Personal Biometric Data Tracking: Risk and Regulation

Timothy S. Hall
Professor of Law
Louis D. Brandeis School of Law
University of Louisville

The potential benefits of health-related data tracking and data mining are vast and expanding. At the macro level, there can be benefits in using the aggregated data of millions of individuals to predict health risks and disease outbreaks. These data can potentially improve public health responses to such outbreaks, saving lives and improving efficiency of service delivery. At the same time, at the micro level, collecting, sharing and analysis of individual health data can improve health outcomes for those involved in the data collection, and can provide those individuals with a level of insight about their health – related behaviors that is not easily achievable through other means.

We are currently in the midst of a convergence of personal technology and health informatics. Advances in portable computing, the near-ubiquity of the smartphone with its app-driven marketing structure, the availability of high-speed mobile internet connectivity and the rise of "cloud-based" computing services –both data storage and data processing, analysis and mining – have enabled the emergence of a cluster of health-related data collection and tracking apps, devices and services. These include nutritional tracking apps, weight management devices and apps, pedometers which track the user's movement and calculate the health effects of one's exercise (or lack thereof), wristbands which purport to measure the

quality of one's sleep, and others too numerous to list here. This practice of personal data tracking and analysis is often referred to as the "Quantified Self" movement, or as "Life-logging" or "Life-Hacking." Currently, health tracking apps primarily rely on the manual input of data from the user, with some exceptions. This is starting to change with the advent of devices that measure health parameters directly from the individual user. However, commentators have predicted that in the near future, there will be sensors – perhaps implantable or wearable sensors - that will send streams of biometric data from the individual user to a smartphone to create a database of information and/or to monitor potential adverse health events. These sort of uses of mobile computers such as smartphones have not gone unnoticed by makers of the devices. Smartphones and other portable and wearable technologies have started to include hardware and software features explicitly dedicated to current and future uses of these devices for health data tracking.

Proponents of these devices and apps envision a near future in which individuals will have a level of information about and control over their daily lives unequalled in human history, and predict that this unprecedented exercise of healthcare consumer autonomy will have dramatic effects on the way in which healthcare is practiced, virtually ending the practice of medicine as we know it. This essay will explore some of the potential pitfalls associated with collection of detailed individual biometric or health-related information, and will demonstrate that current laws and regulations are not well designed to protect users of these devices and apps from unauthorized use or misuse of their data.