January 13, 2017

Re: Comments to the Commission on Smart Wearables

Dear Dr. Lymberis and Mr. Gümüşdere,

On behalf of the Center for Data Innovation (datainnovation.org), we are pleased to submit these comments in response to a request for comments from the Commission on its reflection and orientation paper on smart wearables.

The Center for Data Innovation is the leading think tank studying the intersection of data, technology, and public policy. With staff in Brussels and Washington, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as predictive analytics, open data, cloud computing, and the Internet of Things. The Center is a nonprofit, nonpartisan research institute affiliated with the Information Technology and Innovation Foundation.

The Center welcomes the reflection paper and agrees with the majority of its conclusions. The paper correctly identifies the reasons why wearables present a unique opportunity for Europe, as well as many of the issues that still need to be addressed. However, the Center is also concerned that the report overlooks and misunderstands some important details, which could impact Europe's ability to realize the opportunity that wearables present. These points are addressed in more detail in the attached pages.

Yours sincerely,

Daniel Castro
Director
Center for Data Innovation
dcastro@datainnovation.org

Nicholas Wallace
Senior Policy Analyst
Center for Data Innovation
nwallace@datainnovation.org

SUMMARY

The Directorate-General for Communications Networks, Content, and Technology in the European Commission drafted a "reflection paper" on smart wearables, which it released for public comment in November 2016.[1] The Center for Data Innovation welcomes the paper and agrees with the majority of its conclusions, which show pragmatic thinking at DG Connect about how Europe can become more competitive in the data economy. The paper correctly identifies the reasons why wearables present a unique opportunity for Europe, such as Europe's strong manufacturing base and the fact that the sector is not yet dominated by any player. The report also correctly highlights issues that need to be dealt with appropriately, such as standards and liability.

However, the Center is also concerned by other trends in European policy that may get in the way of the ambitions described in the paper, some misconceptions in the paper itself, as well as matters it does not discuss in sufficient detail. These include excessive privacy regulations, simplistic approaches to European competitiveness and standards, misconceptions about the privacy implications of wearable devices, and insufficient consideration of market-based solutions to improve cybersecurity.

EUROPEAN COMPETITIVENESS

The paper correctly identifies business opportunities for European firms in wearables technology, but its authors should also consider the importance of the platforms that developers rely on and the role of mergers and acquisitions in scaling-up products: these are often foreign in origin, and present an opportunity for European competitiveness, not a threat.

"Smart wearables" is a new market with no dominant players. This presents a market opportunity for European businesses. Furthermore, what strong players there already are in wearables (e.g. manufacturers of fitness trackers) are often foreign SMEs with which European business can reasonably compete.[2] However, there are two important nuances to this opportunity that the Commission should consider.

[1] "Smart Wearables: Reflection and Orientation Paper," European Commission, November 28, 2016, http://ec.europa.eu/newsroom/document.cfm?doc_id=40542.
[2] "Fitness Trackers in the Lead as Wearables Market Grows 3.1% in the Third Quarter," IDC, December 5, 2016, https://www.idc.com/getdoc.jsp?containerId=prUS41996116.

First, firms producing smart wearables succeed by taking advantage of existing platforms, especially mobile platforms such as iOS and Android, to scale their products. Thus, the goal of European policy should not be to create European clones of major digital platforms—as some at the Commission seem to mistakenly believe—or to otherwise disrupt existing digital platforms, but rather to enable European firms to take advantage of these platforms in order to build innovative, value-added services.[3]

Second, European policy should enable the innovative ideas produced by Europe's small and medium-sized enterprises (SMEs) to turn into mass-market products. While this transformation sometimes occurs through organic growth, it also occurs through mergers and acquisitions, and the profits from such deals are often re-invested in new start-ups and new ideas. Improper signaling from policymakers could have a chilling effect on such deals.[4]

STANDARDS

Policymakers do not need to introduce standards through regulation because the market can meet this need. Instead, policymakers should focus on public sector procurement rules, which should include standards requirements to ensure interoperability in essential public services, keep tenders competitive, and prevent vendor lock-in and excessive price inflation.

Standards matter in the private sector, but they should not be mandated through regulations, because this could stifle innovation by freezing out new methods or foreign alternatives. The fledgling global market for wearables should be given the chance to establish interoperability organically. Consumer demand exerts competitive pressure on firms to design products that are interoperable with competing products. For example, Apple's decision to withdraw support for Flash arguably played a strong role in the success of the newer HTML5 standard, even though other companies did not follow suit for some years.[5] This improvement was made possible by a deviation from common standards. Or consider the lack of interoperability between European and

[3] John Springford, "How not to create a 'European Google'," *Politico*, August 27, 2015, http://www.politico.eu/article/not-create-european-google-innovation-tech-monopoly/.
[4] "European Commission Allegations About Facebook Risk Chilling Data-Driven Innovation," Information Technology and Innovation Foundation, December 20, 2016, https://itif.org/publications/2016/12/20/european-commission-allegations-about-facebook-risk-chilling-data-driven.
[5] Keith Collins, "How Adobe Flash, once the face of the web, fell to the bring of obscurity—any why it's worth saving," *Quartz*, December 29, 2016, https://qz.com/863467/how-adobe-flash-once-the-face-of-the-web-fell-to-the-brink-of-obscurity-and-why-its-worth-saving/.

American "standard definition" television standards. Old workarounds, such as TVs with inbuilt PAL-NTSC switches, are being made obsolete by common—and superior—high-definition standards. Moreover, the original problem was caused by differing electrical standards, which are the result of decisions taken by regional monopolies at a time when consumer demand for interoperability was much lower.

Developers for smart wearables are entering a market where consumers already want their smartphones to interact wirelessly with their Korean TVs, American laptops, Japanese games consoles, German cars, and Swedish lightbulbs. In the 1950s, incompatible standards were mainly a manufacturing cost: consumers just wanted to buy hairdryers they could plug into the wall without them blowing up.

However, it is sensible to stipulate particular standards in public sector procurement.[6] Wearables will have public sector uses in many fields, including health, law enforcement, fire and rescue, and the military. It makes sense for European procurement rules to implement common standards to support cooperation between agencies, keep tenders competitive, and prevent the "vendor lock-in" that causes excessive price inflation by tying agencies to an extremely narrow range of compatible options. As a buyer and a provider of services, the public sector will be an important player in wearables and the wider Internet of Things, and the purchasing decisions it makes will influence the course of standards development, without freezing out alternatives.

PRIVACY

The EU's current privacy regime and incoming rules threaten European competitiveness in smart wearables and the Internet of Things.[7]

It is encouraging that the paper recognizes the need for data protection regulations to be "innovation friendly." Unfortunately, this is not the case in the European Union. The GDPR already imposes excessive restrictions on data re-use, which limits the possibilities for discovering new and valuable uses of existing connected devices. The upcoming ePrivacy directive could also impact this if the rules on how devices transmit data, or on how companies

[6] Joshua New and Daniel Castro, "Why Need National Strategies for the Internet of Things," Center for Data Innovation, December 16, 2015, http://www2.datainnovation.org/2015-national-iot-strategies.pdf.
[7] Nick Wallace, "Regulation Will Make or Break Europe's Internet of Things," Center for Data Innovation, November 21, 2016, https://www.datainnovation.org/2016/11/regulation-will-make-or-break-europes-internet-of-things/.

can analyze the way customers use apps to generate revenue from advertising, are too restrictive. These restrictions could stifle Europe's opportunities to succeed in wearables and the Internet of Things more broadly, as they limit avenues for innovation and revenue generation that will leave foreign competitors free to offer better, cheaper services. It would be helpful if the Commission identifies where existing policy fall short of creating "innovation friendly" regulations.

The orientation paper raises special concerns about the fact that devices that contain cameras, such as smart glasses, may record passersby. However, the paper does not give any reasons for why this might be a problem. Insofar as it could be, existing regulation is sufficient to deal with it. Controls already exist on filming in sensitive places, such as hospitals. That the cameras in some wearable technology—such as Google Glass—are not especially prominent raises no more concerns than older concealed cameras, which are both less noticeable and have entirely legitimate uses. The responsibility for obeying applicable laws in all such cases lies with camera owners, not manufacturers. Furthermore, filming in a public place—whether the camera is visible or invisible—is in itself entirely legal, including when passersby are inevitably caught on camera. The above arguments also apply in a similar fashion to devices that record audio data: putting them inside wearables does not introduce anything new in regulatory terms.

Wearables will also collect location data in order to provide consumers with certain services, and privacy regulations should be nuanced so as not to limit the range of services customers can choose from.

Similarly, data shared with medical practitioners (whether it is video, audio, health information, or anything else) is already subject to the strong protections that go with medical confidentiality laws.

FREE FLOW OF DATA

European policymakers should ensure free data flows, not only between EU member states but also to non-EU countries. This will ensure data can easily be aggregated and analyzed across borders, and that wearables are part of a global Internet of Things, not a walled-off EU one. Data localization does not protect privacy, but good cybersecurity practices do, regardless of where the data is stored.

The report is right to recognize that free data flows are important for supporting the development of smart wearables. For example, small businesses entering this market cannot afford data

centers capable of storing, processing, and securing the vast amount of data their products generate. Cloud computing lowers this barrier to entry, but restricting data flows reduces the number of competing cloud companies developers can choose from, which needlessly raises costs. EU policymakers should be resolute in resisting attempts to introduce unnecessary exemptions to regulations that seek to ensure the free flow of data

However, free data flows between EU member states alone will not be sufficient, even without accounting for exemptions that member states may seek to enforce. To minimize costs for European companies by maximizing competitiveness in cloud services, there should also be free data flows to non-European countries.

European companies' own cybersecurity practices can protect data even if it is held in countries with very different approaches to privacy: proper use of encryption prevents unauthorized disclosure. Similarly, keeping the data inside the EU does not offer much protection to unencrypted, poorly-managed data.

CYBERSECURITY

Better transparency on security features of wearables will spur competition in this area. Rather than impose specific cybersecurity regulations on wearables, European policymakers should require companies to publish security policies that explain how they secure devices and data.[8] These disclosures will expose poor security practices and allow companies to be held to account, which will help to address market failures in Internet of Things security, including in wearables.

Policy makers should not impose technical security requirements on firms, but they should enforce transparency about security practices. Currently, consumers cannot easily distinguish between secure and insecure products. Information asymmetry about security practices causes a market failure where device manufacturers lack incentives to invest in proper security because they receive little benefit from these investments. If the law compelled companies to publish security policies that explain what measures they take to secure devices and data, then consumers, businesses, and the public sector could use this information to make more informed purchasing decisions. Given that compromised Internet of Things devices—including some

[8] Daniel Castro, "How Congress can fix 'internet of things' security," Center for Data Innovation, October 28, 2016, http://thehill.com/blogs/pundits-blog/technology/303302-how-congress-can-fix-internet-of-things-security.

wearables—pose a threat not only to their users, but also to third parties, better security in these devices will have a widespread effect.

While some European policymakers have shown a dim awareness of this issue, their recommendations fall flat—such as requiring sticky labels on devices.[9] This would be no more than a pointless regulatory cost, because security standards change quickly. Security policies should be published digitally.

MEDICAL DEVICE REGULATION

Many wearable devices will have value both as commercial lifestyle products and as medical devices. Policymakers should be careful to ensure that when regulating the latter—such as setting thresholds for accuracy and reliability—the necessary restrictions do not impact the freedom to use otherwise safe devices as consumer products.

Domestic policies that fund medical devices now should be reformed to include support for other general-purpose wearables that offer similar functionality.

In addition, there will be many components of medical devices, e.g. operating systems, wireless networks, and more, that are widely used for non-medical purposes. These components should not be regulated as medical devices simply because they appear in some medical devices.

It is encouraging to see the orientation paper pays particular attention to the debate over medical devices in the United States. The Food and Drug Administration's tiered regulation approach to medical apps is a good place to start.[10]

[9] John E. Dunn, "The EU's latest idea to secure the Internet of Things? Sticky labels," *Naked Security*, October 11, 2016, https://nakedsecurity.sophos.com/2016/10/11/the-eus-latest-idea-to-secure-the-internet-of-things-sticky-labels/.
[10] "Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff," Food and Drug Administration, February 9, 2015, http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf