SECURITY & PRIVACY CHALLENGES IN MOBILE HEALTH (MHEALTH) SYSTEMS

David Kotz

Professor of Computer Science

Institute for Security, Technology, and Society
Dartmouth College

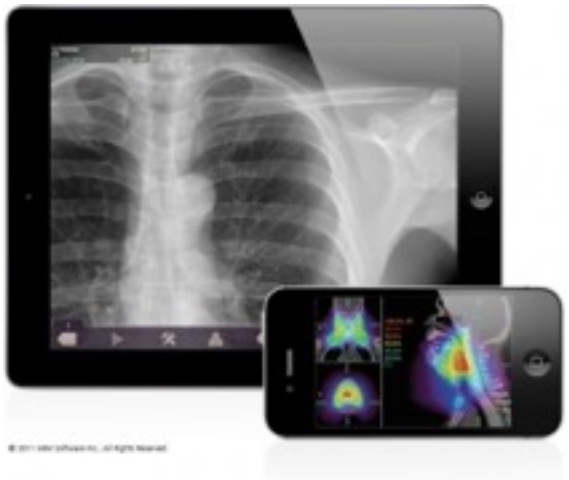
January 2015

mHealth

The use of mobile computing and communications technology in the delivery of healthcare or collection of health information.

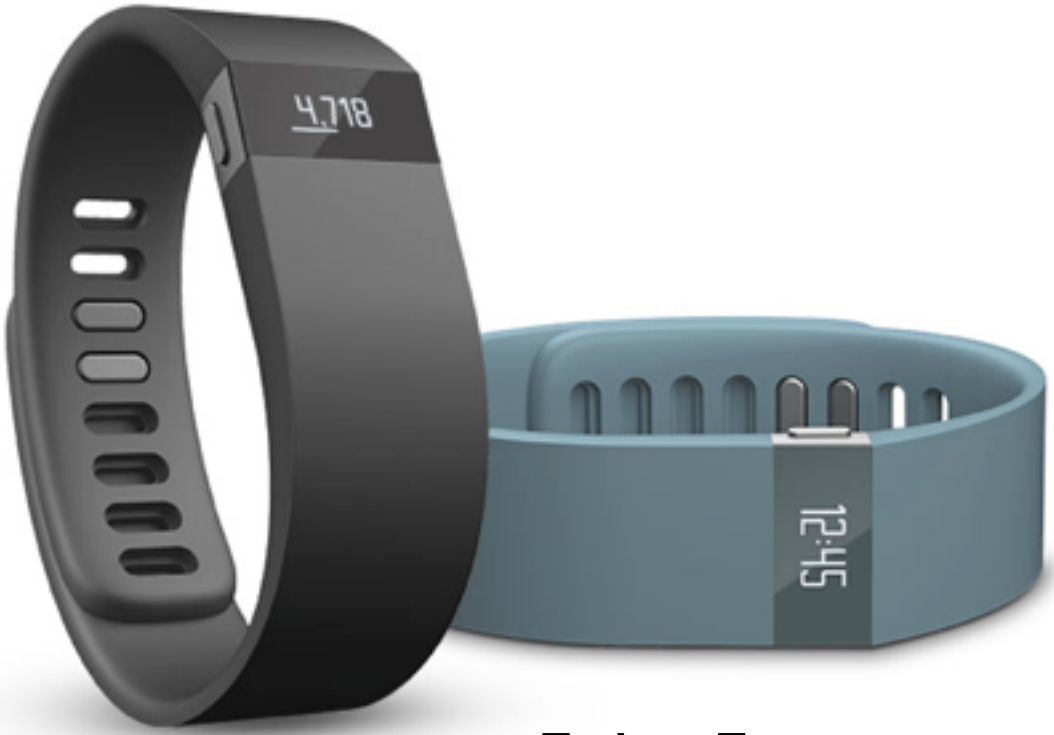
mHealth - in the clinic

Inpatient monitoring



Remote patient monitoring

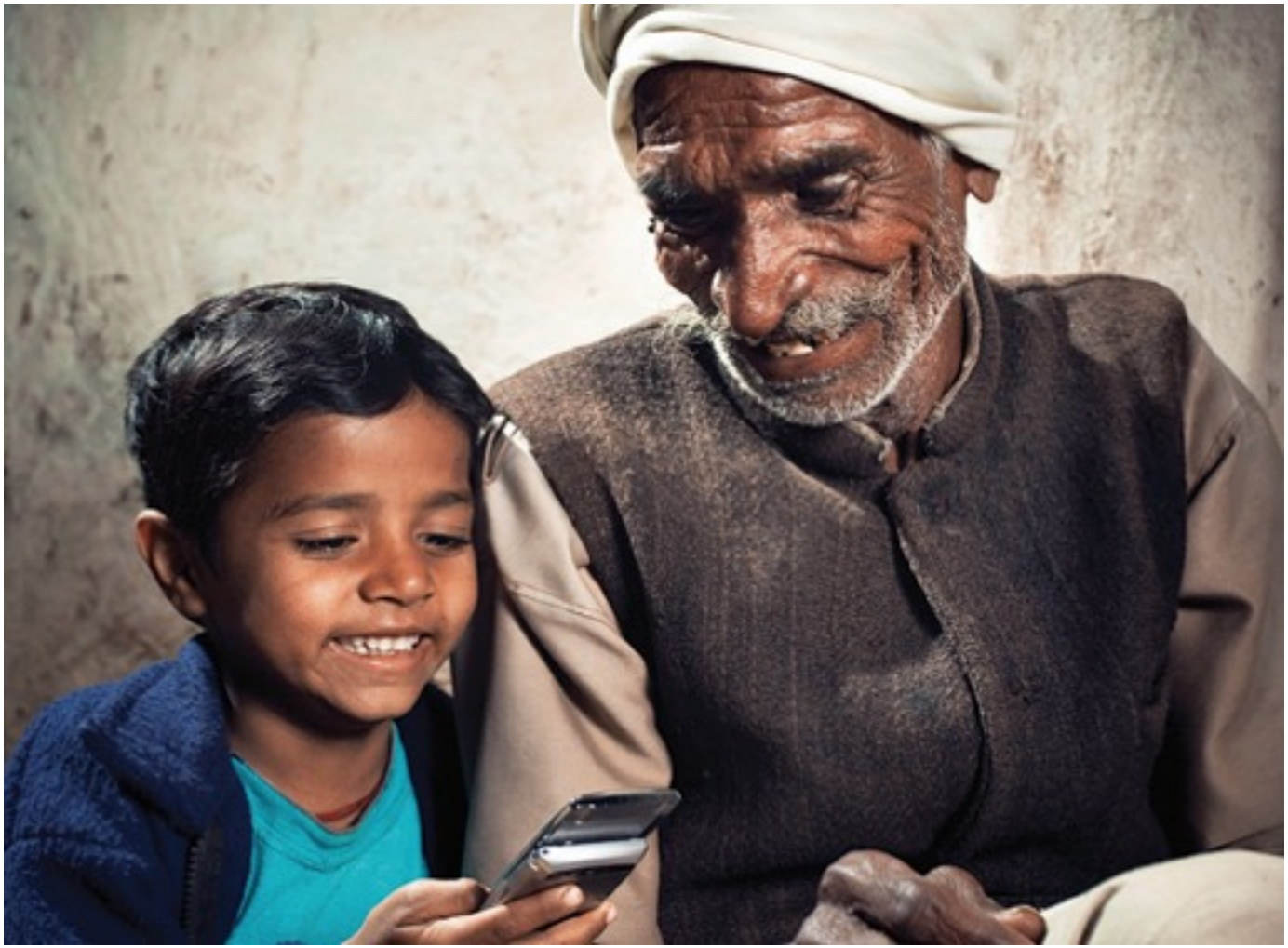
Personal wellness applications



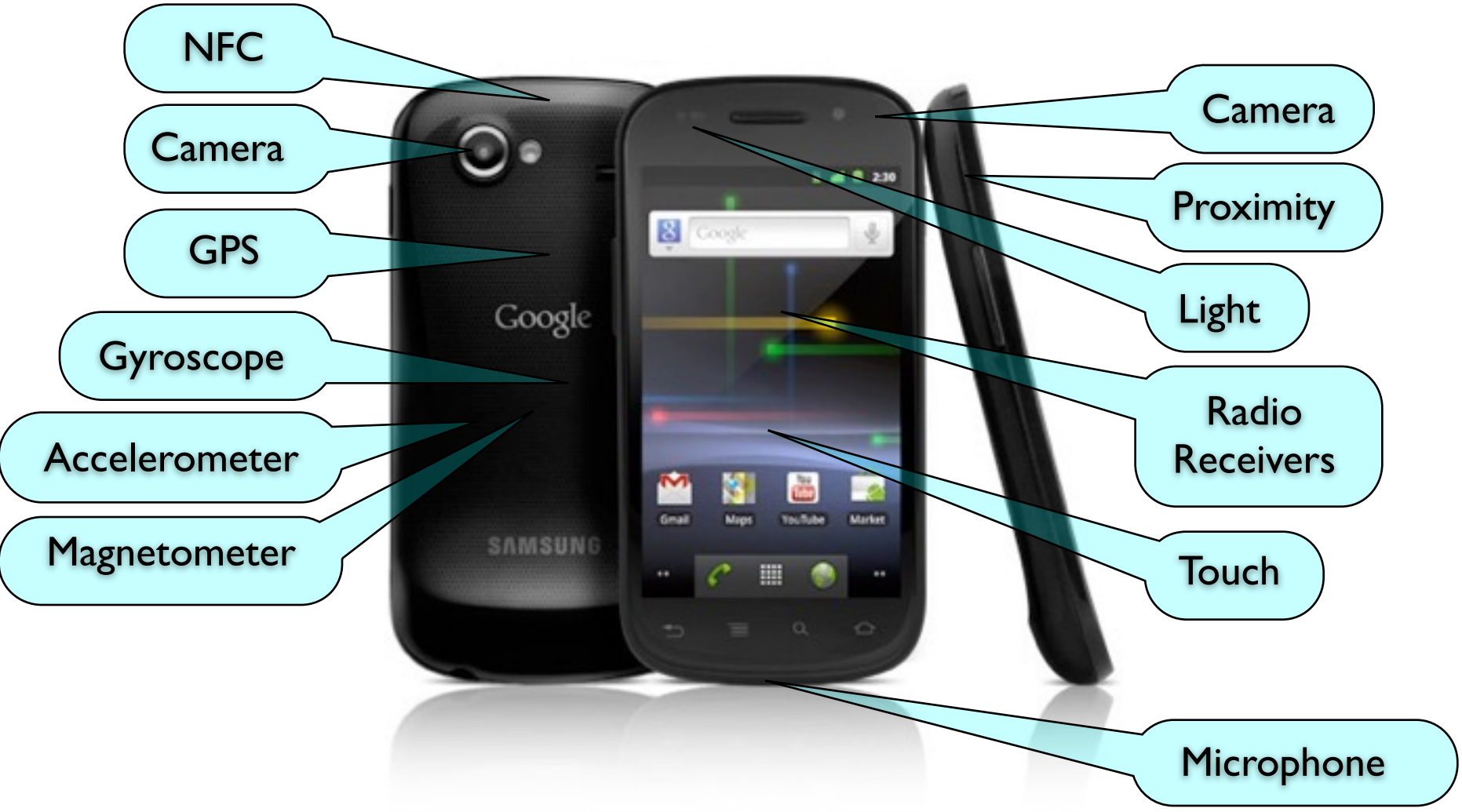
Fitbit Force

Fitbit Classic

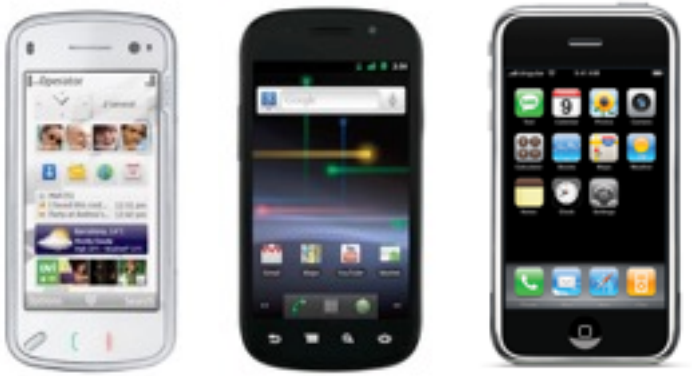
mHealth in the developing world



mHealth platforms: Smart phones



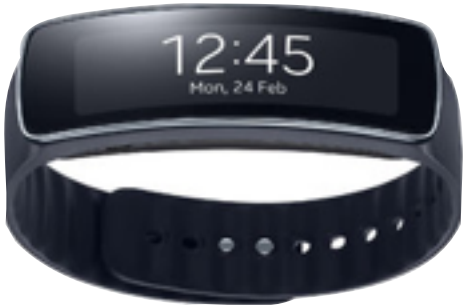
mHealth devices are emerging



smart phones

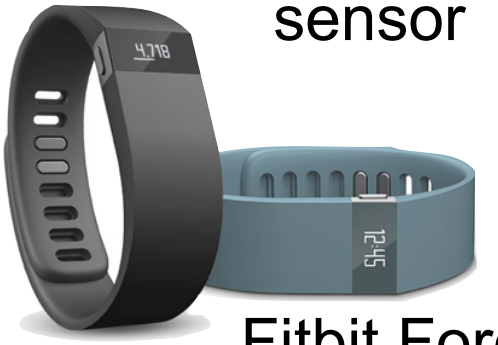
Stella wearable sensors

Philips emotion sensor



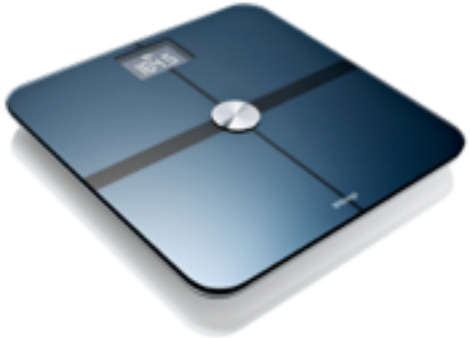
Samsung Gear

Corventis wearable medical sensors



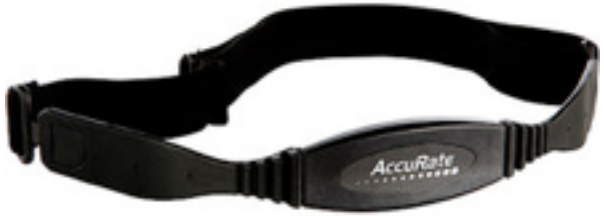
Fitbit Force

Shared sensors, environmental sensors

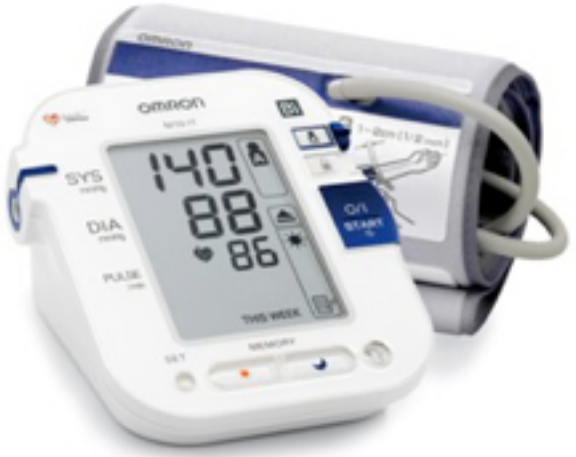


Withings wireless body scale

Caliber III
(temperature and humidity)



Wireless Heart Rate Monitor
(ProForm AccuRate)



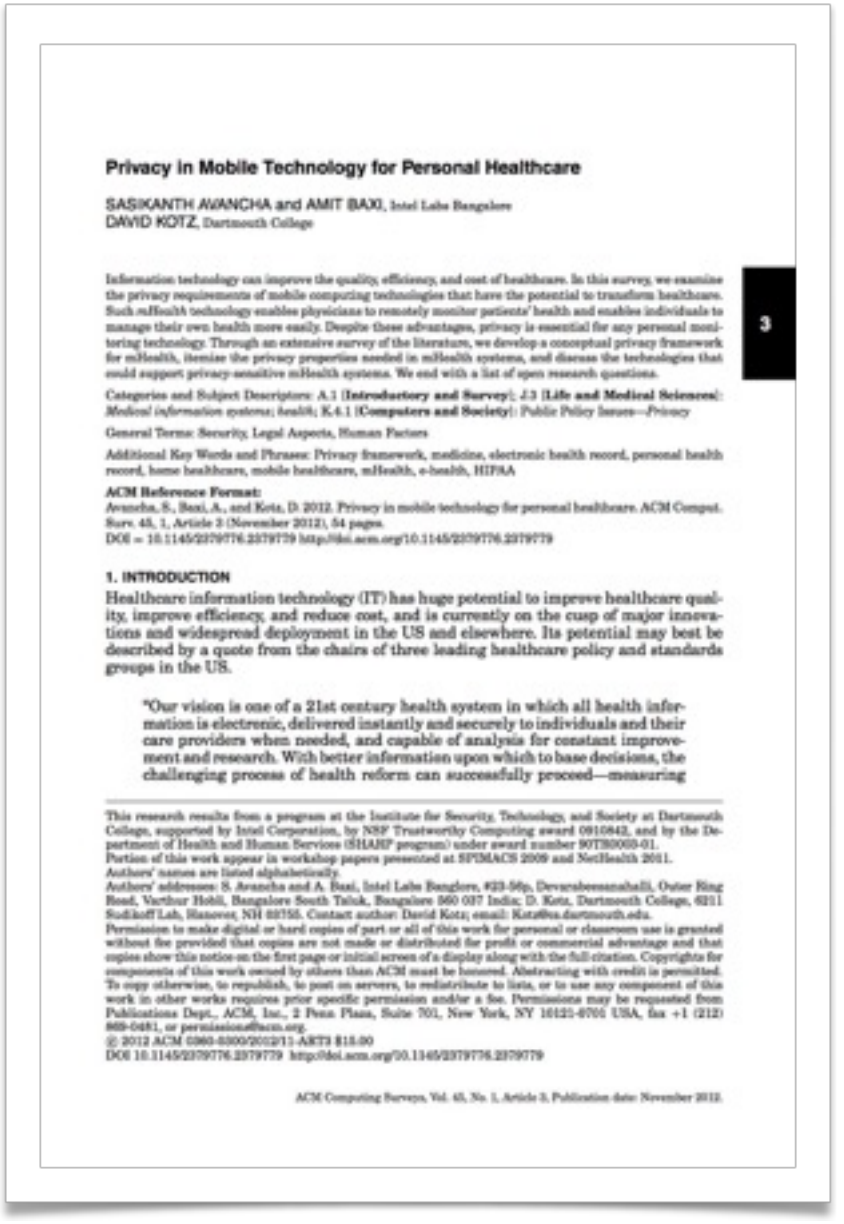
Blood Pressure Monitor
(Omron M10)

mHealth – what's different?

- **Security**
  - **Immediate, personal impact**
    - mHealth devices directly affect your health, or health decisions
- **Privacy**
  - **Sensitivity** of data:
    - mHealth data is inherently personal, literally about *you*
  - **Volume** of data:
    - mHealth collects far more medical data, over extended periods
  - **Diversity** of data:
    - mHealth collects a broader range of information, including lifestyle, activities, and context
  - **Uses** of data:
    - mHealth enables a broad range of apps, outside the doctor-patient relationship

survey paper:

- privacy framework
- security properties
- threat taxonomy
- research challenges



Privacy in Mobile Technology for Personal Healthcare

SASIKANTH AVANCHA and AMIT BAXI, Intel Labs Bangalore
DAVID KOTZ, Dartmouth College

3

Information technology can improve the quality, efficiency, and cost of healthcare. In this survey, we examine the privacy requirements of mobile computing technologies that have the potential to transform healthcare. Such mHealth technology enables physicians to remotely monitor patients' health and enables individuals to manage their own health more easily. Despite these advantages, privacy is essential for any personal monitoring technology. Through an extensive survey of the literature, we develop a conceptual privacy framework for mHealth, itemize the privacy properties needed in mHealth systems, and discuss the technologies that could support privacy-sensitive mHealth systems. We end with a list of open research questions.

Categories and Subject Descriptors: A.1 [**Introductory and Survey**]; J.3 [**Life and Medical Sciences**]: *Medical information systems; health*; K.4.1 [**Computers and Society**]: Public Policy Issues—*Privacy*

General Terms: Security, Legal Aspects, Human Factors

Additional Key Words and Phrases: Privacy framework, medicine, electronic health record, personal health record, home healthcare, mobile healthcare, mHealth, e-health, HIPAA

ACM Reference Format:
Avancha, S., Baxi, A., and Kotz, D. 2012. Privacy in mobile technology for personal healthcare. ACM Comput. Surv. 45, 1, Article 3 (November 2012), 54 pages.
DOI = 10.1145/2379776.2379779 http://doi.acm.org/10.1145/2379776.2379779

1. INTRODUCTION

Healthcare information technology (IT) has huge potential to improve healthcare quality, improve efficiency, and reduce cost, and is currently on the cusp of major innovations and widespread deployment in the US and elsewhere. Its potential may best be described by a quote from the chairs of three leading healthcare policy and standards groups in the US.

> "Our vision is one of a 21st century health system in which all health information is electronic, delivered instantly and securely to individuals and their care providers when needed, and capable of analysis for constant improvement and research. With better information upon which to base decisions, the challenging process of health reform can successfully proceed—measuring

This research results from a program at the Institute for Security, Technology, and Society at Dartmouth College, supported by Intel Corporation, by NSF Trustworthy Computing award 0910842, and by the Department of Health and Human Services (HHSP program) under award number 90TR0003-01. Portion of this work appear in workshop papers presented at SPIMACS 2009 and NetHealth 2011.
Authors' names are listed alphabetically.
Authors' addresses: S. Avancha and A. Baxi, Intel Labs Bangalore, #23-56p, Devarabeesanahalli, Outer Ring Road, Varthur Hobli, Bangalore South Taluk, Bangalore 560 037 India; D. Kotz, Dartmouth College, 6211 Sudikoff Lab, Hanover, NH 03755. Contact author: David Kotz; email: Kotz@cs.dartmouth.edu.

DOI 10.1145/2379776.2379779 http://doi.acm.org/10.1145/2379776.2379779

Avancha, Baxi, and Kotz. "Privacy in Mobile Technology for Personal Healthcare", *ACM Computing Surveys* 45(1), November 2012

TRUSTWORTHY HEALTH AND WELLNESS (THAW)

thaw.org

seeking new students and postdocs…