The Privacy, Security and Discoverability of Data on Wearable Health Devices: Fitness or Folly?

Vishakha Kumari, M.S. student, Human-Computer Interaction
Sara Anne Hook, M.B.A., J.D., Professor of Informatics/Human-Centered Computing

Agenda

- Introduction
- Wearable Health Devices and Their Data
  - Advantages
  - Privacy
  - Security
  - Discoverability
- Research Plan
- Research Goals
- References

Introduction

- One in every ten Americans uses a wearable device
- Perceive and record information continuously
- Amount of information increasing

Advantages of Wearable Health Devices

- Transforming health care industry
- Insights to health with ease
- Bringing health revolution
- Research/predict the future of human health care needs
- Plan for the health care resources (personnel, facilities, resources) that will be needed in the future

Concerns with Wearable Health Devices

- Data is not considered PHI (Protected Health Information)
- Not covered under HIPAA or other state/federal laws
- Storing the confidential health information
  - Privacy
  - Security
  - Discoverability as part of litigation, an investigation, an audit, etc.

Privacy and Security Issues with Wearable Health Devices

- Health info more profitable than SSN in black market.
- Identity theft
- Profiling
- Stalking
- Extortion
- Discrimination

Discoverability Concerns of Wearable Health Devices

- Promise a whole new era of forensic science
- Data from wearable health devices used as “witness” in court cases – civil and criminal
- Part of overall Internet of Things

Data from Wearable Health Devices as Evidence: Case 1

- A 44-year-old woman from West Chester, Pennsylvania, lied about being sexually assaulted.
- Data from fitness device showed that she was awake and walking around when she said that the attack happened.

Data from Wearable Health Devices as Evidence: Case 2

- A Canadian law firm introduced Fitbit data to show that its client was suffering from injuries sustained in an automobile accident.
- Aggregated data showing her activity measurements was compared to other wearers data to prove the plaintiff was less active than women her age and her profession.

Data from Wearable Health Devices: Fit to Be Evidence?

- Must meet the tests for admissibility as outlined in the Federal Rules of Evidence, Federal Rules of Civil Procedure (as amended on December 1, 2015) and corresponding state court rules:
  - Reliability
  - Authenticity
  - Not prejudicial
  - Probative value
  - Relevant

Research

- Review federal and state legislation for wearable health devices
- Propose new legislation or amendments to existing statutes to offer some level of security and privacy of this data
- Explore electronic discovery issues in the context of civil litigation

Project Goals

- Highlight the perception of people with the current and future use of wearable health devices, knowing the security and privacy risks involved and especially when this data is admissible in court
- Raise awareness in HCI and Health Informatics community to be more mindful when designing and testing wearable health devices
- Advocate for stronger statutory protection and greater clarity about the use of - and potential risks to – data from wearable health devices

Data from Wearable Health Devices: Fitness or Folly?

- Public unaware of security and privacy concerns
  - Will this change after some high-profile cases or incidents?
- Experts calling for new regulations
- Proposed amendments to the Federal Rules of Evidence to address concerns with digital evidence

References

- Dan Ledger & Daniel McCaffrey, *Inside Wearables: How the Science of Human Behavior Change Offers the Secret to Long-term Engagement*. Endeavour Partners, LLC, Jan. 2014, *at* http://endeavourpartners.net/assets/Endeavour-Partners-Wearables-and-the-Science-of-Human-Behavior-Change-Part-1-January-20141.pdf (last visited Oct. 19, 2016).
- Amber Hunt, *Experts: Wearable Tech Tests Our Privacy Limits*, USA Today, Feb. 5, 2015, *at* http://www.usatoday.com/story/tech/2015/02/05/tech-wearables-privacy/22955707, (last visited Oct. 25, 2016).
- *Cybercrime and the Health Care Industry*. EMC Corporation, 2013, *at* http://www.emc.com/collateral/white-papers/h12105-cybercrime-healthcare-industry-rsa-wp.pdf, (last visited Oct. 19, 2016).
- Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work*, 16 Yale Journal of Health Policy, Law & Ethics 1 (Winter 2016).

References

- Marilyn Odendahl, *Fitness Trackers Add to Flood of Digital Evidence in Court*, The Indiana Lawyer, Aug. 10, 2016, *at* http://www.theindianalawyer.com/fitness-trackers-add-to-flood-of-digital-evidence-in-courts/PARAMS/article/41112, (last visited Oct. 19, 2016).
- David R. Matthews, *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. CRC Press, 2016, at 147-148.
- Kelly R. Evenson, Michelle M. Goto, & Robert D. Furberg, *Systematic Review of the Validity and Reliability of Consumer-wearable Activity Trackers*. 12 International Journal of Behavioral Nutrition and Physical Activity 159 (2015).
- Karen Weintraub, *Wearable Health Monitors Not Always Reliable, Study Shows,* USA Today, Oct. 12, 2016, *at* http://www.usatoday.com/story/news/2016/10/12/wearable-health-monitors-not-always-reliable-study-shows/91922858/, (last visited Oct. 19, 2016).
- Nicole Chauriye, *Wearable Devices as Admissible Evidence: Technology is Killing Our Opportunity to Lie*, 24 Catholic University Journal of Law and Technology 495 (2016).

Any Questions?
Thank you for attending the HCC Brown Bag session today!