Statement of Professor Scott Peppet
Professor of Law, University of Colorado School of Law

Before the
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
U.S. House of Representatives

Hearing on Wearable Devices
March 3, 2016

> Very soon, we will see inside ourselves like never before, with wearable, even internal[,] sensors that monitor even our most intimate biological processes. It is likely to happen even before we figure out the etiquette and laws around sharing this knowledge.
>
> -- Quentin Hardy, *The New York Times* (2012)[1]

Chairman Burgess, Ranking Member Schakowsky, and Members of the Subcommittee, I appreciate the opportunity to speak with you today about wearable technologies. I am a Professor of Law at the University of Colorado Law School, where my work focuses on technology, markets, and privacy. I am also a member of the Board of Directors of Anixter International Inc., a distributor of industrial cabling and technology components, which is involved in the creation of technology infrastructure although not directly involved in wearable technologies. My comments today are solely in my personal and academic capacity and in no way reflect the views of the Anixter corporation or other organizations with which I am affiliated.

Wearable technologies offer myriad benefits, including better health, increased productivity in the workplace, economic efficiencies, and higher quality of life. Encouraging continued innovation in this growing field is important: wearable technologies are

[1] Quentin Hardy, *Big Data in Your Blood*, Bits, N.Y. Times (Sept 7, 2012).

relatively new and we are only beginning to see their potential. At the same time, wearables create at least four risks that industry and lawmakers should monitor and work together to control: (1) new types of data security risks; (2) risk of context-violative uses of data produced by wearable devices; (3) de-anonymization or re-identification risks; and (4) the reality that consumers are not being afforded meaningful opportunities to consent to these risks.[2] By providing clear guidance on how to manage these four risks, lawmakers and regulators can ensure that consumers can trust wearable devices, thereby encouraging continued innovation in this growing industry.

I. Types of Wearables

It is important to recognize that wearable technology has already progressed far beyond simple electronic pedometers or fitness monitors. Wearables now include:

Fitness devices, such as:

- Fitness bracelets that can track steps taken, calories burned, minutes asleep, heart rate, and sometimes location[3]
- Bicycling helmets and baseball caps that can track heart rate and caloric consumption[4]
- Sensor-filled socks that can detect how far and fast a user runs as well as detect risk of injury[5]
- Bio-tracking clothing with fitness sensors embedded in the fabric[6]

[2] For a more complete treatment of these issues, see Scott Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 95 Texas Law Review 85 (Nov. 2014). *See also See* Christopher Wolf, Jules Polonetsky, and Kelsey Finch, *A Practical Privacy Paradigm for Wearables* (Future of Privacy Forum, Jan. 8, 2015).
[3] Fitbit Blaze, http://www.fitbit.com; Garmin Forerunner, http://www.garmin.com.
[4] LifeBEAM, http://www.life-beam.com.
[5] Sensoria Fitness Socks, Sensoria Fitness, http://store.sensoriafitness.com.

Medical devices, such as:

- Health monitors that can track blood glucose levels,[7] temperature[8] and breathing patterns[9]
- A brassiere that can track slight variations in skin temperature for use in detecting breast cancer[10]
- Epidermal electronic patches worn as a bandage that can detect temperature, heart rate, brain activity, hydration levels, exposure to ultraviolet radiation, and even blood stream variations including glucose or potassium levels and kidney function[11]
- Ingestible and implantable sensor devices including "smart pills" that can monitor pH levels, temperature, and other internal bodily functions[12]
- Sensors worn between two teeth or mounted on dentures or braces to assess dental disease or unhealthy dental habits[13]

Workplace or employee monitoring devices, such as:

- Sensors worn around or on the lower back that can detect poor posture or risk of back injury[14]

---

[6] OmBra, http://www.omsignal.com; Ralph Lauren PoloTech Shirt, http://www.ralphlauren.com; Athos, http://www.liveathos.com.
[7] Joseph Walker, *Easier Blood-Sugar Monitoring for Diabetics*, Wall Street Journal (June 29, 2015).
[8] Peak, Basis, https://www.mybasis.com.
[9] Spire, http://www.spire.io.
[10] Cyrcadia Health, http://cyrcadiahealth.com.
[11] Biostamp, MC10, http://www.mc10.com; Sano, http://www.sano.co.
[12] Given Imaging, http://givenimaging.com.
[13] Ross Brooks, *Tooth-Embedded Sensor Relays Eating Habits to the Dentist*, PSFK (July 30, 2013).
[14] Lumo Back, Lumo, http://www.lumoback.com; Upright, http://www.uprightpose.com.

- Employee identification badges or lanyards that can record time spent at an employee's desk, tone of voice, and proximity to other employees to measure productivity and work habits[15]
- A wristband to track when workers lift heavy objects to provide safety analytics[16]

Cognition and emotion devices, such as:

- A bracelet to track changes in a user's autonomic nervous system to detect mental state (e.g., passive, excitable, pessimistic, anxious, balanced)[17]
- Headbands to track brain activity, focus and cognitive performance[18]
- An electronic mood ring that can track emotional well being[19]

This is by no means an exhaustive list, but it is suggestive. It illustrates both the incredible innovation in wearable devices and the intimate details such devices can sense, record, and transmit.

II. Four Risks: Lax Security, Misuse, Re-identification, and Lack of Consent

These wearable devices share four risks to which industry and lawmakers should attend: lax security, context-violative data uses, re-identification, and lack of meaningful consent.

[15] Humanyze, http://www.humanyze.com.
[16] Kinetic, http://www.wearkinetic.com.
[17] W/Me Bracelet, http://www.rootilabs.com.
[18] Muse headband, http://www.choosemuse.com; Melon headband, http://www.daqri.com.
[19] Moodmetric, http://www.moodmetric.com.

1. Wearable Devices are Prone to Data Security Problems: Many wearables are small consumer devices such as a fitness-tracking bracelet, a health monitoring patch, or a smart watch. Recent news has highlighted that such devices often have inadequate data security protections. A February, 2016 report, for example, showed that of eight wearable fitness devices studied, only one—the Apple Watch—had properly secured the device's BlueTooth connectivity.[20] These problems are not new: researchers have been demonstrating such vulnerabilities for years.[21] They persist because wearables have limited form factors, which can make robust security more difficult to implement, and often relatively low target price points, which can make incorporation of security measures prohibitive. In addition, these devices are often developed by startups or other firms unfamiliar with or not focused upon data security issues. Finally, these devices often have limited processing power and limited Internet connectivity abilities, making it difficult to push software-based security updates to them to address discovered security flaws.

These data security vulnerabilities create various policy decisions for lawmakers. I will mention two. First, Congress should confirm that the Federal Trade Commission (FTC) has authority under Section 5 of the FTC Act to oversee data security, as was recently affirmed in the Wyndham case by the U.S. Court of Appeals for the Third Circuit.[22] Much has been written and said about this, so I will not dwell on it.

[20] Open Effect, Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security (Feb. 2, 2016).
[21] Mahmudur Rahman et al., *Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device* 1 (Apr. 20, 2013).
[22] FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

Second, and more broadly, if Congress continues to consider Federal data breach notification legislation, it should ensure that such legislation protects wearable device data (and "Internet of Things" sensor data generally). The vast majority of state data breach notification laws do not protect the biometric and sensor data produced by wearable devices.[23] If consumers' wearable device data were hacked from a device or from the cloud, at the moment most device manufacturers would be under no obligation to warn the public. Data breach notification statutes help the market to discipline firms with lax security by providing the public with the information it needs to make informed consumer choices. Wearable device data—particularly biometric data—should be included in these legal regimes. The states should include biometric sensor data created by wearable devices in their definition of what constitutes protected data, and/or Congress should do so if it adopts a Federal data breach notification statute.

2. Wearable Device Data Invite Misuse: A consumer knows that wearing an exercise monitor will create data that reveals her exercise habits or sleep patterns. These inferences are obvious and direct. Wearables permit far less obvious inferences, however, that consumers may not expect. As a simple example, research shows that seemingly innocuous accelerometer data--generally used to show how a person is moving in space--can be used to detect location because the movement pattern created by driving down a particular road is often unique and therefore identifiable.[24]

[23] *See* Peppet, *supra* note __ at 139-140 for a full review of these state law issues.
[24] Jun Han et al., *ACComplice: Location Inference Using Accelerometers on Smartphones*, in 2012 Fourth International Conference on Communication Systems and Networks (COMSNETS 2012).

More generally, the data created by wearable device sensors are both massive in quantity—a sensor may track habits or behavior 24/7—and very high in quality. A wearable fitness monitor may track location, three-dimensional movement, heart rate, or other characteristics accurately, precisely, and persistently. This massive quantity and high quality of data can permit unexpected inferences. For example, a fitness monitor's separate measurements of heart rate and respiration might in combination reveal not only a user's exercise routine, but also cocaine, heroin, tobacco, and alcohol use, each of which produces unique biometric signatures.[25] As wearables proliferate, we are likely to find new and more startling inferences. For example, exercise data might permit inferences about a person's character, motivation, employment habits, and even credit-worthiness (e.g., if a person exercises a lot, they are likely diligent and hard-working).

Consumers are rightly nervous about such unexpected uses of wearable device data. A preliminary study found, for example, that Americans are concerned about health-related data being used outside of the medical context: 77% worry about such data being used for marketing, 56% are concerned about employer access, and 53% worry about insurer access.[26] Industry and lawmakers should be clear that such wearable device data will not migrate into employment, credit, insurance, housing, or other decisions without meaningful notice to consumers.

In addition, consumers should not be pressured into disclosing such data. In other contexts we have seen state legislatures forbid insurance companies, for example, from

[25] Annamalai Natarajan et al., *Detecting Cocaine Use with Wearable Electrocardiogram Sensors*, in UbiComp'13: Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing 123, 123 (2013).

[26] Heather Patterson and Helen Nissenbaum, *Context-Dependent Expectations of Privacy in Self-Generated Mobile Health Data* 43-45 (June 6, 2013).

requiring access to vehicular "black box" data as a condition of automotive insurance.[27] Such use constraints allow consumers to adopt such new technologies without fear that their data will end up in the hands of an employer, insurer, bank, or landlord. To the extent that it considers taking action in the wearable device context, Congress should consider similar constraints on the migration of wearable device data.

Finally, consumers should be protected against "in house" migration of wearable device data from one type of use to another. The Fair Credit Reporting Act (FCRA), for example, applies to third-party consumer reports used in credit or employment decisions but does not cover analytics performed by an employer on data generated by employees wearing a fitness device or other wearable technology. As wearable devices proliferate in the workplace, employees are concerned that data ostensibly collected for one purpose—such as participation in a wellness program—might be used for another purpose—such as performance evaluation. Given the powerful inferences an employer might draw from an employee's biometric or other data (e.g., fitness, smoking, or nutrition habits, etc.), new safeguards against such data migration should be considered.

3. Wearable Device Data Are Relatively Easy to Re-Identify: Much privacy law and regulation depends on anonymizing or de-identifying data sets to protect privacy.[28] Unfortunately, data produced by wearable device sensors are particularly difficult to de-

[27] Ark. Code Ann. § 23-112-107(e)(3)-(4); N.D. Cent. Code § 51-07-28(6) (2007); Or. Rev. Stat. § 105.932 (2013); Va. Code Ann. § 38.2-2212(C.1)(s) (2007).
[28] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010).

identify reliably.[29] Recent research from MIT on location data streams, for example, shows that it is relatively easy to re-identify such information: researchers were able to pick out an individual mobile phone user from an anonymized data set of over 1.5 million such users using only four known data points (e.g., that the individual was at location X or Y at time A during the course of the year).[30] This is a remarkable result, and illustrative of the reality that wearable device data is prone to re-identification. The reason is simple: sensor data can capture such a rich picture of an individual that each individual in a sensor-based data set is reasonably unique and therefore identifiable. Heartbeat data, for example, has been shown to be a reliable, if unexpected, biometric identifier.[31]

This creates regulatory problems for all privacy regimes that depend on the assumption that data can be easily protected through anonymization. Specifically, easy re-identification challenges the distinction between legally protected "personally identifiable information" (PII) (e.g., name, address, social security number) and other data that the law affords lesser protection. If wearable device data sets are easily re-identifiable, then all data coming off of such devices may need to be considered personally identifiable. This ties to my suggestion above that if Congress takes up Federal data breach notification legislation, it should be careful to include biometric or other sensor-based data in its definition of PII. More broadly, Congress may need to expand the various definitions of PII found in Federal statutes to include the data created by wearable devices.

---

[29] Andrew Raij et al, *Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment*, in Chi 2011: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 11 (2011).

[30] Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Sci. Rep., Mar. 25, 2013.

[31] Yogendra Narain Singh, *Individual Identification Using Linear Projection of Heartbeat Features*, Applied Comput. Intell. & Soft Comput. (2014).

4. Meaningful Consent is Currently Lacking: Wearable devices are generally small and often have no screen or other complex user interface. As a result, showing a user a privacy policy or other agreement on the device itself is often difficult or impossible. Such privacy notifications could be shipped with the device in the box or package, but currently manufacturers generally do not provide such information.[32] Instead, consumers are left to search out privacy information on a manufacturer's web site, where it is often difficult to locate, confusing, or not specifically focused on the privacy concerns created by wearables. In particular, existing privacy policies often fail in the following respects:

- They often fail to clarify whether biometric or other sensor data collected by a wearable device is considered "personally identifiable information" under the policy;
- They often do not clarify whether consumers own and can access, control, or delete sensor data created by their wearable devices, or they specify that the manufacturer and not the consumer has such rights;
- They often do not explain what data the device collects, what sensors it deploys, and where such data are stored (e.g., on the device, on a user's smartphone, in the cloud, or on the manufacturer's servers);
- They often do not clarify to what use the manufacturer expects to put the data, with whom it will share the data, or by what constraints on use the manufacturer will abide.

Regulators must continue to work with industry to strengthen and clarify such policies, encourage manufacturers to provide such policies in multiple locations and in

[32] *See* Peppet, *supra* note __ at 142-43 (showing that none of twenty popular devices were shipped with privacy policy information in the packaging).

simple terms, and sanction firms with materially misleading policies. The Federal Trade Commission's January, 2015 report titled *Internet of Things: Privacy and Security in a Connected World* took steps in this direction. It also sought general Federal privacy legislation authorizing the Commission to mandate basic privacy protections, including privacy disclosures and consumer choice, even absent a showing of deception or unfairness.[33] Although the Commission did not seek legislation targeted directly at the Internet of Things or wearable devices particularly, it noted that generalized Federal privacy legislation would make it possible for the Commission to strengthen notice to consumers about the privacy implications of these new devices. Such legislation would be well advised to protect consumers and ensure that they continue to adopt and deploy wearable devices in their many forms.

[33] Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World* viii (Jan. 2015).