

# Wearables for student health and wellness

David Kotz

Department of Computer Science

Dartmouth College

July 2015

## Vision statement

Although smartphones are a ubiquitous accessory for nearly every college student today – students seem to have their smartphone with them every moment, even when they carry or wear little else – we should anticipate the advent of wearable devices within a few years. First, the wide variety of current and future wearable devices poses broad potential opportunities for collecting information about student physiology, activity, and social context. Second, there is a real possibility that wearables will even replace the smartphone in a few years, just as smartphones have supplanted laptops, particularly in social and extra-curricular situations.

“Wearable devices” is a broad category. Devices can be worn in a variety of locations – as wrist or ankle bands, chest straps, earpieces, necklaces, stuck directly to the skin; or attached or integrated into clothing. Devices may be worn continuously, or during certain activities (such as sleep or exercise). Devices may be primarily suited for ornamental or recreational purposes, but their data could be captured and re-purposed in support of wellness and health goals. Other devices may be rigorously designed and tested to clinical standards. Devices may act as a partner to a smartphone, or may interact with objects and devices in the environment, or may be suitable for independent use.

Despite the potential opportunity, we face at least two major challenges in making good use of this data for health and wellness. First, we need a common framework for applications to network with these devices, extract their data, and interpret that data in context. Such a common framework may be difficult to achieve, given the rapid development of these devices in diverse sectors of the industry. Second, we need to ensure strong security and privacy principles are employed from the earliest development of these devices, lest malicious parties can too-easily hack into a person’s body-area network of wearable devices to cause confusion or harm, or the devices expose personal and sensitive information to eavesdroppers, network operators, cloud providers, or device vendors.

## Biographical sketch

David Kotz is the Champion International Professor in the Department of Computer Science at Dartmouth College. He served as Associate Dean of the Faculty for the Sciences for six years and as the Executive Director of the Institute for Security Technology Studies for four years. In 2013 he was appointed to the US Healthcare IT Policy Committee. His research interests include security and privacy, pervasive computing for healthcare, and wireless networks. He has published over 100 refereed journal and conference papers and obtained over \$56m in grant funding. He is PI of a \$10m grant from the NSF Secure and Trustworthy Cyberspace program and leads a five-university team investigating Trustworthy Health & Wellness technology (see [thaw.org](http://thaw.org)). He is an IEEE Fellow, a Senior Member of the ACM, a 2008 Fulbright Fellow to India, and an elected member of Phi Beta Kappa.

After receiving his A.B. in Computer Science and Physics from Dartmouth in 1986, he completed his Ph.D in Computer Science from Duke University in 1991 and returned to Dartmouth to join the faculty. For more information see <http://www.cs.dartmouth.edu/~dfk/>.