Weared Data; the Personal and Proprietary Nature of Data on Wearable Technology Devices

Dr. Michael Conyette

Contents

- Rising demand for wearables.
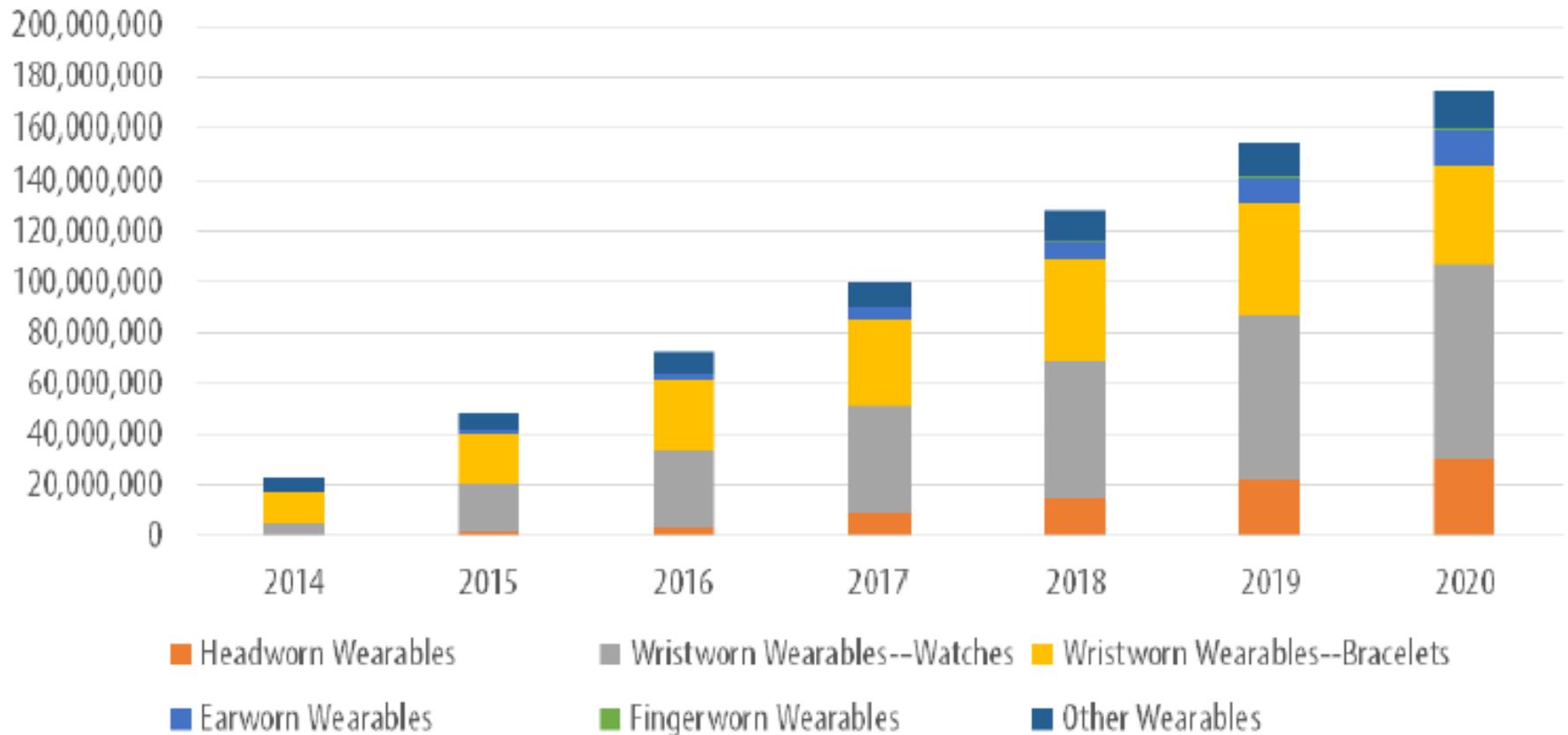- Driving factors for adoption.
- Changing marketplace for new generation of wearables.
- *Weared Data* security issues.
- Wearables in travel and museums.

Smart Wearables Forecast

Wearable tech devices arrive

- Pricewaterhouse Coopers forecasts sales of wearables could reach over 130 million units and gross almost $6 billion by 2018.

- Big Data could see a rival through the unique *Weared Data* created by wearables.

- *Weared Data* is subject to security breaches.

Wearable tech driving factors

- Adoption of lightweight messaging standards that push traditionally heavy messages to smaller devices (Joyce, 2013).

- Efficient messaging makes it possible to send data (rich notifications including status updates, comments, photo tags, check-ins, data) to wearable devices like a smart watch.

Past developments with Mobile

- 2008 - milestone is the mobile revolution. Apple launched its first iPhone earlier, and made the iOS SDK available for third party developers.

- Hilton - first to introduce its mobile app for iPhone in November 2009.

- In 2010 - US volume of mobile phone sales surpassed PC sales.

- Smartphones comprised twice as much usage as tablet devices.

Other driving factors

- Wearable computing is a natural evolution of smartphone technology.

- Availability of lower cost MEMS sensors - miniaturized accelerometers, gyroscopes, microphones, digital mirror displays.

- Standardization in protocols for connecting devices and interoperability of devices.

Predictions for Wearables

- Acquisitions between software and hardware vendors means powerful wearables providing more than simple streams of data and metrics.
- Internet connectivity and complex data used on these devices will make them more of a target to cyber threats.
- Wearables may eclipse smartphones in the future.
- The role of technology will change from supporting mediation to embodiment.

Wearables used in travel industry

- Disney's MagicBands
- Royal Caribbean Cruiselines wristbands
- Westin Hotels "Heavenly" sleep bracelet
- TripCase travel notifications sent directly to Samsung Gear S smartwatch
- Smart luggage – Bluesmart, Trunkster, Samsonite
- Virgin Atlantic, EasyJet
- Various museums – smart glasses, EEG biosensor

Disney's MagicBands

- Wristbands instead of hotel room keys.
- They contain a radio-frequency identification (RFID) chip and a radio.
- Contains a near field communication (NFC) chip.
- Connects a guest to a large system of sensors within a theme park.

Disney's MagicBands

A MagicBand is detected at short-range touch points and also by long-range readers to deliver personalized experiences, as well as provide information that helps Disney improve the experience to visitors.

Wearable tech sleeping in hotels

Wearable notifications by hotels

Wearable tech in museums

Wear Geared's
Museum Glasses

- *Museum Glasses* prototype application on Epson Moverio BT-200 smartglasses platform and augmented reality (AR) software.

- 'Look-through' binocular lens - museum visitors can switch between real objects and AR.

- Look at real artifacts through the glasses and also trigger associated digital content such as videos, games, photos, or audio on the smartglasses.

Epson Smart Glasses

Augmented Reality in a museum
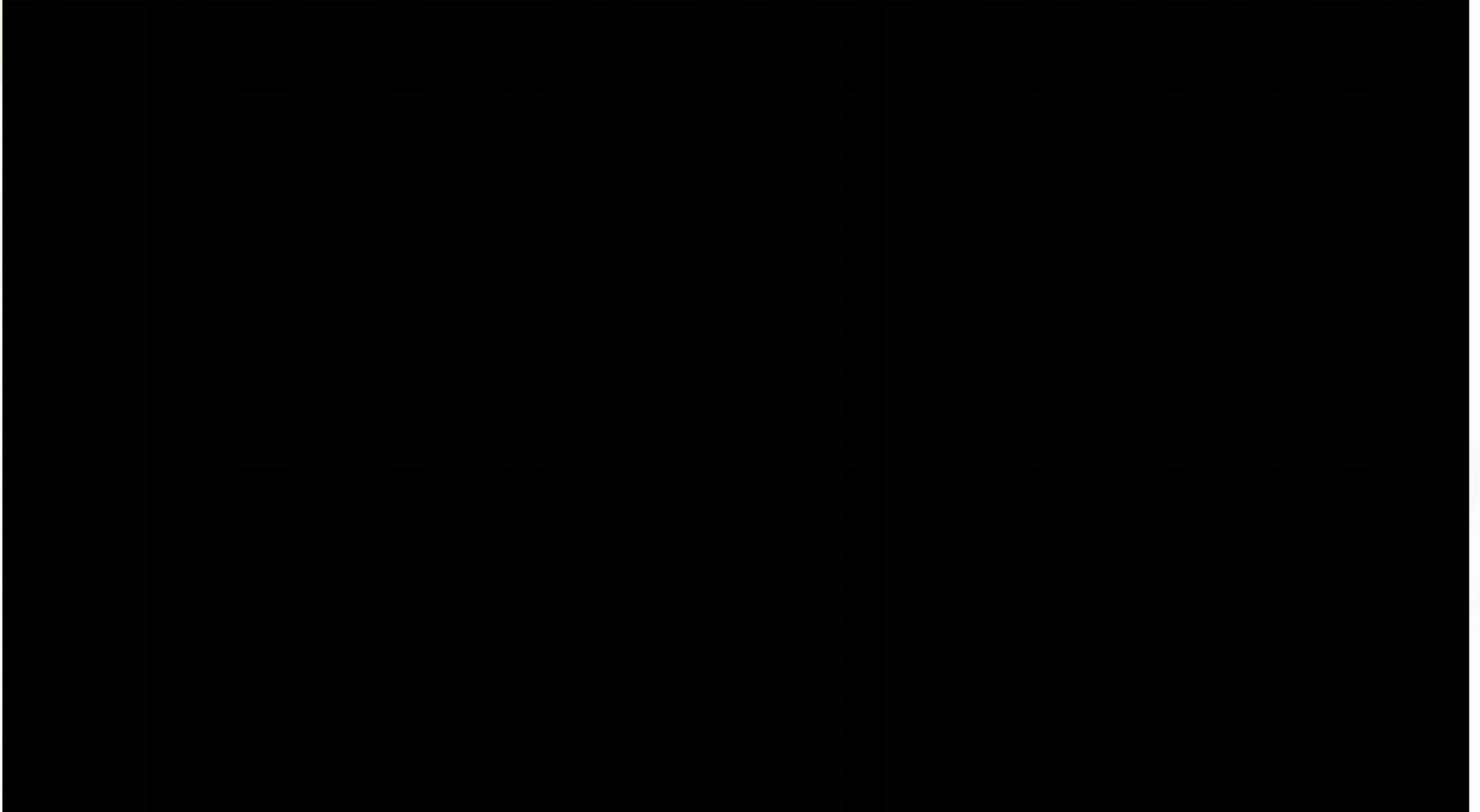
Museum interactivity
Imagine wearing smart glasses on a visit

Conclusions

- Mobile travel means wearables will be used.
- Consumers demanding more than simple streams of data and metrics means wearable tech rivals design advanced generations.
- Increased complexity of information collected on these devices is also deeply personal to consumers & proprietary to users.
- Using wearables could put travelers more at risk for identity theft, profiling, and stalking.

Conclusions & wearables

- Other related devices such as injestables, embedables, and implantables which could eventually be added to IoT.

- Now is the opportune time to consider the security implications of the proliferation of such devices.

- *Weared Data* needs to be appropriately valued, guarded and secured.

Details of 8 devices studied in the Open Effect / Citizen Lab research report

Device	App	Data encryption	Tamper-proof	ID privacy
Apple Watch	Watch	Yes	Not tested	Yes
Basis Peak	Basis Peak 1.14.0	Yes	Not tested	No
FitBit Charge HR	FitBit 2.10	Yes	Yes	No
Garmin Vivosmart	Garmin Connect	No	No	No
Jawbone UP 2	Jawbone UP 4.7.0	Yes	No	No
Mio Fuse	Mio GO 2.4.4	Not Applicable	Not Applicable	No
Withings Pulse O2	Withings Health Mate 2.09.00	Partial	No	No
Xiaomi Mi Band	Mi Fit 1.6.122	Yes	Partial	No