Fitness tracking data in courts – persuasive, but not conclusive

Beyond simply counting steps, fitness tracking technology creates personal black boxes that archive everything we do – even sleeping.

So it’s not surprising to see that a Calgary law firm, representing a fitness instructor injured more than four years ago, announced last week it will use data taken from the plaintiff’s FitBit as an “objective” measure of activity in a personal injury lawsuit in order to show a reduction in physical activity post-injury.

With the inevitability that self-tracking data, like social media profiles, will become accessible to courts, there’s a range of issues that self-trackers, legal professionals and others will need to consider. Deborah Lupton touched on the topic of privacy before, but should fitness data be treated as conclusive evidence?

In this particular case the data is being given over voluntarily. But data from your FitBit, Apple watch or any number of other devices and apps used to measure and log information about yourself could be subpoenaed by courts in a range of different circumstances including some where the data could be used against the wearer.

Entities – especially those based in the US – such as employers and health insurers and even certain retailers (for their customer loyalty schemes) have shown interest in collecting health and fitness information about individuals.

In this light, perhaps it is not a surprise that self-tracking data is also of interest to those involved in various types of legal proceedings.

Analysing the data

Most devices available to consumers work by using small sensors including accelerometers and altimeters that measure the amount and intensity of movement. The software, coupled with these devices, rely on algorithms to convert data from the sensors into useful information.

Given that most people who self-track want to achieve a certain goal – taking 10,000 steps per day, getting more sleep or reducing calorie intake – little thought is given to the ways in which the raw data collected by the device could be re-purposed (and by whom).

The majority of fitness tracking devices on the market are not able to tell the difference between the type of activity a user is engaging in. For the data to be more accurate, users have to manually specify certain activity types like running or bike riding via a web account or mobile app. This leaves fitness tracking systems open to abuse by users who could create fraudulent data sets.

The law firm representing the plaintiff in Calgary will make the data available to Vivametrica a company specialising in standardising and comparing self-tracking data at the population level. The scope and application of self-tracking data is likely to become more complex as the major players like FitBit allow developers access to their application programming interfaces (APIs).

Reverse engineering and open source development in health technology also allows users and third parties greater freedom to modify the devices. This access to direct tracking is often in violation of software licences,
presenting a range of potential abuses and legal quagmires.

**So is fitness data conclusive?**

It remains to be seen whether self-tracking data from wearable devices will be used to the same extent as DNA evidence or fingerprints in litigation. But the treatment of these kinds of evidence may provide some guidance as to how data from wearable technology should be approached in the courtroom.

While DNA and fingerprint evidence may generally be considered as admissible in proceedings – and authoritative – there have still been challenges as to their use in certain instances. Indeed, miscarriages of justice have been remedied and caused by these types of evidence.

The quality of the evidence is of high importance, and encompasses factors including the methods used to collect the sample and analyse it in a laboratory. For DNA evidence, the laboratory analysing it must be accredited to ensure quality control. An expert witness may also be called to discuss the sample and the methods for collection.

Accordingly, similar questions should be asked of self-tracking data obtained via wearable devices: data science experts could be called to discuss how reliable or accurate the data is. More could also be done to educate judges and the legal profession more generally about this kind of data gathering.

In practice, courts should not view the data collected from wearable devices as the objective truth about that individual’s state of health, fitness or activity. At most this data should constitute “opinion” rather than “fact” and should be treated as persuasive at most, but certainly not definitive of “truth”.

While DNA evidence or fingerprints are used to determine whether a particular individual was present at the crime scene, self-tracking data and its analysis is used to try to answer more nebulous and less binary questions about a person’s state of health or level of fitness.

Since there will be various other ways of making these determinations – and various assumptions underpinning
each method, such as precisely what being healthy or fit means – courts should at most regard this kind of evidence as indicative or persuasive rather than conclusive.