January 15, 2017

Attn: Dr. Andreas Lymberis and Mr. Gökalp Gümüşdere
Directorate-General for Communications Networks, Content and Technology Digital Industry
Competitive Electronics Industry Unit
Avenue de Beaulieu 25
1160 Brussels, Belgium

RE: Comments of ACT | The App Association to the European Commission Directorate-General for Communications Networks, Content and Technology regarding *Smart Wearables: Reflection and Orientation Paper*

ACT | The App Association writes to provide input to the European Commission's (EC) Directorate-General for Communications Networks, Content and Technology Digital Industry (DG CONNECT) on its request for public comment on its Orientation and Reflection paper (R&O) addressing the potential benefits and challenges facing smart wearable technologies and the role the EU government should play in its success.[1]

The App Association represents more than 5,000 small business app companies and technology firms located around the globe that create the apps used on mobile devices. As the world has quickly embraced mobile technology, our member companies have been creating innovative solutions that power the growth of the internet of things (IoT) across modalities and segments of the economy. We applaud the European Commission's (EC) efforts to understand IoT and to explore ways in which it can fully realize the immense benefits of smart wearables. These comments address some of the challenges and opportunities raised in the European Commission's R&O.

I. Mobile Apps are the Interface for the Smart Wearables Revolution

As DG CONNECT discusses in its R&O paper, the rise of IoT is a concept that encompasses the wide range of smart wearable technologies available today as well as those in development. IoT is expected to enable improved efficiencies in processes, products, and services across every sector. Across segments of the economy, from healthcare to infotainment to defense, the use of smart wearables demonstrates efficiencies unheard of

[1] *Smart Wearables: Reflection and Orientation*, European Commission: http://ec.europa.eu/newsroom/document.cfm?doc_id=40542 (hereinafter R&O).

even a few years ago. The R&O notes that IoT, specifically the wearables market, will grow into a multi-billion euro business in less than a decade.[2]

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

We agree with DG CONNECT that smart wearable applications will be highly dependent on use cases. The technology industry, to date, has done well through open Application Programming Interfaces (APIs) and other widely-adopted standards (e.g., Transmission Control Protocol/Internet Protocol [TCP/IP]) to enable interoperability. For example, in healthcare, a miniaturized and embedded connected medical device must automatically communicate bi-directionally in real-time. This capability enables a healthcare practitioner to monitor a patient's biometric data as well and facilitates patient communications with caregivers 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 mobile app industry has been in existence less than a decade, but it has experienced explosive growth alongside the rise of smartphones and smart wearables. 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 startups and small businesses. While smart wearables encompass a diversity of applications across the consumer and enterprise experiences, the interface for communicating with these devices will likely remain a mobile app on a smartphone. The rise of smart wearables will hinge on the app economy's continued innovation, investment, and growth; in short, apps are the interface for smart wearable revolution.

[2] *See* R&O p. 10.

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

For example, the App Association's innovative members in the smart wearables space include:

- UnaliWear (http://www.unaliwear.com), which makes the Kanega watch, a device that helps seniors live independently in their homes. Using a variety of sensors, the watch helps users monitor biometric markers, improve medication adherence, access geolocation support, and call for emergency assistance.
- Moov (https://welcome.moov.cc), a health and fitness wearable company that, through their unique apps, allows users to get the benefits of personal training in the comfort of their own home. Their software can count your reps, calculate things like distance and speed, and provide information on the success of a workout and how to improve it. They collect things like weight, height, and activity to help users set and keep health and fitness goals.
- ResMed (http://www.resmed.com/us/en/healthcare-professional.html) changes lives with award-winning medical devices and cutting-edge cloud-based software applications that better diagnose, treat, and manage sleep apnea, chronic obstructive pulmonary disease (COPD), and other chronic diseases. ResMed is a global leader in connected care, with more than 2 million patients remotely monitored every day.

II. Recommendations to DG CONNECT Regarding Challenges and Opportunities Facing Smart Wearables

In its R&O paper, DG CONNECT offers a number of recommendations regarding challenges and opportunities related to smart wearables, and offers proposed direction to EC staff on how to address them. Based on our position as the globe's leading voice for small business innovators in the app economy, the App Association offers the following recommendations. We strongly urge that the R&O paper be updated to incorporate these recommendations before DG CONNECT take further steps related to smart wearables and that any future policy decisions related to smart wearables carefully consider our experienced viewpoints.

The App Association's specific recommendations follow within this section. We strongly encourage DG CONNECT and any other European government stakeholders to work with us to realize the full potential of smart wearables in the European Union.

a. A Tailored and Coordinated European Approach to Smart Wearables is Essential

To realize the full potential of smart wearables (and IoT at large) across economic segments, the coordination of the EC, EU member states, and other government agencies will be essential. When considering entry into a new market, app makers must understand the regulatory environment. A lack of harmony between these entities – including localities – creates uncertainty, discouraging the hypercompetitive app economy where time-to-market is a critical factor. Due to the rise of the app economy across industries and use cases, countless European government entities will play key roles in empowering the future of mobile apps and smart wearables. Agency coordination will not only help avoid duplicative or conflicting regulations and parallel efforts, but it will also help governmental authorities ensure that considerations for and execution of its actions are deliberate and well-informed. The App Association is committed to working in partnership with DG CONNECT, other European government entities, and other stakeholders across the public and private spheres to develop an effective coordinated approach to enable smart wearables to improve the lives of countless European citizens and businesses.

Further, the App Association urges DG CONNECT to avoid approaching smart wearables as its own "vertical" for which a new layer of regulation is applied. As we discuss above, the wide range of smart wearable use cases and market needs negate the "one-size-fits-all" approach to such a broad concept. Rather, sector-specific regulatory approaches, addressed appropriately by relevant authorities on a case-by-case basis, are strongly recommended and will ensure a more tailored and scalable approach to smart wearables.

b. Data Security and End User Privacy for Smart Wearables

While the rise of smart wearables holds incredible promise, it inevitably also raises more security threats due to a broadened attack vector, necessitating more evolved and dynamic risk management practices. Whether in consumer or enterprise settings, no data is more important to Europeans than their own information. The App Association and its members appreciate this and put extensive resources into ensuring the security and privacy of end user data. Doing so is a business necessity in an internet-enabled global economy where end user trust must be earned and maintained in order to meet market demands.

For example, fully leveraging all technical measures available pursuant to a scalable risk management approach, including the use of end-to-end encryption, is a critical element to protecting data broadly, enabling key segments of the economy – from industrial to financial to healthcare – by protecting access to, and the integrity of, data. Encryption's role should not be understated – without strong encryption, entire economies and industries are put at a significantly heightened risk of their data being compromised, and smart wearables are no exception. Therefore, the App Association calls on DG CONNECT to discuss and emphasize the integral role the use of strong encryption has to the success of smart wearables in the R&O

paper. Further, DG CONNECT, in coordination with other relevant governmental bodies, should work to: facilitate the broad sharing of encryption tools and practices; provide a resource for encryption standards and guidelines; and identify key encryption resources to support smart wearable stakeholders across the public and private spheres.

The App Association notes that, despite the important role encryption plays in protecting consumers and businesses, some interests persist in demanding that "backdoors" be built into encryption algorithms for the purposes of lawful access. While supporting appropriate lawful access to data, we reject such suggestions as mandates that will degrade the safety and security of end users by creating vulnerabilities that criminals and state-backed hackers will exploit. The App Association strongly believes that the R&O paper should recognize the vital role encryption and other technical measures play in securing the smart wearable data.

Further, public-private partnerships are a useful vehicle for cooperation on ways to confront both current and emerging cyber-based threats to smart wearables and facilitate the ability to rapidly change in response to ever-developing risks. The App Association is committed to working collaboratively with any public and private stakeholders in such fora to ensure a secure cyberspace and to grow opportunities in IoT. DG CONNECT has already recognized the value of the public-private partnership model in a number of contexts, and the R&O paper should be no exception.

Additionally, the voluntary timely sharing of cybersecurity threat indicators among organizations from both the public and private sectors will be crucial in the detection, mitigation, and recovery of cybersecurity threats, particularly with the rise of smart wearables. Cybersecurity threat information sharing fora, 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. As an example, the U.S. government has relatively recently created the concept of Information Sharing Analysis Organizations (ISAOs), which are envisioned in Executive Order 13691[4] to be formed to fill needs to timely cybersecurity threat information for unique communities large and small, sometimes across economic segments. ISAOs, as a complement to existing 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. 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, because the vast majority of cybersecurity breaches occur due to human error and are preventable,[5] end user (both consumer and enterprise) education is a crucial aspect of

[4] 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.

[5] https://www.scmagazine.com/human-error-contributes-to-nearly-all-cyber-incidents-study-finds/article/538590/.

improving cybersecurity when using smart wearables. In the context of smart wearables, we urge that DG CONNECT address how the EU can inform end users across the business and consumer communities of steps to take to ensure that proper cyber "hygiene" is practiced.

c. The Smart Wearable Revolution Requires Sound Wireless Spectrum Management by Governments

We congratulate DG CONNECT for acknowledging the need for a robust internet infrastructure to support the smart wearables revolution. With a wireless network that is stronger and more reliable, the app economy will in turn grow stronger and more inventive, powering a "virtuous cycle" of innovation. New 5G networks hold the potential to provide needed infrastructure to support higher bandwidth requirements of new apps and smart wearables. 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., Wi-Fi) spectrum arrangements. As part of its approach to smart wearables, the App Association urges the EU to utilize a spectrum management approach that is responsive and informed, utilizing appropriate reallocation and band sharing techniques where appropriate.

d. Reasonable Access to Standard-Essential Patents Will Power the Smart Wearables Revolution

The convergence of computing and communication technologies will continue as a diverse array of industries come together to build IoT, with a major component being smart wearables. Technological standards, like Wi-Fi, LTE, Bluetooth, etc., will enable IoT's seamless interconnectivity. Often, many companies will collaborate to develop these standards within trusted fora 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 deliberately abusing their unique positions as owners of SEPs by reneging on those promises made during standard development with unfair, unreasonable, or discriminatory licensing practices. These deceptive practices, which have been (and in some cases, are being) closely examined by competition regulators around the globe, not only threaten healthy competition and unbalance the patent system, but also impact the viability of new markets like the nascent IoT and smart wearables markets. 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. The App Association believes that it is important for DG CONNECT to acknowledge the key role that SEPs and FRAND obligations will play in the growth of smart wearables and IoT at large.

The importance of these issues to app developers and entire industries is why The App Association launched the All Things FRAND (http://www.allthingsfrand.com/) project. The App Association urges the European Commission to utilize All Things FRAND as a resource to better understand how regulators and courts around the world are defining FRAND. As evidenced by the judicial cases decided and regulatory guidance finalized, basic principles underlie the FRAND commitments 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 the App Association's FRAND principles.[6]

However, because SDOs vary widely in terms of their memberships, the industries and products they cover, and the procedures they use to establish standards,[7] each SDO will need the ability to tailor its intellectual property policy for its particular requirements and membership. The App Association believes that some variation in patent policies among SDOs is necessary and that the EU should not prescribe overly prescriptive or one-size-fits-all requirements that all SDOs must implement.

For example, the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) has revised its patent policy to clarify required FRAND commitments within its

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

[7] 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.

process, which were later determined to be pro-competitive by antitrust authorities.[8] Despite this, IEEE-SA's revised intellectual property rights policy has been under attack by a minority of entities that receive significant royalties and would prefer to leave FRAND undefined so that they can continue to exploit this lack of clarity. To date, only a small number of SDOs of which the App Association is aware have taken steps similar to IEEE-SA. We therefore 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.[9]

Because of the interconnectedness of the EU's economy and technology development, the collective decisions by policymakers, courts, and regulators around the world create the conditions that weave the fabric of innovation. The App Association therefore urges that the R&O paper acknowledge the European Commission's role in promoting the realization of smart wearables and IoT widely by addressing standards and intellectual property rights matters consistent with the above.

III. Copyright Law Protections Are Crucial to the Smart Wearable Revolution

Copyright protections are foundational to rewarding the creativity and innovation that sustains and grows much of the U.S. and EU economies and IoT generally. With the rise of smart wearables, these copyright protections have only become more important for those who utilize this global marketplace.

Piracy presents a major threat to the success of the App Association's members and the billions of consumer and enterprise end users who rely on their digital products and services, including the use of smart wearables. Piracy, no matter where it originates, 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 because they may fall victim to those posing as legitimate content owners and sellers. Further, with the rise of

---

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

[9] 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.

enterprise mobile app development, apps are being used as a means to attack mobile users of an entire enterprise.

In 2016, the App Association submitted detailed comments to the United States Copyright Office regarding the role of copyright law with respect to software-enabled consumer products including smart wearables, which we encourage DG CONNECT to review and consider.[10] As we explain in these comments, governments should disregard calls for sweeping changes to their copyright laws based on theoretical legal theories and undemonstrated impacts. We urge DG CONNECT to ensure that the R&O paper reinforce the important role this area of intellectual property has in the future of smart wearables.

e. The Essential Role of Cross-Border Data Flows in the Growth of Smart Wearables

In order to continue to grow and to meet customer demands, smart wearable companies must engage in the global digital economy, which represents approximately $8 trillion of commerce annually.[11] 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 (particularly in the smart wearables space), the App Association's members face a diverse array of trade barriers when entering new markets (we broadly define trade barriers 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"[12]). These barriers take many forms, such as technology-specific national standards and data localization requirements and undermine the very purpose of a mobile app. Regardless of their form, they all have the same net effect: impeding and investment and innovation.

To ensure that policies that would discourage the growth of smart wearables that rely on the free international flow of data do not impede the rise of IoT, the App Association urges the development of international agreements (treaties or bi-lateral agreements) to facilitate the seamless flow of data across borders. We believe that omitting this facet from the R&O paper

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

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

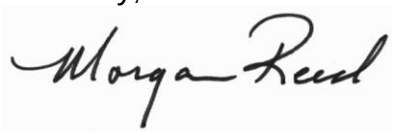
[12] https://ustr.gov/sites/default/files/2015%20NTE%20Combined.pdf at 1-2.

is an oversight and encourage that the important role of cross-border data flows be acknowledged and promoted.

IV. Conclusion

ACT | The App Association appreciates this opportunity to provide input on the European Commission's R&O paper. We encourage DG CONNECT to work with all stakeholders to establish policy frameworks that will incent the exponential growth of smart wearables. The App Association is committed to realizing the full potential of smart wearables, and the IoT generally.

Sincerely,



Morgan Reed
Executive Director
ACT | The App Association