Mobile Health and Privacy Challenges

Abstract

Anne SY Cheung

The increasing popular use of mobile devices, wearables and apps to monitor one's health, lifestyle and fitness has set a new trend known as mobile health - mHealth. In 2016, there were 165,000 health-related apps which run on two main smartphone operating systems. The mHealth ecosystem includes (1) self-tracking apps and appliances that used to monitor wearers' physical fitness e.g. Fitbit, Jawbone and Apple Watch; (2) prescribed apps and devices required by medical practitioners or authorities to be worn by patients e.g. UK's GDm-health project on diabetes patients; and (3) self-volunteered participation in large scale population study for health (e.g. Apple ResearchKit and Google's Baseline).

We are often amazed by the power of mHealth gadgets but we seldom question how the health data are streamed and analysed. Not only are we being confronted with our own data on steps, sleep, stress, dreams, fertility or even sex, we may have let others getting insights on ourselves 24 hours a day. While mHealth has brought convenience and has lowered the cost of healthcare, the increasing individualization and consumerism in healthcare has also transformed our notion on consent, and how data are collected, used and shared. Attempts have been made in the European Union and the United States to set out privacy and security guideless in this area of mHealth. This study provides an overview of the privacy issues on mHealth and identifies the legal gaps in regulation. What is needed is an appropriate legal response.