Internet Association

National Telecommunications and Information Administration,
U.S. Department of Commerce,
1401 Constitution Avenue NW,
Room 4725,
Attn: IOT RFC 2016,
Washington, DC 20230

June 2, 2016

**The Benefits, Challenges, And Potential Roles For The Government In Fostering The Advancement Of The Internet Of Things**

**Docket No. 160331306–6306–01**

The Internet Association (IA) welcomes the opportunity to provide comments to the Department of Commerce (DoC) on this timely and important issue. The IA also welcomes the manner in which the DoC has framed its Request for Comments so as to "capitalize on the Department's experience and holistic economic perspective to craft an approach to IoT and its potential impacts that will best foster IoT innovation and growth."[1] Similarly, IA members support an approach in Congress that plans for and encourages "the proliferation of the Internet of Things in the United States."[2]

NTIA and other government actors should facilitate the continued success of the US Internet economy as the Internet of Things expands in the coming years. From a technological standpoint, the Internet of Things marks as much an evolution as a revolution in how the Internet is deployed. For this reason, new, wholesale public policies and regulations are not needed in this space. Instead, government efforts should be directed at facilitating a comprehensive audit of existing rules, requirements, and policies. New laws and regulations should only be contemplated after the audit is complete, and even then only as absolutely necessary and narrowly tailored to fill in critical gaps.

[1] Department of Commerce, Request for Comment, 81 Fed. Reg. 19956 (Apr. 6, 2016) ("RFC"),

[2] DIGIT Act, S. 2607, 114th Cong. (2016), https://www.congress.gov/114/bills/s2607/BILLS-114s2607is.xml.

The approach from DoC to the Internet of Things is consistent with decades of successful, flexible policy approaches to the Internet. In the 1990s, the U.S. government adopted landmark policies that fostered the nascent Internet's growth. These enlightened policies included, for example, the 1993 White House blueprint for building an "Information Superhighway,[3] as well as the safe harbors created for online intermediaries in Section 230 of the Communications Decency Act[4] and Section 512 of the Digital Millennium Copyright Act.[5]

Of particular relevance to the DoC's present inquiry, over the past 20 years, U.S. privacy and data security laws have enabled innovation and growth while protecting consumers. Similarly, the historic U.S. approach to standardization and interoperability that supports a bottom up, industry-led and consensus-driven process was key to the Internet's growth and success. The common denominator of these policies is clear: **in contrast to other jurisdictions, U.S. Internet policies have proven flexible enough to support innovation and growth yet robust enough to meet important consumer protection and other public policy goals.**

In turn, these U.S. policies have played a significant role in making the U.S. Internet industry a world leader. According to a recent Internet Association study, the Internet industry represented 6 percent of real U.S. GDP in 2014 (over $900 billion).[6] Importantly, these levels more than doubled Internet industries' real contributions from seven years earlier.[7] Beyond our borders, US policies also played a role in making the Internet the great American export of the 21st century. Today, the global Internet economy is somewhere in the neighborhood of $10 trillion US dollars and by the end of this year, half the world's population – about 3 billion people – will use the Internet.[8]

---

[3] *See* John Marjoff, *Building the Electronic Superhighway*, N.Y. Times, Jan. 24, 1993, http://www.nytimes.com/1993/01/24/business/building-the-electronic-superhighway.html?pagewanted=all.

[4] *See* 47 U.S.C. § 230.

[5] *See* 17 U.S.C. § 512.

[6] *Measuring the U.S. Internet Sector*, Internet Association, at 5, http://internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf.

[7] *Id.*

[8] *The Internet of Things*, Samuel Greengard, at 27, MIT Press (2015).

**Internet of Things: Benefits and Economic Impact**

The economic benefits from the growth of the Internet to date are expected to carry through to the Internet of Things. These benefits mirror those created by previous advances in the Internet and include:

- Economic growth;
- Lower costs for businesses; and
- Lower costs and increased choice for consumers.

The economic growth from the Internet of Things has been well documented. According to Cisco Systems, which has established an Internet of Everything (IoE) index, businesses already generate $613 billion of additional profits annually as a result of connected devices - but this represents only about 50 percent of the potential of the Internet of Things. The figure could reach $14.4 trillion in net profits within a decade, Cisco estimates.[9] In addition, the McKinsey Global Institute estimates the potential economic impact of the Internet of Things to be $3.9 trillion to $11.1 trillion per year by 2025.[10]

As with previous Internet advances, the Internet of Things will also deliver significant productivity gains and cost savings both to businesses and consumers. Within the industrial and commercial realm, the IoT will likely spawn huge productivity gains. For example, even a 1 percent reduction in fuel costs or similar improvement in capital expenditures of system inefficiency could produce savings in the tens of billions or hundreds of billions of dollars for industry. For consumers, home automation could result in huge energy costs savings.[11] Researchers at the University of Virginia estimate that a typical 20 to 30 percent energy reduction would result in savings of 100 billion kilowatts and $15 billion annually in the US alone.[12]

In its Request for Comments, DoC asks whether the government should measure the economic impact of the Internet of Things and how it might fit within existing industry classification systems.[13] In late 2015,

---

[9] *Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion*, Cisco, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf.

[10] *Unlocking the potential of the Internet of Things*, McKinsey & Company (June 2015), http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[11] *Industrial Internet: Pushing the Boundaries of Minds and Machines*, Peter C. Evans and Mark Annunziata, November 2012, http://www.ge.com/docs/chapters/Industrial_Internet.pdf

[12] *The Smart Thermostat: Using Occupancy Sensors to Save Energy in Homes*, http://www.alice.virginia.edu/~stankovic/psfiles/sensys10-final169.pdf.

[13] RFC at 19959.

the Internet Association published a study measuring the economic impact of Internet industries on the U.S. economy using the NAICs industry classifications. In the report, our economic expert, Steve Siwek, devised a bespoke methodology to capture the true and accurate value of the Internet economy using existing NAICS codes. To assess the extent that Internet activities were conducted in multiple NAICs codes, Mr. Siwek made use of "product line receipts" for multiple NAICs codes in 2007 and 2012. However, this degree of analysis would not have been necessary if the NAICs classification system had already been revised to report "Internet only" industries. In such industries, Internet activities would have remained separate and would not have been comingled with non-Internet activities.

With Internet-only NAICs accounts, measuring the size and economic importance of the Internet, including the Internet of Things, would be far less complicated than it is today. Although the Office of Management and Budget (OMB) through its Economic Classification Policy Committee (ECPC) has recently solicited comments on and issued proposed changes to the NAICs, the changes clarified but did not change the existing content of industries. As the Internet and the Internet of Things continue to grow in economic importance, this is a decision that OMB and other relevant agencies may wish to revisit.

**Internet of Things: Revolution Or Evolution?**

The inquiries in the DoC's Request for Comments underscore one important and overarching question: is there something unique about the Internet of Things such that new and bespoke public policies and regulations are needed?

Although some have described Internet of Things as the "Industrial Revolution 4.0,"[14] our members view the Internet of Things as the third *evolution* in the Internet's development. Internet Association members have been present at each inflection point along this timeline and are therefore well-placed to speak to these evolutions. Even in the Internet of Things context, our members have not only developed the hardware that connects the Internet to devices such as the Nest thermostat, Amazon's Echo, and the Oculus Rift, but they also provide the infrastructure that helps power the Internet of Things, namely cloud services.

Broadly speaking, the Internet's three evolutions to date are[15]:

- The first evolution, during which the Internet created the **information graph** that changed how we produce, access, share and generate knowledge. This evolution resulted in

---

[14] *See The Fourth Industrial Revolution: Things to Tighten the Link Between IT and OT*, Sogeti, 33

[15] *See IEEE: Internet of Things*, Vint Cerf (Dec. 15, 2015), http://wfiot2015.ieee-wf-iot.org/EMAIL%20VERSION-%20IoT%20Keynote%20-%20Vint%20Cerf%20-%20IEEE%20Milan%20-%20Dec%2015th%202015.pdf.

widespread access to and ubiquity of content online;

- The second evolution, during which social media created the **social graph** that changed how we establish and foster relationships with one another. This evolution enabled power to the crowd; and

- The Internet of Things that is creating the **physical graph,** which in turn is changing how we interact with objects and environments**.** This evolution is resulting in adaptive environments that understand context and adjust accordingly.

Although these three evolutions mark distinct and different ways through which we interact with the Internet, the Internet's core function remains relatively unchanged, even in an Internet of Things world. As one expert puts it, from an engineering standpoint, "the Internet serves as the electrical wiring for the IoT. It makes real-time communications and data sharing possible on a mass scale."[16] In this sense, its function in the Internet of Things space is no different from its function on social media or for the sharing economy.

**Privacy And Data Security In An Internet of Things World: Balancing Flexibility And Robust Consumer Protections**

Although the Internet of Things marks an evolution as opposed to a revolution, there is a broad consensus that it marks a sea change in the volume, velocity, and variety of data on the network (the so-called "Three Vs" of big data), as well as the sources of that data. Machine-generated data currently accounts for only 15 per cent of overall data. However, experts estimate that the figure will likely rise to around 50 percent within the next decade. Alongside this volume increase, connected devices will deliver increased variety in network data, such as parameter readings, usage information, operator behavior, and patient condition and health monitoring.[17]

These changes will create a greater need for flexible but robust approaches to online privacy and data security. In order for the economic benefits of the Internet of Things to be realized, privacy and data security practices will need to be robust enough to foster trust between consumers and device makers. At the same time, approaches to privacy and data security must also be flexible enough to allow for continued innovation in the Internet of Things space.

The correct balance between flexibility and robustness can be challenging to strike. Fortunately, the US Internet industry and government have proven adept at striking this balance in the past, and the essential

[16] *Supra,* note 8 at xvi.

[17] *Id.* at 59.

building blocks needed to establish end-user trust are already available. These building blocks include encryption technology; industry best practices for transparency in data use practices and data security; and the Federal Trade Commission's time-tested, comprehensive policy and enforcement frameworks.

Government support for encryption technology, both for data in transit and at rest, will certainly be a major part of the solution to ensuring adequate data security in an Internet of Things world. On the Internet, privacy and security increasingly are safeguarded through strong encryption, and the record shows that it works: recent data breaches – both in the public and private sectors - have happened because firms failed to encrypt their customers' data, not because hackers broke through strong protections. By extending encryption down to the level of individual devices, the owners of those devices have gained a new kind of control over their personal information.[18]

The US government understands the cyber threat and the benefits of strong encryption in countering it. Three years ago, the President issued an Executive Order finding that cyber threats to critical infrastructure represent one of the most serious national and economic security challenges to our nation.[19] The White House's National Security Council has also spotlighted cyber threats to the Internet economy, warning that "[p]ervasive criminal activity in cyberspace not only directly affects its victims, but can imperil citizens' and businesses' faith in these digital systems, which are critical to our society and economy."[20] Similarly, FBI Director Comey has told the Senate Judiciary Committee that "[t]he development and robust adoption of encryption is a key tool to secure commerce and trade, safeguard private information, promote free expression and association, and strengthen cyber security."[21] Importantly, technologists within the FBI also understand and support this viewpoint, with Director Comey's Assistant Director for Science and Technology testifying last year, "we in the FBI support and encourage the use of secure networks and sophisticated encryption to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data."[22]

In addition to strong encryption, the Internet Association's members support bottom-up industry best

---

[18] *See* Neil Gershenfeld & JP Vasseur, *As Objects Go Online*, Foreign Affairs (Mar./Apr. 2014), https://www.foreignaffairs.com/articles/2014-02-12/objects-go-online.

[19] Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 12, 2013).

[20] *Strategy to Combat Transnational Organized Crime* (2011), Executive Summary at II, https://www.whitehouse.gov/administration/eop/nsc/transnational-crime.

[21] James B. Comey, Dir., FBI, *Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee* (Jul. 8, 2015).

[22] Amy Hess, Exec. Assistant Dir. Sci & Tech. Branch, FBI, *Statement Before the House Oversight and Government Reform Committee, Subcommittee on Information Technology* (Apr. 29, 2015).

practices to enhance privacy and data security. The guiding principles in these industry efforts are transparency and user control. Internet Association members design transparent data use policies based on feedback from users, regulators, and other stakeholders, recognizing that we live in a world in which no one-size-fits-all approach to privacy will satisfy every person's expectations. Giving users clear and easy data management controls elicits greater trust and confidence in end-users, which is why Internet Association members continuously refine their cutting-edge tools in response to end user feedback.

Although industry best practices in privacy and data security will play a role as the Internet of Things matures, government plays an important role as both "privacy arbiter"[23] and backstop enforcer. Since the late 1990s, the FTC has served as the nation's *de facto* data protection authority. The agency has used its broad authority under Section 5 of its enabling statute, which prohibits "unfair or deceptive acts or practices in commerce" to address alleged violations of data privacy and security standards. As privacy scholars Bamberger and Mulligan have noted "since 1996 the FTC has actively used its broad authority under Section 5 [] to take an active role in the governance of privacy protection, ranging from issuing guidance regarding appropriate practices for protecting personal consumer information, to bringing enforcement actions challenging information practices alleged to cause consumer injury."[24]

FTC privacy and data security enforcement actions – which result primarily in publicly available consent decrees – bind individual companies to lengthy, twenty-year privacy audits and potential liability of up to $16,000 per customer harmed per violation. Beyond individual companies, these enforcement actions also serve as precedent to the rest of the market. For this reason, FTC consent decrees have been identified as the nation's 'common law' of privacy.[25]

Applying these privacy and data security norms in the IoT context is an issue the FTC examined in recent years at a public workshop and follow on staff report.[26] The FTC report focused on the application of four Information Privacy Practice Principles (FIPPs) the IoT space, namely (1) data security; (2) data minimization; (3) notice and (4) choice.[27] Participants and FTC staff also discussed whether new and bespoke legislation is needed to cover IoT, and concluded that it was not.[28]

---

[23] Katy Bachman, *FTC Chair Edith Ramirez Fights for Data Security and Privacy Rights*, Adweek (May 27, 2014), http://www.adweek.com/news/television/ftc-chair-edith-ramirez-fights-data-security-and-privacy-rights-157930.

[24] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*, 69 (2015).

[25] Woodrow Hartzog and Daniel J. Solove, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2013).

[26] *Internet of Things, Privacy & Security in a Connected World*, FTC Staff Report, January 2105. The report is limited to a discussion about IoT devices sold to or used by consumers and does not address machine-to-machine communications, e.g. RFID.

[27] *Id.* at ii.

With respect to data security, the FTC staff in the IoT report lauded the benefits of security by design and gave favorable mention to the use of encryption to secure sensitive data in transit and at rest, in particular for data passing over consumers' home wifi networks.[29] As described in the staff report, both security by design and encryption had previously been road tested in the FTC's first IoT specific enforcement action, TRENDnet. [30]

Following its IoT report, the FTC went on to reinforce its encryption message in last year's "Start with Security"[31] guidance and series of regional workshops in which the agency counseled businesses to, among other measures, "use strong cryptography to secure confidential material during storage and transmission."[32]

**Standardization And Interoperability In An Internet Of Things World**

The Internet 1.0 was built innovation facilitated by open standards and interoperability. As Internet Founding Father Vint Cerf explains "[t]he principal goal" in the Internet's early days "was to create a way for companies to communicate with one another." In so doing, Cerf and others did not want to repeat the mistakes of past eras. As he relays in the same interview "[w]e certainly didn't want to wind up with a situation parallel to the 1930s and 1920s when business had a dozen different telephones sitting on a desk – all using a different proprietary system and requiring a person to know which telephone service to use to reach someone else." In order to avoid these inefficiencies, the early Internet settled on Cerf's TCP/IP protocol that allowed computers and various networks to seamlessly interconnect. [33]

Today, one of the primary roadblocks on the path to a more robust and all-encompassing Internet of Things is a battle over protocols and standards where they are needed. Within one vertical alone – domestic connected devices - existing protocols are fragmented in a way that is confusing to consumers and businesses. In order for the Internet of Things to emulate the success of previous Internet evolutions,

---

[28] *Id.* at vii.

[29] *Id.* at 30.

[30] In the matter of TRENDNet, Inc, FTC File No. 122 3090, https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter

[31] *Start with Security: A Guide for Business,* June 30, 2015, https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

[32] *Id.*

[33] Interview with Vinton Cerf for America West magazine in 1999. Quoted by Greengard, *supra* note 8.

work must continue to standardize technologies while allowing consumers to reap the full benefits of competition and consumer choice. Beyond the consumer benefits that standards can deliver, standardization will also be important for non-traditional Internet companies as well as startups entering the Internet of Things space. Standards will lower entry barriers, allowing non-traditional companies and startups to build viable and competitive businesses over time. [34]

The need for standards and interoperability in an Internet of Things world is not in dispute. The question is more whether there are existing models that can be tapped into to achieve these goals and what principles that should guide those models. In fast-moving technology markets, the IA supports a standard-setting model that is private sector-led, open, voluntary, consensus based, and nimble. While government has a role to play in encouraging industry standards and interoperability, the work itself should be driven by industry. Helpfully, OMB long ago recognized the importance of this standard-setting model in updated Circular A-119.[35]

The Internet Association also encourages the U.S. Government to promote this approach to standard-setting overseas as well as here at home. Internet markets are global markets and the need for technical interoperability in such markets is particularly acute. Commerce Secretary Pritzker recently appointed digital attaches[36] in several key jurisdictions overseas; the Internet Association submits that monitoring standard-setting policies and forums overseas could become a key metric for these attaches over time.

**Patent Litigation and the Internet of Things**

The Internet of Things presents a number of challenges for the patent system including abusive patent assertion entity (PAE) litigation and the looming threat that this litigation could proliferate to include design patents. Abusive PAE litigation has long since been an issue of concern to the Internet Association and, as the IoT matures and expands into new sectors, patent litigation will likely proliferate. Absent legal or policy changes to tackle these issues, PAEs could shut the door on an open platform for promoting innovation in the digital economy, economic growth, and opportunity.

PAE activity has been well documented elsewhere and there is little reason to think that it will not become a feature of the IoT patent litigation landscape in due course. According to a White House report, PAEs "focus on aggressive litigation, using such tactics as: threatening to sue thousands of

[34] *Supra,* note 14.

[35] Circular No. A-119 Revised, February 10, 1998, Office of Management and Budget, https://www.whitehouse.gov/omb/circulars_a119/

[36] Commerce Secretary Pritzker Launches Digital Attache Program to Address Trade Barriers, March 11, 2016, https://www.commerce.gov/news/press-releases/2016/03/us-secretary-commerce-penny-pritzker-launches-digital-attache-program

companies at once, without specific evidence of infringement against any of them; creating shell companies that make it difficult for defendants to know who is suing them; and asserting that their patents cover inventions not imagined at the time they were granted." [37] According to 2015 data, patent litigation involving PAEs was at record high levels. About two-thirds of patent lawsuits are filed in the high-tech sector and, of these high-tech cases, more than 88 percent involved PAEs. Many of the patents asserted by PAEs are of very poor quality. [38]

The economic impact of PAE activity on high-tech companies is severe, but the activity impacts smaller companies even more severely. More than half of the firms sued by trolls have less than $10 million in annual revenue. [39] These victims lack the resources to fight in court, even if they have a valid case. One study found that the average troll settlement costs a small or medium sized company $1.33 million, versus $1.75 million per case for an in court defense. Startups - including IoT startups - are doubly impacted by PAE activity, both as small businesses defending these lawsuits and also as businesses seeking to attract venture capital funding. One study investigated the indirect costs of patent litigation and found that litigation by frequent litigators—such as patent trolls—is associated with a direct and negative effect on innovation. VC investment over the last five years "would have likely been $21.7 billion higher [] but for litigation brought by frequent litigators." [40]

The Internet Association continues to call for comprehensive patent reform from all branches of government. Action is needed, and we ask the administration to support initiatives including:

- Legislation that would curb the negative effects of PAE activity on our economy;
- Comprehensive action by the Patent and Trademark Office to improve the quality of patents the agency issues;
- Case law development by the courts that would invalidate vague and overbroad patents that try to claim every possible way to achieve a stated function using software.

In addition to current PAE activity, the over protection of design patent rights may inhibit IoT development and deployment. The Internet Association is very concerned that the epidemic of PAE

---

[37] *Patent Assertion and U.S. Innovation,* EOP Report, at 1 (June 2013)
https://www.whitehouse.gov/sites/default/files/docs/patent_report.pdf

[38] "Trolls made 2015 one of the biggest years ever for patent law suits", Arstechnica, January 5, 2015,
http://arstechnica.com/tech-policy/2016/01/despite-law-changes-2015-saw-a-heap-of-patent-troll-lawsuits/

[39] RPX, 2014 NPE Litigation Report,
http://www.rpxcorp.com/wpUcontent/uploads/sites/2/2015/03/RPX_LitigationUReportU2014_FNL_040615.pdf

[40]Tucker, Catherine, The Effect of Patent Litigation and Patent Assertion Entities on Entrepreneurial Activity (2014),
http://cdn.arstechnica.net/wp content/uploads/2014/06/TuckerUReportU5.16.14.pdf

litigation will soon expand to embrace design patents with even more devastating results. The Federal Circuit recently held[41] that although a design patent may cover only a minor aspect of a device (e.g., the appearance of a corner or an icon), the patent owner is entitled to the infringer's *total* profit on the entire device. The ruling makes no economic sense as it gives the patent owner a windfall far out of proportion to the value of the design. Unless this rule is corrected, either by the Supreme Court in the upcoming Samsung v. Apple case or by legislation, a PAE with a design patent can demand all of a company's profits on any product, thereby chilling R&D and the creation of new products.

**Conclusion**

The Internet Association thanks the DoC for the opportunity to submit comments on this important and growing part of the U.S. economy. The Department is to be commended for its "holistic economic perspective" and for seeking "to craft an approach to IoT and its potential impacts that will best foster IoT innovation and growth."[42] We look forward to continued dialogue with DoC and other stakeholders regarding how best to strike this balance.

Respectfully submitted,

Michael Beckerman
President & CEO
The Internet Association

[41] *Apple v. Samsung Electronics Co., Ltd.*, No. 14-1335, 15-1029, slip op. at 21 (Fed. Cir. May 18, 2015).

[42] *Supra,* note 1.