“While the various models of Fitbit are probably the most widely used wearable biometric monitors, the Apple Watch is currently the most polished example of the category—indeed, lower-than-anticipated sales when initially marketed as a fashion accessory have spurred Apple to reposition its offering as a high-performance fitness device.

The data can be both positive and negative but never been natural. Depends on the sensitivity of it, so how people/ designers utilizing those data, how we protect our users away from privacy concerns.

“The clear aim of such “smart home” efforts is to as nearly as possible short-circuit the process of reflection that stands between one’s recognition of a desire and its fulfillment via the market.

The smart home that knows the user body data might be the solution of the calm tech because it can avoid active put and use passive input, heart rate, sweat and position instead. It can provide user a friendly interface without any annoying command to the home ai. Also the ai can do every quietly for you.

“Every networked device that goes unprotected in this way isn’t simply exposing its own controls. It can be suborned as a point of access to the entire local network and every other device connected to it,19 offering intruders an aperture through which they might install backdoors, intercept traffic passing across the network, or launch denialof-service attacks.”

If every data can be collected, and the device and database are connected online, it is dangerous for users because it directly exposes them under the threat of the hacker. Usually hacker will not attack individual, however, the model result from the illegal dataset is dangerous. The data is also critical if it sold to other adversities.