March 13, 2017

Attn: IOT RFC 2017
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, District of Columbia 20230

RE: Comments of ACT | The App Association to the National Telecommunications and Information Administration regarding *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (Docket No. 170105023–7023–01)

ACT | The App Association writes to provide input to the National Telecommunications and Information Administration (NTIA) in response to its request for public comment (RFC) on its green paper, "Fostering the Advancement of the Internet of Things,"[1] which lays out an approach and areas of engagement for the Department of Commerce's possible future work on the Internet of Things (IoT).[2]

The App Association represents more than 5,000 app companies and technology firms that create the apps used on mobile devices around the globe. As the world has quickly embraced mobile technology, our member companies have been creating innovative solutions that power the growth of IoT across modalities and segments of the economy. We applaud NTIA's efforts to understand IoT and to explore ways in which the federal government can help the United States fully realize the immense benefits of IoT. The App Association submitted detailed comments[3] to NTIA in mid-2016 to support NTIA's creation of the Green Paper, and appreciate consideration of those comments and our views expressed in this communication.

I. ACT | The App Association's General Reactions to the IoT Green Paper

The App Association appreciates NTIA's extensive efforts to examine new approaches and areas of engagement for the Department of Commerce regarding the IoT. As we noted in our initial comments to

[1] Department of Commerce, *Fostering the Advancement of the Internet of Things* (Jan. 2017), *available at* https://www.ntia.doc.gov/other-publication/2017/green-paper-fostering-advancement-internet-things (Green Paper).

[2] *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 82 Fed. Reg. 4313 (January 13, 2017) (RFC).

[3] Comments of ACT | The App Association, Docket No. 160331306–6306–0 (filed June 2, 2016), *available at* https://www.ntia.doc.gov/files/ntia/publications/act_comments_re_ntia_iot_green_paper_060216.pdf (App Association Comments). These are also appended to this filing.

NTIA, we believe that the Department of Commerce is well-positioned to serve as a leader and coordinator within the U.S. government with respect to realizing the potential of the IoT. The completion of this Green Paper takes an important step in establishing this role.

The App Association believes that the Green Paper represents an inclusive and deliberate investigation of the appropriate role of the U.S. government in realizing an IoT-enabled future and we support its strong policy commitments, namely that the IoT environment is (1) inclusive and accessible in both the consumer and enterprise contexts; (2) stable, secure, and trustworthy; (3) interoperable based on industry-driven consensus technical standards; and (4) not unnecessarily inhibited by barriers to entry. As such, the App Association does not believe there are any significant changes with respect to the "areas of engagement" discussed in the Green Paper.

We also appreciate the extensive commitments that NTIA has proposed for the Department of Commerce in the Green Paper. Many of the proposed activities are a continuation of widely-supported activities and/or can (and should) be driven by the range of stakeholders in the IoT ecosystem. Overall, the App Association is supportive of NTIA's proposed next steps (and offer some further suggestions for improvement below).

II. ACT | The App Association's Specific Recommendations to NTIA on Improving the IoT Green Paper

Highlighting our support for NTIA's work product in the Green Paper and noting our appreciation to provide further suggestions, we offer the following proposals to NTIA and urge for changes to be made to the Green Paper accordingly:

- From a definitional perspective, in our comments to NTIA to inform the Green Paper, the App Association discussed our views on the term "Internet of Things," describing it as a concept of enhanced connectivity across consumer and enterprise contexts.[4] Because the incorporation of IoT applications is (and will increasingly) touch each and every segment of the economy, we are troubled by references in the Green Paper to the IoT as a "sector"[5] (and in another portion of the Green Paper, to the plural "IoT sectors"[6]). We fear that by referring to the IoT as a "sector" it may be interpreted by some reading the Green Paper as one that is distinct from one or more of economy sectors that the IoT will improve (e.g., healthcare, transportation, etc.). Consequently, we recommend that the Green Paper remove references to the IoT "sector" or IoT "sectors."
- In describing the IoT and its benefits to the U.S., we urge the Green Paper to explore the potential of the IoT's rise to fuel job creation, particularly for American small businesses (including small business software development companies that the App Association represents). While we believe that NTIA appreciates this, we do not find that it has been adequately described in the Green Paper's text aiming to capture the IoT landscape.

[4] *See* App Association Comments at 1-2.

[5] NTIA IoT Green Paper at 51.

[6] NTIA IoT Green Paper at 40.

- We believe that NTIA and the Department of Commerce understand and appreciate the vital role competition will play in the success of the IoT, and the limits of U.S. agency authority across areas of responsibility. As far as U.S. government action, the App Association believes that the Green Paper should contain an unambiguous policy recommendation that any government action, whether *ex ante* or *ex* post, be conditioned on the establishment of a clear data-driven evidence base. Government actions (or reactions) based on hypothetical and/or anecdotal harms will pose a significant threat to the innovation in the app ecosystem that will drive the growth of the IoT. We strongly urge NTIA to ensure that the Green Paper contain a strong commitment to this concept, which would send a clear and inviting signal to innovators regarding U.S. government approach to the IoT.
- We appreciate NTIA's discussion of the role of industry-led and consensus-based technical standards in the success of the IoT,[7] and specifically the role of patents within these crucial standards.[8] In previous comments to NTIA in mid-2016, we provided detailed discussion about the critical role of patents in these standards and the need for reasonable access to these patents in order to properly utilize standards that will be the foundation of the IoT.[9] While NTIA discusses various viewpoints on this topic in the Green Paper, its only related proposed activity is to "[w]ork to promote the positive evolution of intellectual property and its protection in the digital economy."[10] We encourage the Green Paper to make a commitment to the success of standards in the IoT's growth *as well as* reasonable access to patents in standards when owners of the same have voluntarily committed to limit their ability to exclude implementers from use.

III. Conclusion

The App Association appreciates the opportunity to provide input on the Green Paper, and encourages the Department of Commerce to consider action consistent with the above.

Sincerely,

Morgan Reed
Executive Director
ACT | The App Association

[7] *See* NTIA IoT Green Paper at 44-48.

[8] *See* NTIA IoT Green Paper at 36.

[9] The App Association will not restate its views on this issue, which we describe in detail in our comments to NTIA to inform the content of the IoT Green Paper. *See* App Association comments at 6-10.

[10] NTIA IoT Green Paper at 44.

June 2, 2016

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

RE: Comments of ACT | The App Association to the National Telecommunications and Information Administration regarding *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (Docket No. 160331306–6306–0)

ACT | The App Association writes to provide input to the National Telecommunications and Information Administration (NTIA) on its request for public comment (RFC) on the potential benefits and challenges of Internet of Things (IoT) technologies and the role the U.S. government should play in its success.[1]

ACT | The App Association represents more than 5,000 app companies and technology firms that create the apps used on mobile devices around the globe. As the world has quickly embraced mobile technology, our member companies have been creating innovative solutions that power the growth of IoT across modalities and segments of the economy. We applaud NTIA's efforts to understand IoT and to explore ways in which the federal government can help the United States fully realize the immense benefits of IoT. These comments address some of the questions raised in the RFC.

I. The Internet of Things and its Potential

The IoT is an encompassing concept where everyday products use the internet to communicate data collected through sensors. IoT is expected to enable improved efficiencies in processes, products, and services across every sector. In key segments of the U.S. economy, from agriculture to retail to healthcare and beyond, the rise of IoT is demonstrating efficiencies unheard of even a few years ago. The IoT is projected to be worth more than $947 billion by 2019.[2]

[1] *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 81 Fed. Reg. 19956 (April 25, 2016) (RFC).

[2] "Internet of Things Market and M2M Communication by Technologies, Platforms and Services (RFID, Sensor Nodes, Gateways, Cloud Management, NFC, ZigBee, SCADA, Software Platform, System Integrators), by M2M

The real power of IoT comes from the actionable information gathered by sensors embedded in every connected device. IoT devices are useful in direct consumer interactions, but will see the largest value in how the data becomes part of what is now commonly referred to as "big data." For this document, we define this term to mean structured or unstructured data sets so large or complex that traditional data processing applications are not sufficient for analysis. As sensors become smaller, cheaper, and more accurate, big data analytics enable more efficiencies across consumer and enterprise use cases.

IoT deployment will be highly use case-dependent. The technology industry, to date, has done well through open Application Programming Interfaces (APIs) and other widely-adopted standards (e.g., TCP/IP) to enable interoperability. For example, in healthcare, a miniaturized and embedded connected medical device must be able to automatically communicate bi-directionally in real-time. This capability enables a healthcare practitioner to monitor a patient's biometric data as well as for the patient to be able to communicate with a caregiver in the event of a medical emergency. Other uses, such as sensors deployed to alert security of an unauthorized presence, may only require the ability to send data to security professionals with minimal (or even no) capability to receive communications.

The app industry has been in existence less than a decade, and has experienced explosive growth alongside the rise of smartphones. As we detail in our annually-released *State of the App Economy* report,[3] apps have revolutionized the software industry, touching every sector of the economy. The app economy is a $120 billion ecosystem today that is led by U.S. companies, the vast majority of which are startups or small businesses. While IoT devices encompass every fathomable object in our lives, the interface for communicating with these devices is likely to remain a mobile app on a smartphone. The rise of IoT will hinge on the app economy's continued innovation, investment, and growth. In short, apps are the interface for IoT revolution.

While many definitions of IoT have been put forward since the term was coined in the late 1990s,[4] a universal definition has not yet emerged. Should NTIA move forward with defining IoT, we urge them to ensure that this definition reflects the encompassing scope of IoT both from a use case and technology perspective. If the U.S. government definitions and policies related to IoT translate to the government "locking in" particular technologies (whether directly or effectively), it will be deeply damaging to the United States' role in the rise of IoT, as no one can predict what shape future successful deployments will take in response to marketplace trends and competition. At the same time, however, it is also important that the Department of

---

Connections and by IoT Components - Global Forecasts to 2019," MarketsandMarkets (November 2014), *available at* http://www.marketsandmarkets.com/Purchase/purchase_report1.asp?id=573.

[3] ACT | The App Association, State of the App Economy 2016 (Jan. 2016), available at http://actonline.org/state-of-the-app-economy-2016/.

[4] Kevin Ashton, "That 'Internet of Things' Thing, in the real world things matter more than ideas," RFID Journal, June 22, 1999.

Commerce provide a generally accurate description of IoT for the community of impacted stakeholder.

II. A Coordinated USG Approach to IoT

To realize the full potential of IoT, the coordination of federal agencies is essential. When considering entry into a new market, app makers must understand the regulatory environment. A lack of harmony between federal regulatory agencies, states, and even localities creates uncertainty and damages the hypercompetitive app economy where time to market is critical. Due to the rise of the app economy across industries and use cases, countless agencies play key roles in empowering the future of mobile apps and therefore IoT. Agency coordination will not only help avoid duplicative or conflicting regulations and parallel efforts, but it will also help agencies ensure that inquiries into opportunities and actions are well-informed.

ACT | The App Association is committed to working in partnership with the U.S. government and other stakeholders towards a coordinated approach to enable IoT. For example, we strongly support the Developing Innovation and Growing the Internet of Things (DIGIT) Act introduced by Senators Fischer, Ayotte, Booker, and Schatz, which would utilize an open and consultative process to bring forward key recommendations to Congress on how to appropriately plan for and encourage the proliferation of IoT in the United States.[5]

The planned Green Paper presents the Department of Commerce with a unique and appropriate opportunity to position itself as a coordinator of other agencies, building on a successful track record. For example, in addition to statutory roles related to electronic health records,[6] standards coordination,[7] and information security standards and guidelines for federal agencies,[8] the National Institute of Standards and Technology (NIST) led in the development of the Cybersecurity Framework[9] and the National Strategy for Trusted Identities in Cyberspace (NSTIC).[10] We urge that the IoT Green Paper reflect the need for a coordinated and harmonized U.S. government approach to the deployment of IoT.

---

[5] http://actonline.org/2016/03/01/digit-act-is-crucial-step-in-ensuring-u-s-iot-leadership/

[6] NIST's roles in this context have been articulated in both Federal Health IT strategic plans (2008–2012 and 2011–2015) and in the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009.

[7] Under the National Technology Transfer and Advancement Act (NTTAA), NIST manages assigned responsibility to coordinate federal, state, and local technical standards and conformity assessment activities, as well as coordinates with those in the private sector.

[8] Title III of the E-Government Act of 2002 (P.L. 107-347).

[9] http://www.nist.gov/cyberframework/index.cfm.

[10] http://www.nist.gov/nstic/.

III. Data Security and Privacy

While the rise of the Internet of Things holds great promise, it also raises more security threats due to a broadened attack vector, necessitating more evolved and dynamic risk management practices. No data is more important to Americans than their own personal information. Our members appreciate this and put extensive resources into ensuring the security and privacy of end user data to earn and maintain the trust the market demands.

For example, fully leveraging technical measures including end-to-end encryption is a critical element to protecting data broadly, enabling key segments of the economy—from banking to national security to healthcare—by protecting access to, and the integrity of, data. Encryption's role should not be understated – without encryption, entire economies and industries are put at a significantly heightened risk of their data being compromised. NIST itself currently plays an important role in promoting the use of encryption. NIST's Computer Security Resource Center (CSRC) facilitates broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia.[11] NIST also provides the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-1 Security Requirements for Cryptographic Modules and other FIPS cryptography-based standards.[12]

Despite the important role encryption plays and the Department of Commerce's related responsibilities, some interests persist in demanding that "backdoors" be built into encryption for the purposes of lawful access. We reject such proposals as mandates that degrade the safety and security of consumers. Worse still, these "backdoors" could create vulnerabilities that state-backed hackers and criminals can exploit. ACT | The App Association strongly believes that the IoT Green Paper should recognize the vital role encryption and other technical measures play in securing the data that makes IoT so invaluable and commit to preserving the availability of these tools.

Public-private partnerships are a useful vehicle for cooperation on ways to confront both current and emerging cyber-based threats, and facilitate the ability to rapidly change in response to ever-developing risks. We are committed to working collaboratively with all public and private stakeholders in these fora to ensure a secure cyberspace. For example, the App Association co-chairs the Federal Communications Commission's (FCC) Commission Communications Security, Reliability, and Interoperability Council (CSRIC) Working Group 6 which has developed "security-by-design" recommendations and best practices for securing

[11] *See* http://csrc.nist.gov/.

[12] *See* http://csrc.nist.gov/groups/STM/cmvp/.

the core communications network[13] and continues to develop voluntary assurance mechanisms around these recommendations and best practices.

Additionally, the voluntary timely sharing of cybersecurity threat indicators among organizations from both the public and private sector will be crucial in the detection, mitigation, and recovery of cybersecurity threats, particularly with the rise of IoT. These organizations, from the most formal to those more loosely organized, can be of assistance to those looking to improve their cybersecurity posture through the sharing of threat information. For example, Information Sharing Analysis Organizations (ISAOs), which are envisioned in Executive Order 13691[14] to be formed to fill needs for unique communities large and small, sometimes across economic segments. ISAOs, as a complement to Information Sharing Analysis Centers (ISACs), are expected to help to address the resource limitations of small businesses as well as the convergence of business models that may make it difficult to determine the best way to engage in information sharing. We encourage the IoT Green Paper to ensure that these key fora are included in its guidance to federal agencies and stakeholders at large.

Further, small app companies and connected device makers are increasingly threatened by cyber attacks. With fewer resources than larger entities, small companies need clear guidance on where and how to share cyber threat information. Other key NIST efforts, such as the NIST Cybersecurity Framework[15] (and others influenced by NIST's approach) have embraced a scalable cybersecurity risk management approach which lends to a feasible approach by smaller entities. As the digital economy continues to expand, powered by smaller organizations that develop software apps, fluid bi-directional sharing of information between and among these entities and the government will be crucial.

Finally, end user education is a crucial aspect of improving cybersecurity in IoT because many cyber-based attacks are preventable. We therefore urge that the IoT Green Paper address how the U.S. government can inform end users across the business and consumer communities of steps to take to ensure that proper cyber "hygiene" is practiced.

---

[13] *See* https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability#block-menu-block-4.

[14] Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing* (Feb. 13, 2015), https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[15] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

IV. Wireless Spectrum and the Internet of Things

With a wireless network that is stronger and more reliable, the apps marketplace will in turn grow stronger and more inventive, powering a symbiotic cycle of IoT innovation. There is little debate around the need for the U.S. government to take proactive steps to ensure that this wireless bandwidth is available, and we urge the planned Green Paper to directly address spectrum availability's role in the success of IoT.

New 5G networks hold the potential to provide the robust infrastructure needed to support higher bandwidth requirements of new apps. These technologies will need to interoperate and support one another in a hybrid of interdependent scenarios that will incorporate both licensed (e.g., LTE) and unlicensed (e.g., WiFi) spectrum arrangements. The U.S. government must utilize a spectrum management approach that is responsive and informed, utilizing appropriate reallocation and band sharing techniques where appropriate.

V. Standard-Essential Patents

The convergence of computing and communication technologies will continue as a diverse array of industries come together to build IoT. The IoT's seamless interconnectivity will be made possible by technological standards, like WiFi, LTE, Bluetooth, etc. Often, several companies will collaborate to develop these standards by contributing their patented technologies to these efforts. These technological standards, which are built on contributions through an open and consensus-based process, bring immense value to consumers by promoting interoperability while enabling healthy competition between innovators.

When an innovator gives its patented technology to a standard, this can represent a clear path to being rewarded in the form of royalties from a market that likely would not have existed without the standard being widely adopted. To balance this potential with the need for access to the patents that underlie the standard, many standard development organizations (SDOs) require holders of patents on standardized technologies to license their patents on fair, reasonable and non-discriminatory (FRAND) terms. FRAND commitments prevent the owners of patents that must be used in order to implement the standard (known as "standards-essential patents" [SEPs]) from exploiting the unearned market power that they otherwise would gain as a consequence of the broad adoption of a standard. Once patented technologies are incorporated into standards, manufacturers are compelled to use them to maintain product compatibility. So, in exchange for making a voluntary FRAND commitment with an SDO, SEP holders gain the ability to obtain reasonable royalties from a large number of standard implementers who might not have existed absent the standard. Without the constraint of a FRAND commitment, SEP holders would have the same power as a monopolist that faces no competition.

Unfortunately, a number of owners of FRAND-committed SEPs are flagrantly abusing their unique position by reneging on those promises with unfair, unreasonable, or discriminatory

licensing practices. These practices, which have been closely examined by antitrust and other regulators in many jurisdictions, not only threaten healthy competition and unbalance the patent system, but also impact the viability of new markets like the nascent IoT. The negative impacts on small businesses are only amplified because they can neither afford years of litigation to fight for reasonable royalties nor risk facing an injunction if they refuse a license that is not FRAND compliant.

Patent policies developed by SDOs today will directly impact the way we work, live, and play for decades to come. The importance of these issues to app developers and entire industries is why ACT | The App Association has launched the All Things FRAND (http://www.allthingsfrand.com/) project. The App Association urges the Department of Commerce to utilize All Things FRAND as a resource to better understand how regulators and courts around the world are defining FRAND. In its Green Paper, the Department can then encourage SDOs involved in developing IoT standards to clarify their patent policies accordingly.

SDOs vary widely in terms of their memberships, the industries and products they cover, and the procedures for establishing standards.[16] In part due to the convergence associated with the rise of IoT, each SDO will need the ability to tailor its intellectual property policy for its particular requirements and membership. ACT | The App Association believes that some variation in patent policies among SDOs is necessary and that the U.S. government should not prescribe detailed requirements that all SDOs must implement. At the same time, however, as evidenced by the judicial cases and regulatory guidance posted on www.allthingsfrand.com, basic principles underlie the FRAND commitment and serve to ensure that standard-setting is pro-competitive and the terms of SEP licenses are in fact reasonable. Ideally, an SDO's intellectual property rights policy that requires SEP owners to make a FRAND commitment would include all of the following principles that prevent patent "hold up" and anti-competitive conduct:[17]

- Fair and Reasonable to All – A holder of a SEP subject to a FRAND commitment must license such SEP on fair, reasonable, and nondiscriminatory terms to all companies, organizations, and individuals who implement or wish to implement the standard.
- Injunctions Available Only in Limited Circumstances – Injunctions and other exclusionary remedies should not be sought by SEP holders or allowed except in limited circumstances. The implementer or licensee is always entitled to assert claims and defenses.

---

[16] U.S. Fed. Trade Comm'n & U.S. Dep't of Justice, *Antitrust Enforcement and Intellectual Property Rights: Promoting Innovation and Competition*, at 33-34, footnote 5 (2007), *available at* https://www.ftc.gov/sites/default/files/documents/reports/antitrust-enforcement-and-intellectual-propertyrights-promoting-innovation-and-competition-report.s.department-justice-and-federal-tradecommission/p040101promotinginnovationandcompetitionrpt0704.pdf.

[17] http://www.allthingsfrand.com/about/about-allthingsfrand.com/.

- FRAND Promise Extends if Transferred – If a FRAND-encumbered SEP is transferred, the FRAND commitments follow the SEP in that and all subsequent transfers.
- No Forced Licensing – While some licensees may wish to get broader licenses, the patent holder should not require implementers to take or grant licenses to a FRAND-encumbered SEP that is invalid, unenforceable, or not infringed, or a patent that is not essential to the standard.
- FRAND Royalties – A reasonable rate for a valid, infringed, and enforceable FRAND-encumbered SEP should be based on several factors, including the value of the actual patented invention apart from its inclusion in the standard, and cannot be assessed in a vacuum that ignores the portion in which the SEP is substantially practiced or royalty rates from other SEPs required to implement the standard.

We also note that a number of SDO (Intellectual Property Rights) IPR policies require SDO participants to disclose patents or patent applications that are or may be essential to a standard under development. Reasonable disclosure policies can help SDO participants evaluate whether technologies being considered for standardization are covered by patents. Disclosure policies should not, however, require participants to search their patent portfolios as such requirements can be overly burdensome and expensive, effectively deterring participation in an SDO. In addition, FRAND policies that do not necessarily require disclosure, but specify requirements for licensing commitments for contributed technology, can accomplish many, if not all, of the purposes of disclosure requirements.

The U.S. Department of Justice (DOJ) has already encouraged SDOs to define FRAND more clearly. For example, DOJ's former assistant attorney general Christine Varney explained that "clearer rules will allow for more informed participation and will enable participants to make more knowledgeable decisions regarding implementation of the standard. Clarity alone does not eliminate the possibility of hold-up…but it is a step in the right direction."[18] As another example, Renata Hesse who now is the head of the DOJ's Antitrust Division, provided important suggestions for SDOs to guard against SEP abuses that included at least three of the aforementioned principles.[19]

In response to DOJ's calls for more clarity, the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) recently revised its patent policy to clarify the required FRAND commitments. IEEE-SA's revised patent policy incorporates many of the principles we

[18] Christine A. Varney, Assistant Att'y Gen., Antitrust Div., U.S. Dep't of Justice, *Promoting Innovation Through Patent and Antitrust Law and Policy*, Remarks as Prepared for the Joint Workshop of the U.S. Patent and Trademark Office, the Federal Trade Comm'n, and the Dep't of Justice on the Intersection of Patent Policy and Competition Policy: Implications for Promoting Innovation 8 (May 26, 2010), *available at* http://www.atrnet.gov/subdocs/2010/260101.htm.

[19] Renata Hess, Deputy Assistant Attorney General, *Six 'Small' Proposals for SSOs Before Lunch*, Prepared for the ITU-T Patent Roundtable (October 10, 2012), *available at* https://www.justice.gov/atr/speech/six-small-proposals-ssos-lunch.

listed above and that DOJ suggested SDOs adopt. Per IEEE's request, the DOJ reviewed IEEE-SA's revised policy and found it to be consistent with U.S. law.[20] The DOJ explained in detail why the revised policy "has the potential to facilitate and improve the IEEE-SA standard-setting process" by "bringing greater clarity to the IEEE RAND Commitment."[21] For example, the DOJ found that the provision of Reasonable Rate in the IEEE-SA's revised policy "could help speed licensing negotiations, limit patent infringement litigation, enable parties to reach mutually beneficial bargains that appropriately value the patented technology, and lead to increased competition among technologies for inclusion in the IEEE standards."[22]

Unfortunately, despite DOJ's detailed review and blessing, IEEE-SA's revised intellectual property rights policy has been under attack by a few entities that receive significant royalties and would prefer to leave FRAND undefined. To date, only a small number of SDOs of which ACT | The App Association is aware have taken steps similar to IEEE. This is largely due to the fact that most SDOs struggle to follow IEEE's example because their membership includes SEP holders that make significant sums of money through licensing their patents and do not want FRAND commitments to restrain their ability to charge high royalties. For this reason, we believe there is a need for regulatory guidance – not just to encourage SDOs to clarify their patent policies, but also to help guide courts in resolving disputes over FRAND commitments.[23]

Insofar as the role of government in standards is concerned, ACT | The App Association supports the goals of the National Technology Transfer and Advancement Act[24] and the recently-revised OMB Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*.[25] Notably, OMB

---

[20] *See generally* Letter from Renata B. Hess, U.S. Department of Justice, to Michael A. Lindsay, Dorsey & Whitney LLP (February 2, 2015).

[21] *Id.* at 8.

[22] *Id.* at 14.

[23] In the last several years, many agencies in multiple jurisdictions have issued binding and non-binding guidance on FRAND. *See, e.g.,* U.S. Department of Justice and U.S. Patent & Trademark Office, "Policy Statement On Remedies For Standards-Essential Patents Subject To Voluntary F/RAND Commitments" (January 8, 2013); European Commission, *Competition policy brief: Standard-essential patents* (June 2014), *available at* http://ec.europa.eu/competition/publications/cpb/2014/008_en.pdf; Competition Bureau Canada, *Enforcement Guidelines: Intellectual Property* at 54 (Mar. 31, 2016) (http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/cb-IPEG-e.pdf/$file/cb-IPEG-e.pdf; *Guidelines for the Use of Intellectual Property under the Antimonopoly Act* at 10-11 (Jan. 21, 2016), *available at* http://www.jftc.go.jp/en/pressreleases/yearly-2016/January/160121.files/IPGL_Frand_attachment.pdf (tentative translation); *Review Guidelines on Unfair Exercise of Intellectual Property Rights* (Dec. 17, 2014), *available at* http://eng.ftc.go.kr/bbs.do?command=getList&type_cd=62&pageId=0401 (translated version); *KFTC initiates public comment period on the amendment to its IP guidelines* (Dec. 16, 2015), *available at* http://eng.ftc.go.kr/bbs.do?command=getList&type_cd=52&pageId=0305. Much of this guidance is new and will need to be refined as agencies and courts gain more experience with disputes over FRAND commitments.

[24] National Technology Transfer and Advancement Act of 1995, Pub. L. No. 104-113 (1996).

[25] Revision of OMB Circular No. A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities", 81 FR 4673 (Jan. 27, 2016).

Circular A-119 creates a clear preference for the use of "voluntary consensus standards" as a basis for regulatory and procurement activities in lieu of government-unique standards, except when this would be inconsistent with applicable law or otherwise impractical. Moreover, consistent with our prior comments on policies that promote effective standards for the development and deployment of IoT, OMB Circular A-119 defines a "voluntary consensus standard" to include those that "requir[e] that owners of relevant intellectual property have agreed to make that intellectual property available on a non-discriminatory, royalty-free or reasonable royalty basis to all interested parties."[26]

Because of the interconnectedness of our economy and technology development, the collective decisions by policymakers, courts, and regulators around the world create the conditions that weave the fabric of innovation. ACT | The App Association therefore urges that the planned Green Paper clearly establish the U.S. government's role in promoting the realization of IoT by addressing standards and IPR matters consistent with the above.

VI. Copyright Law's Role in the Internet of Things

Copyright protections are foundational to rewarding the creativity and innovation that sustains and grows much of the U.S. economy and IoT. With the rise of the digital economy and the increasing internet-enabled connectivity of consumer products, these copyright protections have only become more important for those who utilize this global marketplace.

Piracy presents a major threat to the success of our members and the billions of consumers who rely on digital products and services. Piracy, whether originating within the United States or abroad, threatens not only the creators of digital content by undermining their ability to innovate, invest, and hire, but also the end users' confidence in software-enabled products and services as there is potential for consumers to be victimized by illegal sellers posing as legitimate content owners and sellers. Counterfeiting software apps can lead to customer data loss, interruption of service, revenue loss, and reputational damage. Further, with the rise of enterprise mobile app development, apps are being used as a means to attack mobile users of an entire enterprise. While the criminal penalties for these activities (e.g., attacking a bank's clients through a counterfeit version of their app) are likely more of a deterrent than the copyright laws being violated when the counterfeit app is created, these criminal acts all begin with first misappropriating application logic and application media content (brands, etc.). These threats have caused significant damage, and continue to pose substantial hazards, to app development companies that service every sector of the economy for countless end users.

The app industry effectively did not exist when the Digital Millennium Copyright Act[27] (DMCA) became law in 1998 following a comprehensive negotiation between policymakers, copyright

[26] *Id.* at 16.

[27] Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

interests, tech firms, network operators, and nonprofits. The DMCA is not without flaws, but it has proven effective and flexible enough to provide for and deal with continued innovation in the tech sector as well consumer protection. Further, courts have reined in attempts to abuse the law on many key issues.

Recently, ACT | The App Association submitted detailed comments to the U.S. Copyright Office regarding the role of copyright law with respect to software-enabled consumer products[28] and further participated in a U.S. Copyright Office public roundtable on the topic. As we explain in these comments, the U.S. government should disregard calls for sweeping changes to U.S. copyright law based on theoretical legal theories and undemonstrated impacts. We urge for the IoT Green Paper to reinforce the role of copyright protections in the future of IoT.

VII. Digital Trade & Cross-Border Data Flows

In order to continue to grow and to meet customer demands, companies must engage in the global digital economy, which represents approximately $8 trillion of commerce annually.[29] The arrival of the app store model and the rise of cloud services have permitted small app companies to access overseas markets where 95 percent of the world's consumers live. In the mobile marketplace, app stores use the cloud to connect app makers with customers around the globe while managing transactions in many different currencies. Cloud-based resources also allow early stage companies to scale swiftly to meet demand in a global marketplace.

While the global digital economy holds great promise for small app development companies, our members face a diverse array of challenges or trade barriers entering new markets, broadly defined as "government laws, regulations, policies, or practices that either protect domestic goods and services from foreign competition, artificially stimulate exports of particular domestic goods and services, or fail to provide adequate and effective protection of intellectual property rights."[30] These barriers take many forms, including unique national standards that impede interoperability and broad data localization requirements that can undermine the very purpose of an app. Regardless of their form, they all have the same net effect: impeding U.S. exports and investment.

A key mechanism for the removal of trade barriers is through the negotiation of robust trade agreements. We support the negotiation of international agreements to facilitate greater trade and actively partner with U.S. government agencies, including the United States Trade Representative and the Department of Commerce, and governments and stakeholders around

[28] http://actonline.org/wp-content/uploads/ACT-Comments-re-Copyright-Software-Enabled-Consumer-Products-021616.pdf.

[29] http://actonline.org/2016/01/04/act-the-app-association-releases-latest-app-industry-report/.

[30] https://ustr.gov/sites/default/files/2015%20NTE%20Combined.pdf at 1-2.

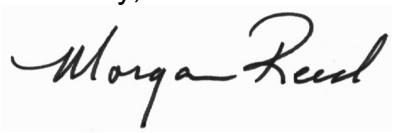
the globe to promote policies that will do so. For example, we have recently released *The Trans-Pacific Partnership, Small Businesses, and the App Economy*, a white paper which explores the benefits of the this trade agreement to the app economy.[31]

Consistent with the above, we urge that the planned Green Paper address the essential role that digital trade has in the growth of IoT. We also encourage the Department of Commerce to establish a U.S. government-wide policy that supports digital trade and IoT through the reduction of trade barriers that impede the benefits of IoT, which depends on a global digital infrastructure.

VIII. Conclusion

ACT | The App Association appreciates this opportunity to provide input on NTIA's RFC and the U.S. government's role in promoting its use and benefits. We encourage the U.S. government to work with stakeholders to establish a policy framework for IoT that promotes interoperability, furthers data security and consumer privacy, utilizes effective spectrum management, provides needed intellectual property protections, and enhances digital trade. We stand ready to work with all stakeholders to realize the full potential of IoT and encourage you to reach out with any questions.

Sincerely,



Morgan Reed
Executive Director
ACT | The App Association

[31] http://actonline.org/wp-content/uploads/App_Assoc_TPP_paper.pdf.