Security, Privacy, and Ethics in Mobile Development

CSE 162 – Mobile Computing

Hua Huang
Department of Computer Science and Engineering
University of California, Merced

Ethical Issues in Mobile Development

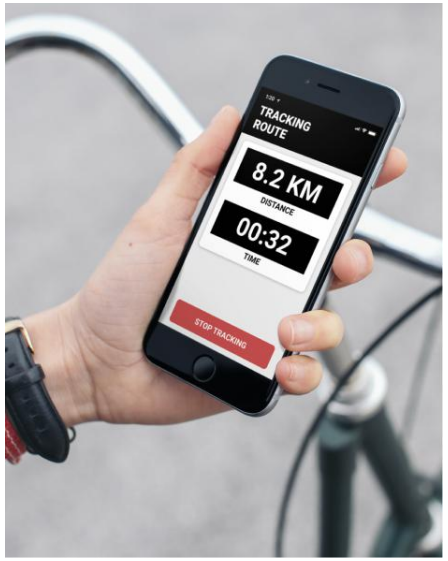
What sensitive information can be collected by mobile systems?

- Video
- Sounds
- GPS
- Locations
- User’s self reported information
- Many more!

- All with one unified API, and cheap

Examples of Legitimate Apps

- Assess pedestrian or bike friendliness of neighborhoods.
- Use the location awareness to understand the user's exposure to air pollution as they move around.
- Use phones to snap, tag and upload photos of community events



Ethical Issues in Mobile Sensing

- Privacy: control over personal data
- Consent: Informed permission
- Equity: fairness in how individuals are treated
- Social forgetting: purposeful discarding of information about individuals in order to enable forgiveness, recovery, or a clean slate.

Privacy

- Mobile systems can gather significant amounts of data about the users.
- However, the data can be subpoenaed, or be demanded by U.S. authorities without warrant
- Unauthorized sharing or data theft can occur at a variety of places
- Complicated end-user licensing agreements may lead users to give away broad rights to share their data in return for services.

Recap: Privacy Preserving in Crowdsensing

- Approaches to protect the data
- Examples:
  - **Anonymization**
  - **Encryption**
  - **Obfuscation**: Adding distracting or misleading data to a log or profile.

Considerations: Privacy vs Functionality

- Commerce can suffer from strong privacy rights, as there is less information for both producers and consumers in the marketplace
  - Example electronic payments, and ant-money-laundering

- Truthfulness, openness, and accountability can suffer at the hands of strict privacy protections
  - Example: new algorithms for mobile sensing that allow users to replace sensitive location data with believable but fake data

Consent

- Consent is a value central to data policies in the United States. A critical component of respect, beneficence and justice is informed consent.

Challenges in Consent

- Consent in mobile apps is complicated by relying on ubiquitous devices.
  - Opting out of the mobile phone network is not a realistic option.
  - In 2011, Apple and Android were storing location data over and beyond what users were notified of and consented to
- Financial interest can conflict with consents
  - Use data to produce targeted advertising, sell valuable behavioral data to third parties, or use location to hone price or product discrimination
- Secondary, unforeseen purposes of data use
  - motion data can infer Parkinson’s disease

Soft Surveillance

- A technique used by agents of power, such as governments, to collect seemingly voluntary but actually mandatary data.
  - Example: searches to enter planes
  - Example: Withheld Social Security benefits if people do not “voluntarily” submit personal information
- Mobile sensing systems can easily become soft surveillance systems
  - Everywhere, all time presence
  - People can be involved by simply agreeing to data collection

Equity

- Fairness and justice in how individuals are treated
- If powerful institutions gather data from relatively less powerful individuals, mobile sensing could tilt towards control and increased surveillance
- Alternatively, distributed sensing and analysis could shape technologies of care or even empowerment.
- Besides, the availability of mobile phones enables systematic data collection with radically lower cost, which enables data-driven decision-making to small institutions and community groups

Social Forgetting

- Purposeful discarding of information to enable forgiveness and a clean slate

- Mobile sensing can create a record of people's movements, habits, and routines that persists
  - A subject of both celebration and concern

Pros and Cons of persistent records

- Pros
  - Augment human memory. Can improve healthcare, and enable memory bank to relive past events.
- Cons
  - Unintended loss of fresh start
  - Increased surveillance

Solution

- The “right to be forgotten”.
  - A combination of policies and technologies that allow for the gradual decay of digital data.

More info

- EU General Data Protection Regulation
- California Consumer Privacy Act

Privacy Policy

Creating a Privacy Policy

- A privacy policy is a document created to go with a product (app, website, etc.) that describes how the product and company behind it will do the following with a customer or client's data:
  - Gather
  - Use
  - Disclose
  - Manage

Creating a Privacy Policy

- Ask yourself some questions:
  - What data is collected?
  - How it is collected?
  - What you will/can do with it?
  - What will happen to it after X amount of time?
  - Is it anonymous?
  - Are there ads?
  - Is the data shared with another organization?
  - … and more…

You need a privacy policy because...

- You are collecting personal data
- You are using a third-party service
- Government regulations
- App Store regulations
- Risk alienating customers
- Open to lawsuits

What's in a policy?

- **Information** - what personal information is being collected on the site
- **Choice** - what options the customer has about how/whether her data is collected and used
- **Access** - how a customer can see what data has been collected and change/correct it if necessary

What’s in a policy?

- **Security** - state how any data that is collected is stored/protected
- **Redress** - what customer can do if privacy policy is not met
- **Updates** - how policy changes will be communicated

Example Policies

- Google: https://www.google.com/policies/privacy/
- Apple: http://www.apple.com/legal/privacy/en-ww/
- Facebook: https://www.facebook.com/policy.php
- Twitter: https://twitter.com/privacy?lang=en

Example Policies

- Note that these are mainly in “regular, plain English!”
- Movement away from “legalese”
- Some privacy policies were automatically processed

What does a privacy policy get you?

- Disclosure of what’s going on
- A level of trust with developer
- Meeting requirements from publishers / government agencies

Example

- Google Analytics is one of the most popular digital analytics software.
  - Allows you to analyze details about the visitors on your website and design strategy to improve business
- If you've enabled any Google Analytics Advertising features, you are required to notify your users:
  - What features you've implemented.
  - How you and third-party vendors use first-party
  - How visitors can opt-out of the Google Analytics Advertising

https://support.google.com/analytics/answer/2700409?hl=en

Beyond Policies

- Writing down what you do is good…
- … following it is even better
- Remember: privacy is not security
- The privacy policy says what you are collecting and what you plan to do
- And absence of this does not mean you shouldn’t protect data you collect!

Wearables (1)

CSE 162 – Mobile Computing

Hua Huang
Department of Computer Science and Engineering
University of California, Merced

In this lecture

- What is wearable computing
- Wearable sensing technologies
- Challenges in wearable computing

- The term “wearable computing” is really built around any device that is attached or worn in some way

- So, the possibilities here are vast
  - Smartwatch
  - Continuous health monitoring
  - Brain-computer interface
  - More

Everyday Realistic Wearable Technology

- What most people think about is watches and/or bracelets
- Smart Watches
  - Apple Watch - https://www.apple.com/watch/
  - Android Wear - https://www.android.com/wear/
  - Some proprietary watches
- Personal Fitness Devices
  - Fitbit - https://www.fitbit.com/home
  - Other devices

What is a wearable computer?

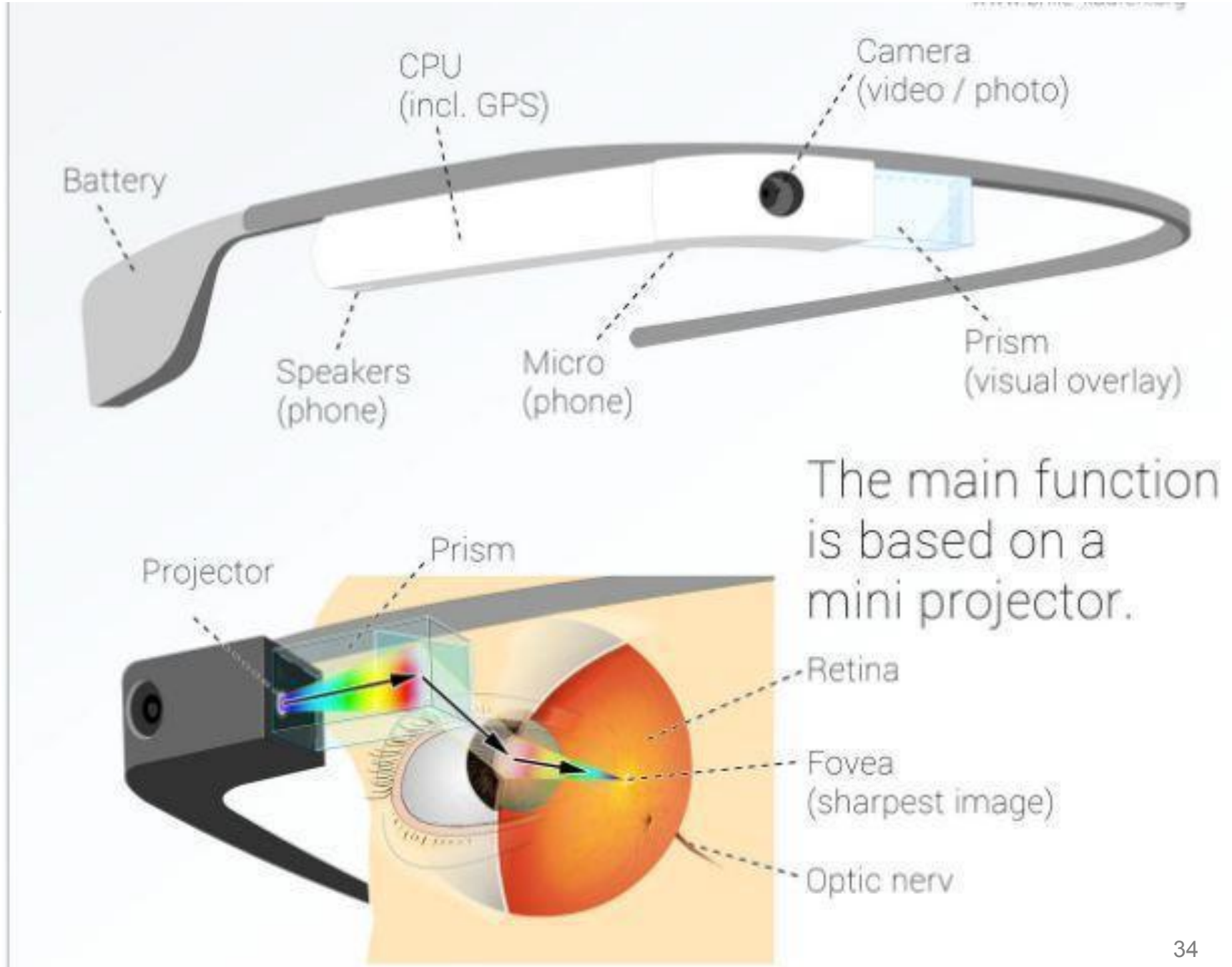
- A computer that is
  - Portable while operational
  - Enables hands-free/hands-limited use
  - Able to get the user's attention
  - Is always on, acting on behalf of the user
  - Able to sense the user's current context

Rhodes, B. J. (1997). The wearable remembrance agent: A system for augmented memory. Personal Technologies, 1(4), 218-224.

Wearable Devices

Smart glasses

- Head Mounted Display (HMD)
- Head Up Display (HUD)



View Through Google Glass

- Always available peripheral information display
  - Combining computing, communications and content capture

Smart watches

Foundation
Mechanical wrist watches established

1880

Imagination
Couldn't a watch do much more?

1940

Electronification
Quartz watches revolutionize the industry

1970

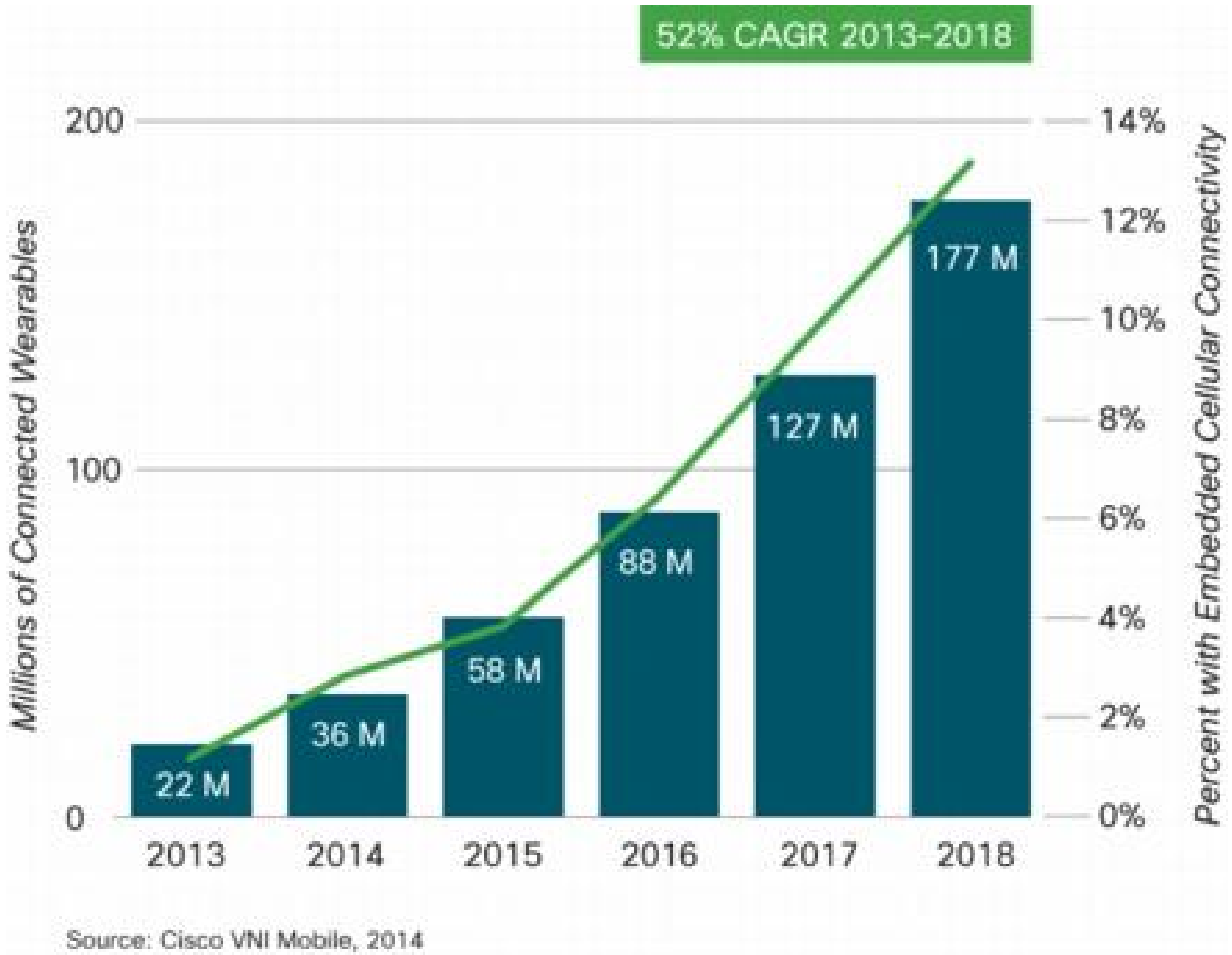
Experimentation
1st smartwatches, but no commercial success

1990

Commercialization
Smartwatches start to sell

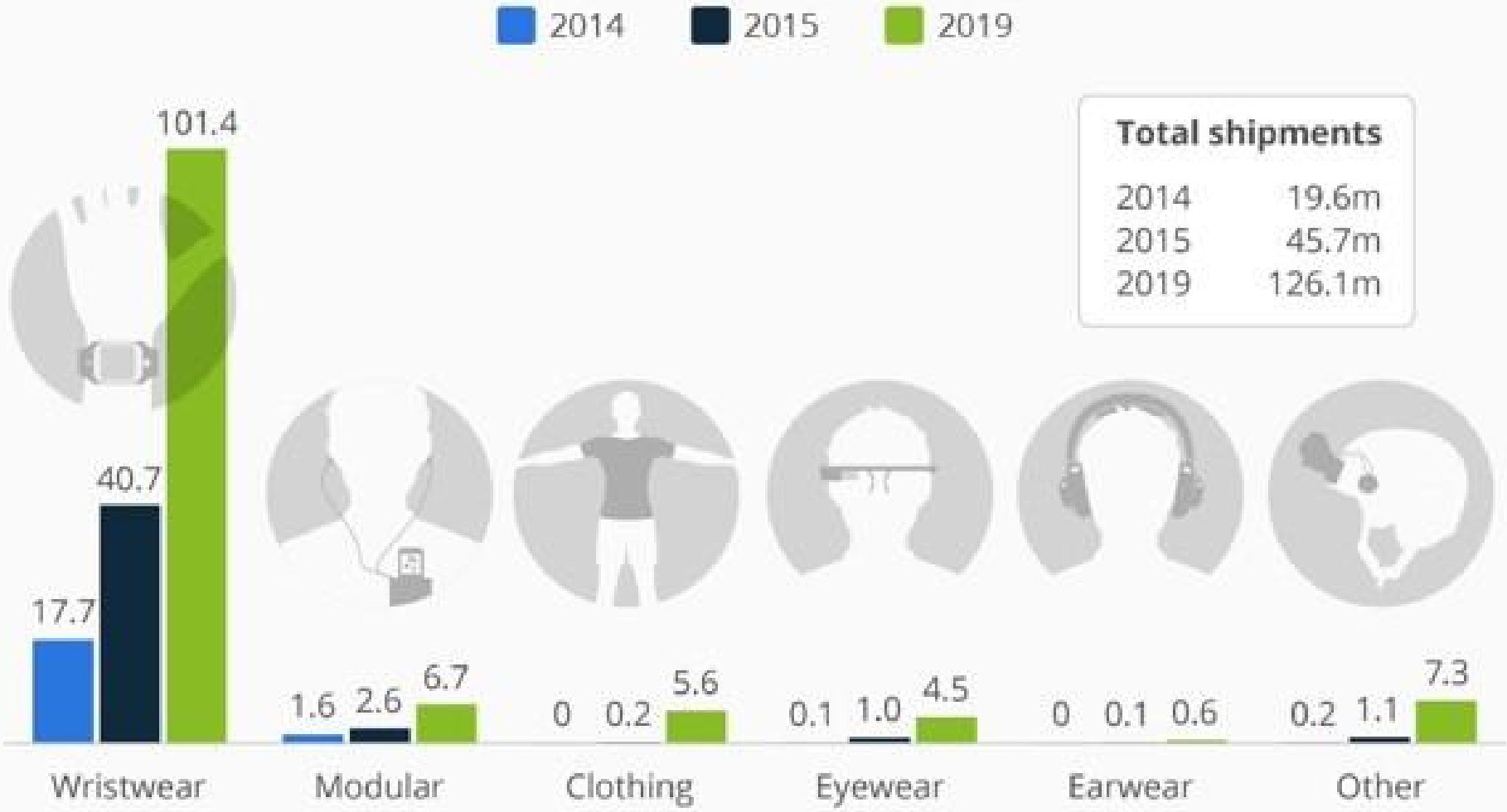
2010

Number of Smartwatches Shipped



The Predicted Wearables Boom Is All About The Wrist

Worldwide wearable device shipment forecast (in million units)



@StatistaCharts Source: IDC

statista

Smart earplugs

- An emerging computing platform
- New features
  - Augmented acoustic reality
  - Real-time translation
  - Monitor biometrics
  - Fitness coaching
  - Biometric identification

Intra-oral sensing

- “Sensor-Embedded Teeth for Oral Activity”

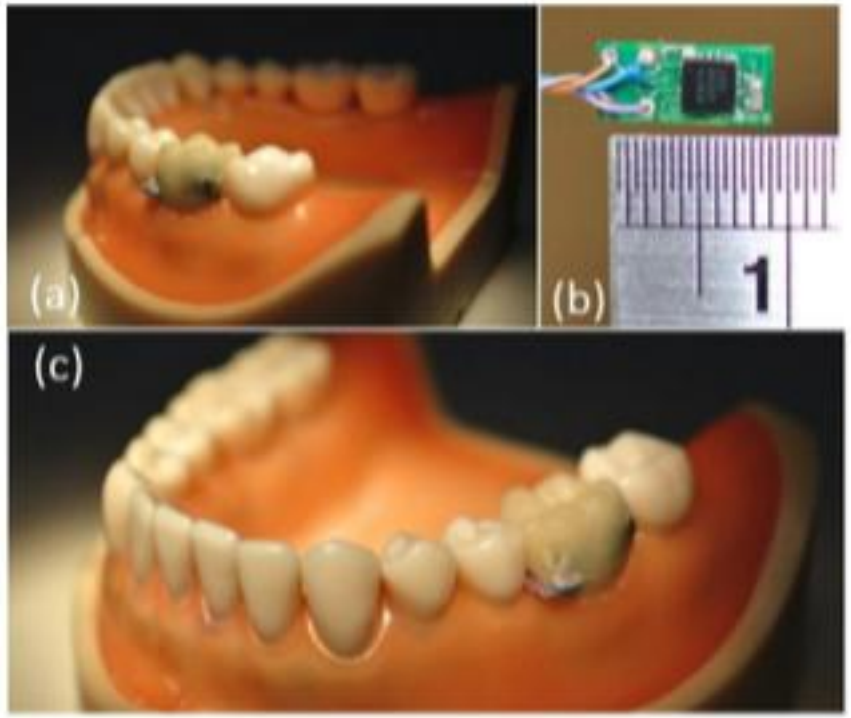


Figure 1. The breakout board with (b) tri-axial accelerometer and (a)(c) sensor embedded denture.

Why discuss this in mobile?

- They are, by definition, mobile devices
- They often run versions of the operating systems we are already working with (Android Wear ⇔ Android)

- The wearable devices often work best when paired with a phone or other mobile device
- Many wearable apps come as part of a pair with a phone version

Ideal Attributes

- Persist and provide constant access to information services.
  - Everyday and continuous use.
  - Wearable can interact with the user at any given time.
  - The user can access the wearable quickly and with little effort.

- Sense and model context.
  - The wearable can observe and model the user's environment, physical and mental state.

- Adapt interaction modalities based on the user's context.
  - The wearable should adapt its input and output modalities automatically to those that are most appropriate and socially graceful at the time.

Why use wearable computers?

- Some people wear too many computers.
  - PDA, cellular phone, pager, laptop, electronic translator, and a calculator.
  - Mp3 player, audio digitizers, digital camera.
- These devices all contain very similar components.
  - Microprocessor, memory, screen, keyboard, battery, and in some cases, a wireless modem.
  - The main distinctions between these devices are the interface and the application software.
- Wearable computers could exploit the commonality in components to eliminate cost, weight and redundancy.

Mediate interactions

- Wearable computers will help provide a consistent interface to computationally augmented objects in the physical world.
  - Example—Gesture Pendant.
  - One gesture could provide an intuitive command for many devices.

Aid communication

- The wearable can also assist in human-to-human communication.
- Wearable computers can also help manage interruption in the user’s daily life.

Augment reality

- Augmented reality overlays information-rich virtual realities onto the physical world.
- In a sense, augmented reality is a combination of the application domains described previously.

Wearable App Development

Android Wear

- Released in 2014
- Android Wear devices were initially designed to be second screens, but can be used independently in more situations
- Like Android itself, Wear can be adapted to many different devices
- Uses the same UI theme that the rest of Android uses

Use Cases

- Telling time
- OK Google
- Notifications and quick replies
- Phone app control (like music, for example)
- Fitness
- Basic functions (alarms, stopwatch, etc.)
- Mobile Payment

When do you want a watch app?

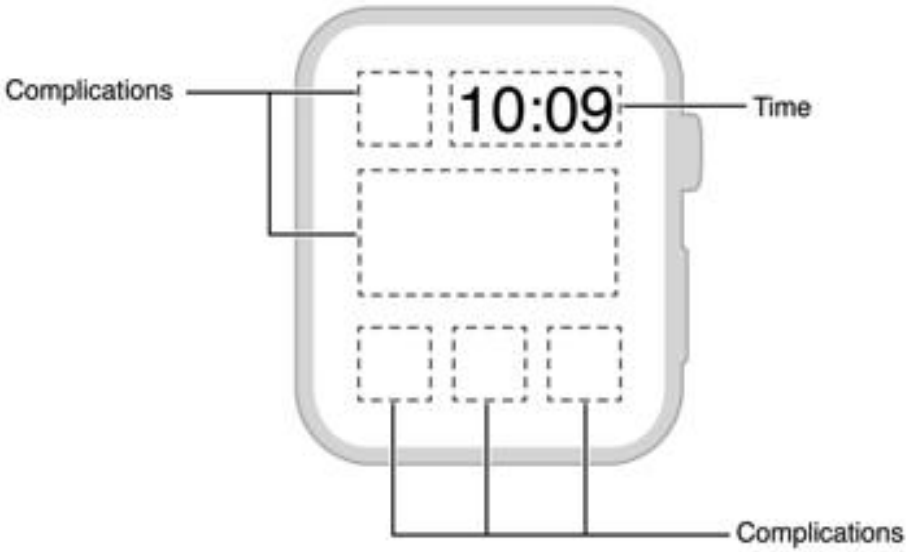
- Good Watch Apps
  - Buy Me a Pie (grocery list)
  - Seven Minute Workout (works with sensors)
  - Due (reminders)
  - Google Maps (directions on your wrist!)
  - Pandora (control your music)
  - Shazaam (what is that song?)
  - Weather Underground (quick weather forecast)

When do you want a watch app?

- Odd Watch Apps
  - Chipotle?
  - FlightRadar?
  - Fandango?
  - AAA?
  - Amazon?

Questions to Consider

- UI concerns regarding touch size and screen size become even more problematic...



Alert

SideBySideButtonsAlert

ActionSheet

Questions to consider

- Would a watch app add anything to my full app?
  - What additional sensing can the watch provide?
  - Can the information be shown in a very small format?
  - Are there simple controls to the app that could be added to a watch?
- What type of interaction do you want the user to have?