FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING

MEMORANDUM

March 1, 2016

To: Subcommittee on Commerce, Manufacturing, and Trade Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Hearing on "Disrupter Series: Wearable Devices"

On **Thursday, March 3, 2016, at 10 a.m. in room 2123 of the Rayburn House Office Building**, the Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing titled "Disrupter Series: Wearable Devices."

I. BACKGROUND

Worldwide sales of wearable electronic devices are expected to reach 274.6 million units in 2016, an increase of more than 18 percent compared with 2015.[1] Wearables, as they are commonly known, are intended to be worn on the body and use internet connectivity to perform various functions. Examples of wearables include smartwatches, brooches that remind the wearer to improve their posture, and bracelets that track physical movements.[2] Internet-connected glasses, such as Google Glass, are another example of wearable technology.[3]

[1] *Smartwatches Will Definitely Overtake Fitness Bands, Report Says*, Washington Post (Feb. 2, 2016) (online at www.washingtonpost.com/news/the-switch/wp/2016/02/02/smartwatches-will-definitely-overtake-fitness-bands-report-says/).

[2] *Companies Are Excited About the Wearables Market. How Can They Convince Consumers?*, Washington Post (June 23, 2014) (online at www.washingtonpost.com/news/the-switch/wp/2014/06/23/companies-are-excited-about-the-wearables-market-how-can-they-convince-consumers/).

[3] *Id.*

Wearables are part of the Internet of Things (IoT), which generally refers to the ability of everyday objects to connect to the internet and to send and receive data.[4] As with the broader IoT, the expansion of wearable technology offers significant opportunities for innovation, but also poses risks for consumers.[5]

II. NOTABLE APPLICATIONS

The availability of wearable devices that can monitor physical parameters, such as heart rate and calories burned, spurred a growing trend in digital health tracking.[6] The increased consumer interest in recording biometric information, in turn, has resulted in the development of more diverse health-related wearables.[7] Some examples include a wearable sensor that can measure the user's sweat for electrolytes to monitor against dehydration; a smart hearing aid that can isolate specific sounds and tune out ambient noise; and a contact lens that measures the glucose in the wearer's tears.[8]

In 2015, the NFL began equipping all players' shoulder pads with wearable, internet-connected radio-frequency identification (RFID) chips that track the players' speed and location on the field and transmit that data to wireless receivers.[9] The chips are increasingly being used during practices to combine with data from other wearable devices that measure dehydration, heart rate, and other biometric information to maximize training.[10]

Perhaps one of the most recognizable categories of wearable technology is the smartwatch, which is expected to make up roughly 40 percent of the overall wearables market in 2016.[11] Smartwatches use Wi-Fi to connect the wearer with features that are traditionally

---

[4] Federal Trade Commission, *Internet of Things: Privacy & Security in a Commercial World*, FTC Staff Report (Jan. 27, 2015).

[5] *The Revolution Will Be Digitized*, Washington Post (May 9, 2015) (online at www.washingtonpost.com/sf/national/2015/05/09/the-revolution-will-be-digitized/).

[6] *Id*.

[7] *Id.*

[8] *Id.*; *What a Wearable Sensor Can See in Your Sweat,* Newsweek (Jan. 28, 2016) (online at www.newsweek.com/wearable-sensor-measures-sweat-body-temperature-dehydration-420387); *The Line Between Wearable Technology and Prosthetics Is Blurring,* Washington Post (July 2, 2014) (online at www.washingtonpost.com/news/innovations/wp/2014/07/02/the-line-between-wearable-technology-and-prosthetics-is-blurring/).

[9] *How RFID Chips Are Changing the NFL*, Forbes (Feb. 6, 2016) (online at www.forbes.com/sites/aarontilley/2016/02/06/how-rfid-chips-are-changing-the-nfl/#7edf547c5ad0).

[10] *Id.*

[11] *See* note 1.

associated with a smartphone; phone calls, texts, e-mails, and directions can be accessed directly from the device.[12]

III. PRIVACY AND DATA SECURITY

Wearables raise basic privacy concerns regarding what data is collected, how that data is used, whether the data is sold to third-parties, and how third-parties use that data. Data collected from fitness tracking sensors can be used to infer a user's stress levels, gender, age, smoking habits, and overall well-being.[13] This data could then be used by the product manufacturer, internet provider, or a third-party. For example, it could be shared with employers as part of a workplace wellness program, which may then be used to measure worker productivity.[14]

There are also concerns about what can happen to data when a wearable manufacturer goes bankrupt.[15] Many user agreements include clauses reserving the right to sell users' data in the event of bankruptcy.[16] It is unclear how much access consumers may have to their data after a sale or reorganization, and there are questions of whether the purchasing company has obtained sufficient user consent.[17]

The Health Insurance Portability and Accountability Act (HIPAA) entitles consumers to certain privacy protections for patient information.[18] Although a large portion of the data collected by some wearables is health information, in many cases that information would not be covered by HIPAA.[19] Devices prescribed by physicians are covered under HIPAA's Privacy Rule, but generally fitness trackers and other similar products are not covered.[20] Because of this

---

[12] *TAG Heuer, Intel and Google Raise the Stakes in Smartwatches*, New York Times (Nov. 10, 2015) (online at www.nytimes.com/2015/11/11/fashion/tag-heuer-intel-google-raise-the-stakes-in-smartwatches.html?_r=0).

[13] Scott Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 Tex. L. Rev. 85 (Mar. 1, 2014).

[14] *Big Doctor Is Watching: How Your Fitness Tracker Could Increase Your Health Insurance Costs Someday*, Slate (Feb. 27, 2015) (online at www.slate.com/articles/technology/future_tense/2015/02/how_data_from_fitness_trackers_medical_devices_could_affect_health_insurance.html).

[15] *The Scary Truth About Data Security with Wearables*, Tech Republic (July 3, 2014) (online at www.techrepublic.com/article/the-scary-truth-about-data-security-with-wearables/).

[16] *Id.*

[17] *When a Wearable Maker Shuts Down, Who Owns Your Steps?*, BuzzFeed News (Feb. 3, 2016) (online at www.buzzfeed.com/stephaniemlee/when-wearable-makers-shut-down-getting-your-data-isnt-always#.voVnolvVX).

[18] *The Price of Wearable Craze: Personal Health Data Hacks*, CNBC (Dec. 12, 2015) (online at www.cnbc.com/2015/12/12/price-of-wearable-craze-your-health-data-hacked.html).

[19] *Id.*

[20] *Id.*

inconsistency, consumers are often unaware of the privacy controls, if any, that protect their personal information from unauthorized parties.[21]

Because of the highly personal information they collect about their users, wearables may be particularly attractive to hackers.[22] Health records are estimated to be ten times more valuable to a thief than a stolen credit card.[23] Wearables may also be vulnerable to attack because many are produced by companies that are relative newcomers to the technology market, and have limited experience building rigorous security measures into devices.[24] Further, many wearables are not standalone devices.[25] Each time these devices interact with other endpoints—such as smartphones, the Cloud, hosting providers, and the device maker—presents opportunities for breaches because each endpoint has different security strengths and vulnerabilities.[26]

IV. FEDERAL GOVERNMENT ROLE

A. Federal Trade Commission

The Federal Trade Commission (FTC) has broad jurisdiction, under Section 5 of the FTC Act, to prohibit "unfair or deceptive acts or practices in or affecting commerce" by a wide variety of individuals and entities.[27] The FTC has used that authority to take action against manufacturers of connected devices who fail to take reasonable measures to secure their products.[28]

In January 2015, the FTC released a staff report entitled "Internet of Things: Privacy & Security in a Connected World," which provided staff recommendations for ensuring consumer protection in the IoT sphere including wearable technology.[29] The report provided recommendations that IoT manufacturers implement reasonable security measures, build those security features into the design of products, and monitor products throughout their life cycles, among others.[30]

---

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] 15 U.S.C. 45(a).

[28] *"Internet of Things" Security Is Hilariously Broken and Getting Worse*, Ars Technica (Jan. 23, 2016) (online at arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/).

[29] Federal Trade Commission, *Internet of Things: Privacy & Security in a Commercial World* (Jan. 27, 2015).

[30] *Id.*

The FTC report did not recommend legislation specific to IoT or wearable technology, but it did recommend that Congress enact baseline privacy legislation to increase consumer choice, require transparency, and mandate some level of privacy by design.[31]

B. Food and Drug Administration

In January 2015, the Food and Drug Administration (FDA) released draft guidance on the compliance policy of the Center for Devices and Radiological Health (CDRH) for "low risk general wellness products."[32] The guidelines define general wellness products as items that pose a very low risk to users' safety and are intended for general wellness purposes only—meaning that their intended use is either for encouraging general health, or for encouraging a healthy lifestyle to help reduce the risk or impact of health conditions that are benefitted by healthy lifestyle choices.[33]

Under the draft guidelines, FDA will ease certain regulations on low risk general wellness products, which includes many wearables such as fitness trackers and mobile applications that store health data.[34] FDA will generally not examine whether those products are medical devices for the purposes of the Federal Food, Drug, and Cosmetic Act, or whether they satisfy the requirements of that Act, including certain labeling requirements and manufacturing practices.[35] General wellness products may be subject to medical device requirements though, if the product makes claims related to treating or diagnosing certain diseases or conditions, such as treating or diagnosing obesity, anxiety, or eating disorders, among others.[36] FDA has not yet issued a final version of this guidance.

C. White House Consumer Privacy Bill of Rights

---

[31] *Id.*

[32] Food and Drug Administration, *General Wellness: Policy for Low Risk Devices* (Jan. 20, 2015) (online at www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429674.pdf?source=govdelivery&utm_medium=email&utm_source=govdelivery).

[33] *Id.*

[34] *The FDA Doesn't Want to Regulate Wearables, and Device Makers Want to Keep It That Way*, Verge (Jun. 24, 2015) (online at www.theverge.com/2015/6/24/8836049/fda-regulation-health-trackers-wearables-fitbit).

[35] *See* note 32.

[36] Food and Drug Administration, *General Wellness: Policy for Low Risk Devices* (Jan. 20, 2015) (online at www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429674.pdf?source=govdelivery&utm_medium=email&utm_source=govdelivery).

In February 2012, the White House released a framework for protecting consumer privacy, which included a proposal for a Consumer Privacy Bill of Rights, which incorporated the Fair Information Practice Principles (FIPPs): notice, choice, access, accuracy, data minimization, security, and accountability.[37]

In February 2015, the White House released draft legislation called the Consumer Privacy Bill of Rights Act of 2015.[38] The proposed legislation would extend credit-reporting protections to makers of wearable devices.[39] The draft, which has been the subject of criticism from members of Congress and consumer advocacy groups, would allow industries to develop their own codes of conduct on the handling of consumer information.[40] It would also charge the FTC with responsibility for ensuring that those codes of conduct satisfy certain requirements, including providing consumers with clear notices about how their personal information will be collected, used, and shared.[41]

V. WITNESSES

Thomas D. Bianculli
Vice President, Enterprise Technologies Office
Zebra Technologies

Meg Burich
Director of Commercial Development and Marketing
Adidas Digital Sports

Suresh Palliparambil
American Sales and Business Development Director
NXP

Scott R. Peppet
Professor of Law
University of Colorado Law School

---

[37] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012) (online at www.whitehouse.gov/sites/default/files/privacy-final.pdf).

[38] The White House, *Consumer Privacy Bill of Rights Act of 2015 Discussion Draft* (online at www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf) (accessed on Feb. 28, 2016).

[39] *Id.*

[40] *White House Proposes Consumer Privacy Bill of Rights*, Wall Street Journal (Feb. 27, 2015) (online at blogs.wsj.com/digits/2015/02/27/white-house-proposes-consumer-privacy-bill-of-rights/).

[41] *See* note 38.

Doug Webster
Vice President, Service Provider Marketing
Cisco