policy).

[20] *See, e.g.*, Timothy J. Muris & Brady P.P. Cummins, *Tools of Reason: Truncation Through Judicial Experience and Economic Learning*, ANTITRUST, Summer 2014, at 46 (discussing application of truncated rule of reason standard by FTC and courts); David Eisenstadt & James Langenfeld, *The Role of Economics in Truncated Rule of Reason Analysis*, ANTITRUST, Summer 2014, at 52 (same). Application of quick look and other truncated rule of reason standards will continue to evolve through government and private enforcement actions, so continued monitoring of case law developments is warranted to identify new applications that increase the risk presented by business practices used with IOT products.

[21] *See, e.g.*, Mark Davidson, *What Schneider Electric's Acquisition of Invensys Means for the MOM Software Space* (Sept. 4, 2013), http://blog.Insresearch.com/blog/bid/186323/What-Schneider-Electric-s-Acquisition-of-Invensys-Means-for-the-MOM-Software-Space (describing Schneider Electric's $5.2 billion acquisition of software/engineering firm Invensys, noting potential synergies to embed real-time energy optimization functionalities from Schneider products into Invensys software services for industrial plant operations).

[22] Agency review has led to challenges of recent vertical mergers in information services markets, which may illustrate the type of market and competitive analysis that may be applied to mergers involving IOT products. *See, e.g.*, Consent Decree, United States v. Google Inc., No. 11-cv-00688 (D.D.C. Oct. 5, 2011), *available at* http://www.justice.gov/atr/cases/google.html (consent decree for Google acquisition of flight search software firm providing, inter alia, (i) requirement to license key software and future upgrades to other flight search companies on fair, reasonable, and nondiscriminatory licensing terms, (ii) prohibition against agreements that unduly restrict airlines from sharing of seat and booking information with Google's competitors, and (iii) prohibition against tying with other Google services); Statement of Fed. Trade Comm'n, In the Matter of Nielsen Holdings N.V. and Arbitron Inc., FTC No. 131-0058 (Sept. 20, 2013), *available at* http://www.ftc.gov/os/caselist/1310058/130920nielsenarbitroncommstmt.pdf (describing consent decree for Nielson acquisition of Arbitron (leading providers of rating services for television and radio, respectively), which required Nielsen to continue cross-platform project with third parties to measure audiences for TV and broadcast radio as well as satellite, Internet, and other platforms, and required Arbitron to license certain software, technology, and data to a third party for audience measurement on portable devices).

[23] *See, e.g.*, FTC Workshop on the IOT, Chuck Bokath, Comments for Standards Development in the Internet of Things (Jan. 10, 2014), *available at* http://www.ftc.gov/policy/public-comments/comment-00014-41 (describing standards programs for the IOT; predicting that standards development may take several years or more); FTC Workshop on the IOT, Comments of CTIA—The Wireless Association 11–14 (Jan. 10, 2014), *available at* http://www.ftc.gov/policy/public-comments/comment-00014-41 (same; recommending against FTC rulemaking over privacy and data use policies for the IOT while industry standards programs are in process).

[24] *See, e.g.*, ABA SECTION OF ANTITRUST LAW, ANTITRUST LAW DEVELOPMENTS 1065–67 (7th ed. 2012) (describing FTC and private enforcement challenging alleged anticompetitive conduct in standards programs).

[25] *See, e.g.*, *id.* at 1084–1107 (describing antitrust standards and enforcement actions for exclusive dealing and other restraints in IP licensing, noting that most restraints are analyzed under the rule of reason and some are presumptively lawful under federal patent and copyright laws, but that potential market or customer allocation concerns may arise if licensor and licensee (or various licensees), are horizontal competitors).

[26] *See, e.g.*, Press Release, Icontrol Networks, Alarm.com and Icontrol Networks Settle Patent Disputes, Announce Cross-Licensing Agreement (Jan. 14, 2014), http://www.icontrol.com/press-releases/alarm-com-icontrol-networks-settle-patent-disputes-announce-cross-licensing-agreement/ (describing settlement of patent disputes and cross-licensing agreement for connected home technology); Press Release, The Network, Google and Cisco Enter into Patent Cross-Licensing Agreement (Feb. 4, 2014), http://newsroom.cisco.com/release/1342051 (describing long-term patent cross-licensing agreement covering broad range of products and technologies to reduce risk of future patent infringement litigation); Shara Tibken, *Samsung Inks Patent Cross-Licensing Pact with Cisco*, CNET (Feb. 5, 2014), http://www.cnet.com/news/samsung-inks-patent-cross-licensing-pact-with-cisco/ (describing cross-licensing deal covering companies' existing patents and new patents over the next 10 years, including patents for connected home technology); *Twitter Buys Patents, Seals Licensing Pact with IBM*, FOXBUSINESS.COM (Jan. 31, 2014), http://www.foxbusiness.com/industries/2014/01/31/twitter-buys-patents-seals-licensing-pact-with-ibm/ (describing agreement for Twitter to acquire 900 patents from IBM, settle patent infringement litigation, and cross license patents); *Microsoft Says Samsung Owes It $6.9 Million in Contract Dispute*, RECODE.NET (Oct. 3, 2014), http://recode.net/2014/10/03/microsoft-says-samsung-owes-it-6-9-million-in-contract-dispute/ (describing litigation to enforce September 2011 cross-licensing agreement for mobile-related patents).

[27] *See, e.g.*, U.S. Dep't of Justice & Federal Trade Comm'n, Antitrust Guidelines for the Licensing of Intellectual Property § 3.2 (1995), *available at* http://www.justice.gov/atr/public/guidelines/0558.htm (describing agency approach to analyzing competitive effects in technology and innovation markets where IP licensing may affect competition to develop new or improved goods or processes).

[28] *See, e.g.*, Food and Drug Administration, U.S. Department of Health and Human Services, Intent to Exempt Certain Class II and Class I Reserved Medical Devices from Premarket Notification Requirements (Aug. 1, 2014), *available at* http://www.gpo.gov/fdsys/pkg/FR-2014-08-01/html/2014-18198.htm (notice of draft guidance to exempt certain mobile device health apps from FDA premarket 510(k) review requirements).

[29] *See, e.g.*, Julie Brill, Comm'r, Fed. Trade Comm'n, The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control 6–7, Presented at Fordham University School of Law Center on Law and Information Policy, What is Your Car Saying to Your Shoes? Assessing the Internet of Things (Mar. 14, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/289531/140314fordhamprivacyspeech.pdf (promoting practices that include privacy by design (i.e., incorporating privacy protections in the design of IOT products and the internal operations of suppliers), de-identification of data outputs, and transparent and readily accessible privacy notices for consumers who use IOT products); *see also* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent*, TEX. L. REV. (forthcoming), *available at* http://ssrn.com/abstract=2409074 (analyzing problems with discrimination, privacy, security, and consent for use of data,

due to inherent traits of consumer IOT products (i.e., compounding effects of "sensor fusion" that promotes uses for data outputs beyond a particular IOT product's original use, near impossibility of truly de-identifying data, likelihood of security flaws, difficulty of meaningful consumer consent for some or all data uses), and proposing regulatory actions to address these problems).

30 *See* TRENDnet, Inc., FTC File No. 122 3090 (Sept. 4, 2013) (complaint and proposed consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter (FTC challenge to security firm's software design and testing of IP-connected security cameras that allegedly allowed hacker to access live feeds from 700 cameras and make them available on the Internet).

31 Similar efficiencies have been suggested to favor using key network interfaces with consumers as a focal point for disclosures about collection and use of personal data by IOT products and for customer control of privacy settings and permission for use. *See, e.g.*, FTC IOT Workshop, Comments of Center for Democracy and Technology 11 (Jan. 10, 2014), *available at* http://www.ftc.gov/policy/public-comments/comment-00016-34 ("Configuring an increasing quantity of network-enabled IoT devices could easily become quite daunting. Accordingly, it may be more usable and practical for users to configure IoT privacy controls at the network level. That is, a network-monitoring device could be designed for IoT environments that would allow a homeowner to block or allow certain kinds of communication both within the home and externally to the Internet."); Julie Brill, Comm'r, Fed. Trade Comm'n, Weaving a Tapestry to Protect Privacy and Competition in the Age of Big Data 4–5, Presented at the European Data Protection Supervisor's Workshop on Privacy, Consumer Protection and Competition in the Digital Age (June 2, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/313311/140602edpsbrill2.pdf (describing legislative proposal to establish a central portal for data brokers to identify themselves, describe their information collection and use practices, and provide links to access tools and opt outs and to use reasonable procedures to ensure that their clients do not use the broker's products for unlawful purposes). Potential tensions between consumer protection and antitrust standards may arise if key consumer interfaces of this type develop as part of a closed business model for IOT products and rival suppliers are restricted from using the interface to disclose data practices and facilitate customer control.

32 *See, e.g.*, Janet Wagner, *The Twitter API: Still an Open Platform?*, PROGRAMMABLE WEB (July 9, 2012), http://www.programmableweb.com/news/twitter-api-still-open-platform/2012/07/09 (describing change in Twitter business practices to restrict use of Twitter API in software developers' Web and mobile applications).

33 *See, e.g.*, Joshua D. Wright, Comm'r, Fed. Trade Comm'n, Remarks at The Economics of Digital Consumer Protection: One Commissioner's View 17–21, TechFreedom and International Center for Law and Economics, Washington, D.C. (July 31, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/573061/010731techfreedom.pdf (commenting on need for careful cost benefit analysis on business practices of data brokers, and with multi-sided markets and software platforms); Maureen K. Ohlhausen, Comm'r, Fed. Trade Comm'n, Promoting an Internet of Inclusion: More Things AND More People 1–2, Consumer Electronics Show (Jan. 8, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/promoting-internet-inclusion-more-things-more-people/140107ces-iot.pdf (commenting that success of the Internet has been driven by freedom to experiment with different business models; noting importance of approaching new technologies with a dose of regulatory humility, by analyzing effects on consumers and the marketplace, and carefully considering whether existing laws and regulations are sufficient to address harms that arise before assuming that new rules are required); Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Opening Remarks, FTC Workshop, The Internet of Things: Privacy and Security in a Connected World 3–4 (Nov. 19, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/opening-remarks-ftc-chairwoman-edith-ramirez-federal-trade-commission-internet-things-privacy/131119iotremarks.pdf (describing best practices to protect consumer rights on the IOT, consisting of privacy by design, simplified consumer choice for control of personal data usage, and transparency in disclosures about data collection and usage).