REGULATION OF HEALTH DATA TRACKERS

Governing Emerging Technologies Conference
Phoenix, AZ
May 29, 2014

TIMOTHY S. HALL
Professor of Law
Louis D. Brandeis School of Law
University of Louisville

HEALTH (FITNESS) DATA TRACKING

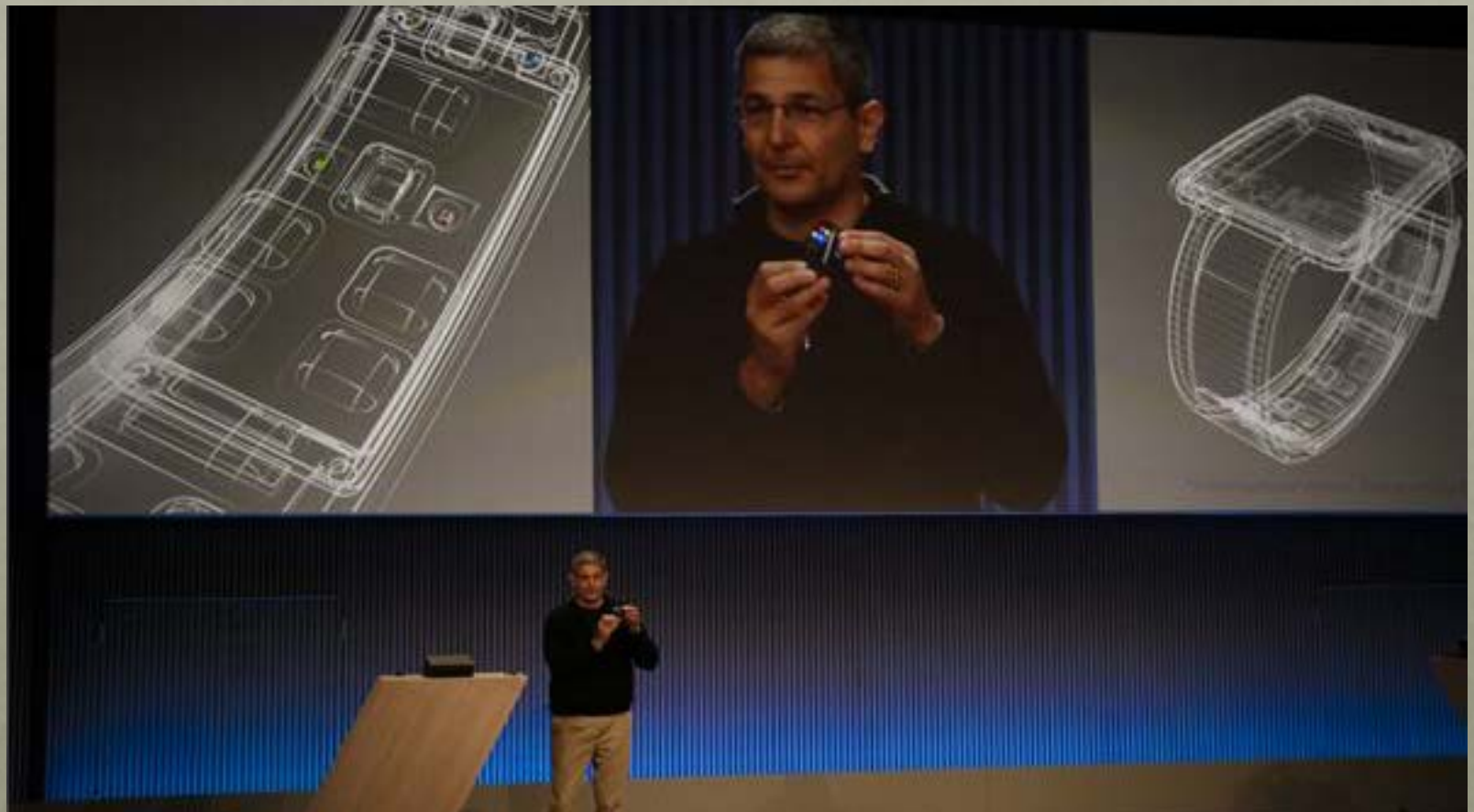
- Includes emerging market of wearables, "connected" fitness devices, apps.
- Health & Fitness App use up almost 50% in 2013.
- 25% of smartphone users, 20% of tablet users estimated to use devices to track health or fitness.
- 156,000,000 health app downloads in 2012 – projected to grow to to 248,000,000 by 2017
- This is something that people want.

WEARABLES

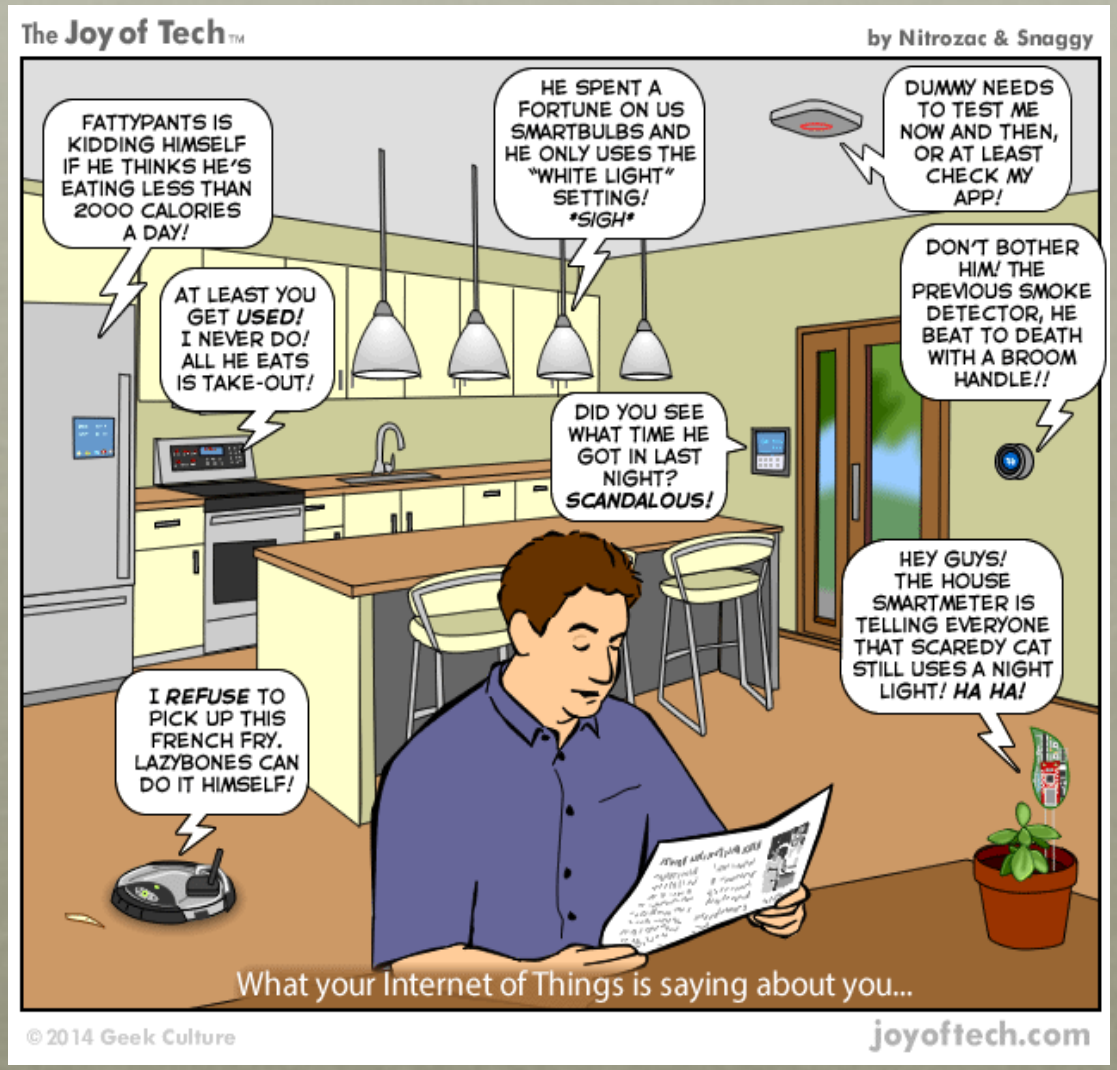
- Apple “Healthbook” probably the most anticipated iOS8 feature
  - (June WWDC? Who knows?)
- Fitbit, Jawbone currently lead the market

AND JUST YESTERDAY

Samsung Announces Agenda for Modular Health Tracking System



THE INTERNET OF THINGS



WHAT IS BEING COLLECTED?

- Activity Tracking
- Nutritional Information
- Basic Vital Signs
  - Heartrate / Pulse
- Sleep Duration and Quality
- Basic imaging with device cameras
- The list will grow and the data will improve in quality and automation.

What can the data tell us?

- Individually
  - Baseline assessment of fitness data
  - Tracking changes over time
  - Incentives to improve health markers
    - Pairing with other social media (Facebook, etc.)
    - Goal-setting, either by individuals, across social media groups, or by the app or service itself

WHAT CAN THE DATA TELL US?

- Aggregated ("Big Data")
- In many ways, this is the promise of health data tracking
- Sheer size of the data sets may enable "data mining" of basic health data that would be impossible or impracticable in a clinical setting
- Power of Big Data predictive analytics applied to basic health information in a way it cannot with EMR information.
- Individually- generated data may be combined with other consumer data currently held by data brokers

PRIVACY CONCERNS

- Are data identifiable?
- What are the limits on use of data?
- What are the limits on disclosure of data?
- Can individually innocuous data points be aggregated to provide accurate, intrusively predictive results?
- Can my data be accessed by others?
  - Employer or potential or past employer?
  - Insurers?
  - Government/ Law Enforcement?

VALUING PRIVACY?


LEMONADE
JDator
"It's free, but they sell your information."


geek
ISN'T IT GREAT? WE HAVE TO PAY NOTHING FOR THE BARN
YEAH! AND EVEN THE FOOD IS FREE
FACEBOOK AND YOU
If you're not paying for it, you're not the customer. You're the product

CURRENT REGULATION

- Health Insurance Portability and Accountability Act
- FDA Medical Device Regulation
- Electronic Communications Privacy Act
- Private Law (Contract or Tort)
- Fourth Amendment

HIPAA

- Prohibits Unauthorized disclosure of protected health information ("PHI")
- Only applies to "Covered Entities"
  - Mainly health plans, healthcare providers and healthcare clearinghouses
  - Written to cover medical and billing records
- App or Fitness Device Providers not "Covered Entities."
- Data generated not "individually identifiable health information" as defined in HIPAA.
- HIPAA does not regulate the collection of data, only the disclosure of data, and is largely consent-based.

HIPAA

- Are Health Tracking Apps Personal Health Records?
- Probably not, depending on how broad your definition of PHR is
- Health tracking data could be part of a covered PHR if sponsored by a covered health provider or plan
- Apps or data collection by non-covered entities are not regulated by HIPAA.

FDA

- Food and Drug Administration has the authority to regulate medical devices.
- Some mobile apps do not meet the definition of a medical device.
- FDA has stated that it intends to exercise regulatory discretion over those that do, but that does not cover the majority of health data tracking devices.

FDA

- FDA only intends to regulate:

  - Apps that connect to a (regulated) medical device to control the device or acquire data from the device

  - Apps that transform the mobile platform into a regulated medical device

  - Apps that provide analysis, diagnosis or treatment recommendations specific to an individual patient.

FDA

- FDA does not intend to regulate:
  - Mobile apps that provide patients a portal into their own health information, such as … historical trending and comparison of vital signs;
  - Mobile apps that allow a user to collect blood pressure data and share this data through email, track and trend it, or upload it to a personal or electronic health record; [and]
  - Mobile apps that are intended for individuals to log, record, track, evaluate, or make decisions or behavioral suggestions related to developing or maintaining general fitness, health or wellness[.]

PRIVATE LAW

- Is disclosure, aggregation or other use of my data a breach of contract?
  - Maybe.
  - Terms of Use are famously one-sided, non-negotiable "contracts of adhesion"
  - User interfaces may not make clear what data are to be kept private and what data are fair game
  - Damages for breach of contract may be limited by traditional "foreseeability" limitations.

PRIVATE LAW

- If a hacker steals my data, is there liability?
  - Not clear whether the data is the property of the user.
  - Many jurisdictions do not permit a claim for conversion of intangibles.
  - In those that do, caselaw largely limited to conversion (theft) of the physical device containing the data.
  - Not a good fit for available-everywhere "cloud" data.

FOURTH AMENDMENT

- Third Party Records Doctrine
  - Records and information turned over to a third party not protected
  - May show signs of change (US v. Jones 2012)
- Administrative searches may have less protection
  - US v. Golden Valley Electric
- May be a gamble to rely on Supreme Court to properly integrate technological developments into the law

PRIVACY LAW

- Emerging US/EU Divide over data privacy
- EU: Data as property; right to control one's own personal data
- US: Data as expression; protected by first amendment free speech guarantees

EUROPEAN UNION

1995 Directive on Processing of Personal Data

2012 Proposed Directive

2014 “Right to be Forgotten” decision

Personal Data Protection as “Fundamental Right”

- Data Individuals Generate
- Data Generated by Others about the subject

US DATA PROTECTION

- Currently, these data exist in largely unregulated space
- Government starting to become aware of and articulate need for concern about data protection
- Including health data, and including consumer-generated, non-EMR data
- However, data collection and mining may be protected speech
  - (Sorrell v. IMS Health – no state ban on mining and sale of pharmacy records describing MD prescription practices)

MAY 2014 WHITE HOUSE BIG DATA REPORT

- Asymmetry of power between those who hold the data and those who supply it
- Few opportunities to control the collection, use and re-use of information in individual data profiles
- De-identification is limited; re-identification technology rapidly evolving
- Lines blurring between personal data and health care data
- Notice and Consent-based regulation inadequate to regulate Big Data practices

CONSUMER PRIVACY BILL OF RIGHTS

- Individual control over collection and use
- Transparency in privacy
- and security
- Respect for context in collection, use and disclosure
- Security in handling of data
- Access and Accuracy
- Focused Collection: reasonable limits on data collection
- Accountability

MAY 2014 FTC DATA BROKERS REPORT

- Survey of Nine leading data brokers
- Focusing on activities not regulated by FCRA
- Report acknowledges the benefits of data collection and processing, but notes that
  - Consumers may not know how (or even that) their data are being collected and used
  - Consumers may not be able to access their data once aggregated
  - Data held may not be accurate or timely

DATA BROKERS REPORT

- FTC recommendations:
  - Consumer Access to broker data on them
  - Opt-Out Rights to data collection
  - Disclosure of data usage and processing (names and sources of data)
  - Requiring firms interacting with individuals to notify that they share data with data brokers and provide opt-out
  - Require opt-in (affirmative consent) for some sensitive data types, such as health (not sure how health information defined)

Questions Going Forward

- Should I be able to "opt out" of data aggregation?
- Should I have to "opt in" to data aggregation?
- Is there a "moral duty" to participate in some way if I want the benefits?
- Is a proper analogy the credit reporting system?
- Should there be "hard" limits on data collection, retention or sale?
- Do I have a "right to remain unquantified"

CONCLUSIONS

- Moving fast – two major US reports, a major EU data privacy decision, plus one (or two) market announcements this month alone
- No robust current regulation of the collection, use and sale of these data, publicly or privately. US tends to regulate sector by sector
- Nascent recognition of the potential for abuse by US, but political will is uncertain and caselaw trends not necessarily favorable
- EU is further along the path to comprehensive regulation, but has fundamental philosophical differences with US

CONCLUSIONS

- Balancing consumer protection with the potential benefits of this data collection will be difficult
- Consent-based regulation is problematic, inadequate
- "To find a needle, you need a haystack"

UNIVERSITY OF LOUISVILLE.
BRANDEIS SCHOOL OF LAW