ACT | The App Association

Testimony

of
Morgan Reed
Executive Director
ACT | The App Association

on
Internet of Things

before the
Committee on the Judiciary
Subcommittee on Courts, Intellectual Property and the Internet

July 29, 2015
2141 Rayburn House Office Building

Chairman Issa, Vice Chairman Collins, Ranking Member Nadler, and distinguished members of the Committee: My name is Morgan Reed and I am the executive director of ACT | The App Association. I thank you for holding this important hearing on the internet of things (IoT).

ACT | The App Association represents more than 5,000 app companies and technology firms around the globe. As the world has quickly embraced mobile technology, our members have been creating innovative solutions to improve workplace productivity, accelerate academic achievement, and help people live healthier lives.

The App Association is spearheading an effort through our group called the Connected Health Initiative to clarify outdated health regulations, incentivize the use of remote patient monitoring, and ensure the environment is one in which patients and consumers can see improvement in their health.[1] This coalition of leading mobile health companies and key stakeholders urge Congress, the Food and Drug Administration (FDA), and Department of Health and Human Services (HHS) to adopt policies that encourage mobile health innovation and keep sensitive health data private and secure.

My goal today is to describe the current landscape of mobile health, how IoT is already dramatically improving the management of personal health and chronic medical conditions, and what is needed to ensure everyone can benefit from these new innovations.

Specifically, there are three key messages for the members of the Committee:

1. Innovation in healthcare is happening; it can lead to lowered costs, better care, and improved patient outcomes.
2. The future of health IoT will be founded on trust, which requires strong security and privacy measures.
3. Regulatory barriers, outdated laws, and lack of clarity around reimbursement are a threat to the advancement of mobile health.

Congress can, and in some cases, must play an important role in improving health outcomes for all Americans through innovative technologies.

Things: A platform for sensors

The widespread use of mobile devices has made consumers comfortable with fitness wearables, smart light bulbs, and connected refrigerators. All combined, the internet of things is projected to be worth more than $947 billion by 2019.[2]

These “things,” however, are not what’s interesting – the real power comes from the actionable insights gathered by sensors embedded in every connected device. Increasingly used in healthcare, sensors are poised to cut costs and help deliver personalized care that leads to better outcomes.[3]

As sensors become smaller, cheaper, and more accurate, wearables and other connected health technologies are set to accomplish several key milestones. Namely, they will be seamlessly interoperable, and maintenance activities that require human intervention, like syncing and charging, will be reduced or eliminated.

The collection of this information, however, is not an end in itself. Real innovation will come from the ***use*** of our data. Patients and clinicians will place greater value on companies that can best interpret sensor data to provide a clearer understanding of health conditions.

Rather than a yearly update on one’s vitals in a doctor’s office, sensors will empower people to share it with a care team, have it incorporated in a cloud-based health record, or shown on a dashboard app in just a few taps.

Big platform providers are trying to make this promise a reality – Microsoft's HealthVault now incorporates more than 371 devices into its storage and management system,[4] and Apple has created HealthKit and ResearchKit.

HealthKit allows health apps and devices to work together in one safe, secure place, providing a user with a complete picture of their health via the Health app. The open source ResearchKit platform makes it easy for researchers and developers to create apps that can incorporate the health data collected by devices in medical studies.[5]

Yet, with all this promise, a recent survey of healthcare providers found that only 15 percent are discussing wearables with patients. This, despite the same physicians saying that nearly half of patients not currently using wearables and apps could benefit from doing so.[6]

Why?

Questions about privacy, security, reimbursement, and government regulation meet to create an environment where companies are worried about making devices more medically relevant, and physicians worry about the impact on their practices.

Patients and care providers must also know that their information is private and secure. Industry best practices around the treatment of sensitive health data, as well as a commitment from government to support these practices, are important to establish trust and push this industry forward.

Getting health IoT right

Our members understand the importance that patient trust plays in an effective healthcare system, and work to keep sensitive health data secure and private.

Connected solutions like those made by App Association member AirStrip® provide a model example of health IoT in a care setting. During an emergency situation, AirStrip® technology is critical to keeping doctors informed on patient vitals while they're still in the ambulance. The company's products use Department of Defense-level encryption that allow doctors to remotely view live patient waveform data from multiple devices and systems on a single mobile screen – all before entering a hospital room.

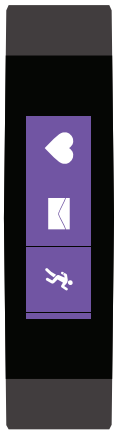
Connected devices have also become an important tool for consumers trying to reach a wellness goal. Whether it's diet tracking and step counting for weight loss, or monitoring heart rate and improving form to train for a marathon, the internet of things has become integral to health and fitness. While wearables and connected health technologies are being purchased at astonishing rates, privacy and security concerns remain.

Sixty-eight percent of consumers say they want a wearable paid for by their insurer in exchange for anonymous data. But if asked to give personally identifiable information, users shift dramatically in the other direction, with most opposing the use of any health data for targeted, interest-based, or behavioral advertising.[7]

It's clear that average consumers and patients with chronic conditions see value in the use of connected health technologies, but they don't want to give up their privacy, and doctors want to know they will be reimbursed for using them. The mobile health industry and other stakeholders must meet these expectations for innovation in this life-saving space to continue.

Once these questions are answered, wearables and other connected devices – including those already on the market – will provide useful insights for care providers. It will lead to earlier detection of irregularities, more accurate diagnoses, and improved care overall.

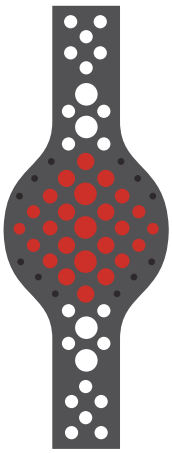
Wearables improve fitness & provide important insights



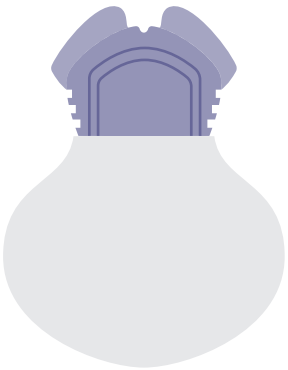
The Microsoft Band includes exercise tracking, guided workouts, and a real-time heart rate monitor

The Apple Watch is packed with sensors that measure move-ment, heart rate, calories burned, and other vitals

The Netatmo JUNE contains UVA and UVB sensors that precisely measure sun exposure



The MOOV NOW uses motion sensors to analyze and correct a user's form during exercise



Medtronic continuous glucose monitors use sensors embedded under the skin to measure glucose levels every few minutes

Landscape

88%

Percentage of health organizations that say cloud computing has cut costs

86%

Percentage of clinicians who say apps will be critical to patient care

$3

Savings f
mon

Sources: PwC, CDW, Juniper Research, Marketresearch.com, Accenture[8]

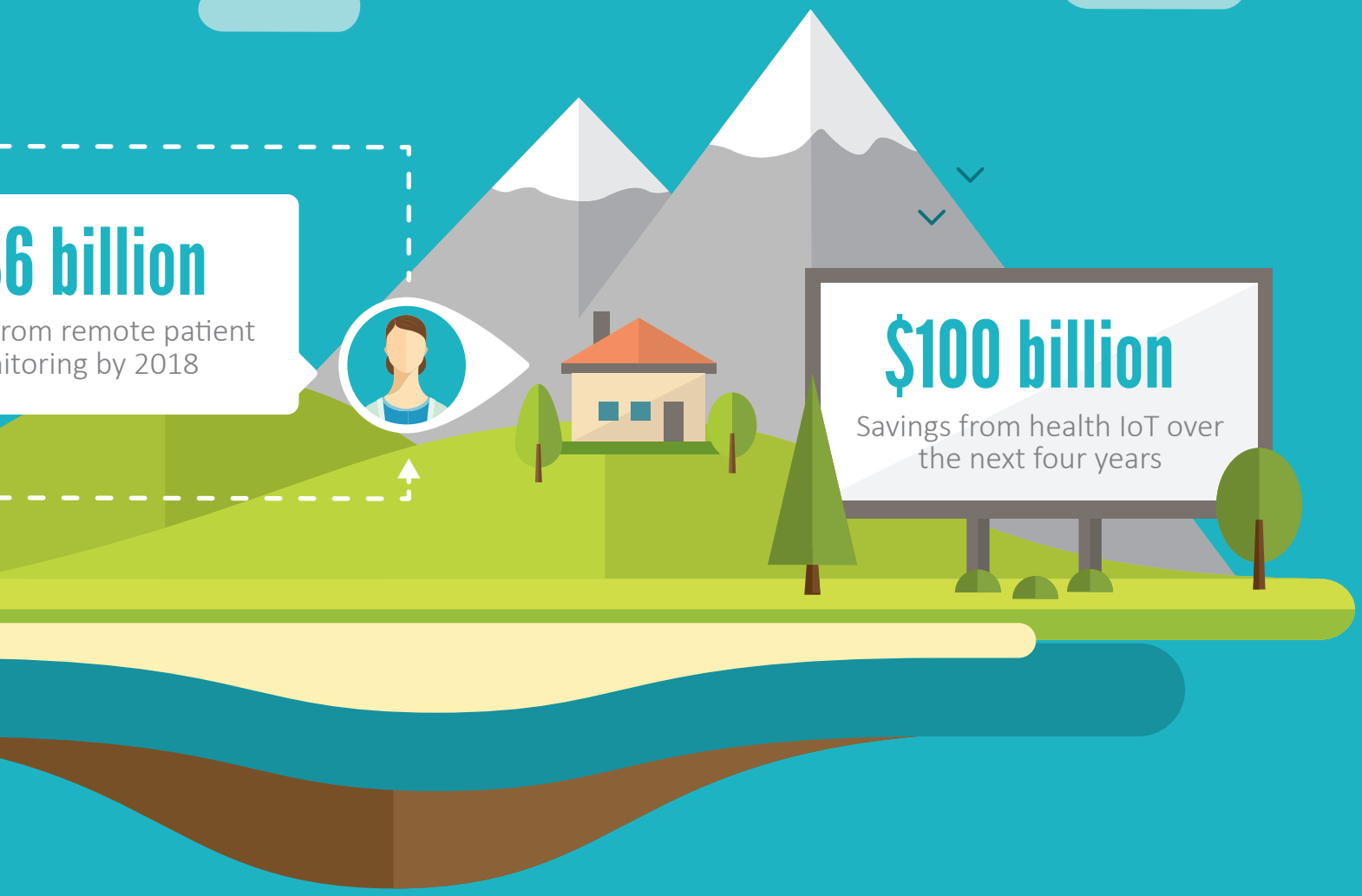
# of Healthcare IoT

$117 billion

Size of health IoT marketplace by 2020

6 billion

rom remote patient
itoring by 2018



$100 billion

Savings from health IoT over the next four years

ACT | The App Association

Case in point: The aging U.S. population

By 2050, there will be 83.7 million Americans over age 65 – twice the amount from 2012.[9] Eighty percent will have at least one chronic condition.[10] With a large portion living in rural areas or far from loved ones who could offer support, the age group's rapid growth will severely strain public and private health resources.[11]

Advanced personal emergency response systems (PERS) are the key to empowering older populations and helping them live comfortably in their homes years longer than today's norm.

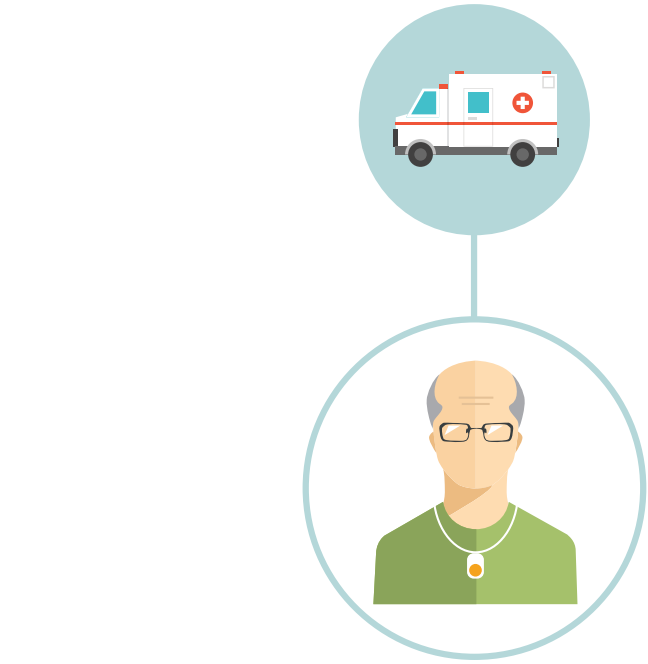
Today, a PERS is typically a single button worn around the neck that directly connects to emergency services when pushed.

A far more sophisticated PERS will be packed with sensors that can track blood sugar, blood pressure, heart rate, biomarkers for medication adherence, geofencing for Alzheimer's patients, and much more. These sensors will be small enough to fit in a watch and will connect to a loved one's phone, a physician's tablet, and a medical record system.

Non-wearables will matter as well, and there are some products already helping our rapidly aging population. The Beddit is a mattress strap that monitors heart rate and sleep patterns.

Even more sophisticated technology, such as the Microsoft Kinect, is used by physical therapists to allow patients to do therapy at home after a knee replacement, while still accurately measuring flex and strength.

This increasingly connected approach to healthcare will lower costs,[12] empower aging populations to live at home longer, and allow physicians and loved ones to help with care in an efficient way. Individuals and their care teams will also have a more complete view of health information, allowing for earlier detection of issues.



PERS of today

PERS of the future

Barriers to health IoT

For this vision of the future to become a reality, there is much work to be done. First, the industry must demonstrate the effectiveness of these technologies. Just as important, innovators must be able to keep sensitive health data private and secure. Lastly, doctors must know that they will be compensated for using these connected solutions.

Our member companies must be able to ensure the security and privacy of sensitive health data to earn the trust of consumers, hospital systems, and care providers. The use of end-to-end encryption is a critical element to accomplishing this.

Recent statements by top law enforcement officials asking companies to weaken security measures threaten that ability. They also reduce the likelihood that health IoT will be implemented in a care setting, and prevent U.S. products from expanding to overseas markets. These requests are coming at the very moment the Office of Personnel Management's (OPM) failure to properly encrypt has led to an incredibly large, potentially harmful, breach. Further, it is in direct conflict with recommendations for encryption of electronic health information by the Department of Health and Human Services (HHS).

Uncertainty around data storage and the cloud is also hampering advancement in IoT. With the grossly outdated Electronic Communications Privacy Act (ECPA) governing electronic data, the law allows for the warrantless search of electronic communications after 180 days – no matter if it's sensitive health information, or private emails.

In the confusion, the U.S. Department of Justice (DOJ) has claimed ECPA gives them the authority to use a warrant to force companies to turn over data of non-U.S. citizens when that data is located outside the United States. This is in stark contrast to the process DOJ goes through to get physical data, creating uncertainty that keeps innovative companies out of the market, therefore hampering advancement in this space.

This problem can't be fixed without action from Congress. The LEADS Act (H.R. 1174) provides the appropriate balance between the needs of law enforcement to conduct criminal investigations and the demand for privacy both at home and by our trading partners overseas.

Having the ability to tell doctors and health systems that a connected health solution is secure, private, and effective is key to moving forward. But, care providers must also know that they will be compensated for the time they spend treating patients using these technologies. There is currently no consistent model for reimbursement around medical devices and apps.

Reimbursing medical practitioners for using connected devices and the data they generate will break down barriers to entry and incentivize companies to go farther, build bigger, and pioneer new things in mobile health. That means better solutions for patients and medical practitioners, reduced healthcare costs, and more opportunities for tech companies.

The pathway to success in the mobile health marketplace requires protecting sensitive information. But for innovators to best achieve this, there must be a commitment from the federal government to update outdated laws, regulation, and guidance.

Conclusion

The internet of things will continue to provide incredible opportunities for innovators. As sensors become more sophisticated, so too will the things in our lives – things that will help lower the cost of healthcare and ultimately improve patient outcomes. We need your help to ensure this future can be a reality for Americans who are eager to embrace connected health solutions.

The success of mobile health is founded on trust. To establish trust, our companies must be able to keep sensitive health data secure and private. While there's currently no legislation on encryption, we ask that you take seriously any government efforts that would require companies to put citizens' data at risk.

Further, we ask that you support the LEADS Act, which would provide clear legal framework for law enforcement agencies to access data stored abroad. It will provide clarity for innovators in this space, and help keep private health data secure.

I thank you again for the opportunity to present testimony about the extraordinary health IoT marketplace. I look forward to our continued work together and pledge our support to help advance measures that promote innovation and foster growth in this space.

End Notes

1 “Connected Health Initiative.” Available at: http://connectedhi.com.

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 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 “Digital Health Solutions Expected to Save U.S. Healthcare System More Than $100 Billion Over Next Four Years,” Accenture (June 2015). Available at: https://www.accenture.com/us-en/Pages/insight-patient-engagement-colossal-clash-disrupt-infographic.aspx.

4 “HealthVault,” Available at: https://account.healthvault.com/us/en-US/Directory.

5 “ResearchKit,” Available at: https://www.apple.com/researchkit/.

6 “Physician recommendations of personal health wearables and apps: a channel to drive consumer adoption?” MedPanel (June 2015). Available at: http://medpanel.com/Expert-Insight/Reports-Tools.aspx.

7 “Health wearables: Early days,” PWC (2014). Available at: http://www.pwc.com/us/en/health-industries/healthcare-new-entrants/index.jhtml.

8 “117 Billion Market For Internet of Things in Healthcare By 2020,” MarketResearch.com (April 2015). Available at: http://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/?ss=tech; “Issue 2: Making the leap from mobile app to medical device,” PwC (2015). Available at: http://www.pwc.com/us/en/health-industries/top-health-industry-issues/mhealth.jhtml; “Remote Patient Monitoring: Can it Be A Solutions to a Key Healthcare Problem?,” Juniper Research (2013). Available at: http://www.healthcare-informatics.com/blogs/rajiv-leventhal/remote-patient-monitoring-can-it-be-solution-key-healthcare-problem?page=2; “Top health industry issues of 2015,” PwC (December 2014). Available at: http://www.pwc.com/en_US/us/health-industries/top-health-industry-issues/assets/pwc-hri-top-healthcare-issues-2015.pdf; “Digital Health Solutions Expected to Save U.S. Healthcare System More Than $100 Billion Over Next Four Years,” Accenture (June 2015). Available at: https://www.accenture.com/us-en/Pages/insight-patient-engagement-colossal-clash-disrupt-infographic.aspx.

9 “An Aging Nation: The Older Population in the United States,” United States Census Bureau (May 2014). Available at: http://www.census.gov/prod/2014pubs/p25-1140.pdf.

10 “Healthy Aging: Improving and Extending Quality of Life Among Older Americans,” Center for Disease Control and Prevention (2009). Available at: http://www.cdc.gov/nccdphp/publications/aag/pdf/healthy_aging.pdf.

11 “Housing an Aging Rural America: Rural Seniors and their Homes,” Housing Assistance Council (October 2014). Available at: http://ruralhome.org/storage/documents/publications/rrreports/ruralseniors2014.pdf.

12 “The Boomer Challenge,” Hospitals & Health Networks (January 2014). Available at: http://www.hhnmag.com/Magazine/2014/Jan/cover-story-baby-boomers.

ACT | The App Association

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130
@ACTonline
ACTonline.org
/actonline.org