Roke

Part of the
Chemring Group

Could fitness trackers solve a murder?

The wealth of information coming from connected devices could one day be an incredible resource for fighting crime, but a few questions must be answered before this becomes the norm. Roke's expert in information security, Mark West, explains…

Could fitness trackers solve a murder?

In 1999, British technologist Kevin Ashton came up with the term Internet of Things (IoT) to define a network that not only connects people, but also the objects around them.

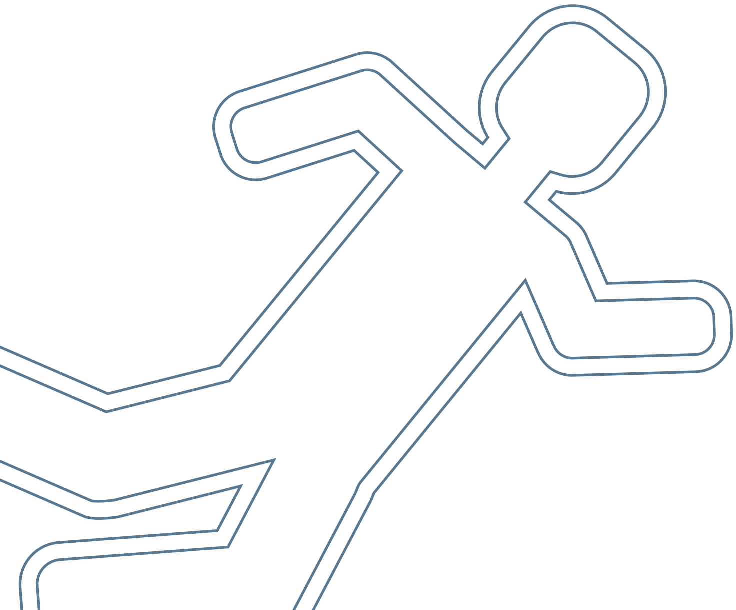
Since then, the desire to improve personal and organisational efficiency has driven the widespread adoption of the IoT. This network of connected devices has grown exponentially year on year, with the number of connected devices forecast to reach 50 billion by 2020.

In its simplest term, the IoT is used to mean devices connected to the internet. But today, when we talk 'IoT', we really mean any number of devices that talk to each other to share and gather data, from smartphones, to smart fridges and connected vehicles.

One of the biggest markets for IoT devices is wearables, with the global market expected to be worth 53 billion U.S. dollars in 2019. The most successful wearables currently on the market are smartwatches and fitness and health trackers with analyst firm IDC highlighting that worldwide shipments of these devices reached 19.7 million units in the first three months of 2016 alone – up by 67.2% from 2015.

These numbers probably come as no surprise. Fitness trackers have a clear consumer application and a price point that is not prohibitive to mass-market adoption. They're essentially a human black box recorder and one little wristband can reveal a lot, including how many calories you burn, the exercise you do, your heartrate, sleep patterns, location and a whole lot more.

Using these devices, it's possible to gather and learn from your own data, opening up a rich world of insights to the user. But what happens if that personal information has the potential to be used against you? Or becomes the crux of solving a crime?



USING DATA TO SOLVE CRIME

Information derived from IoT devices can be applied in all manner of powerful ways, including the ability to understand a complex situation like a crime scene.

In certain cases, the government or a legal institution could request your fitness tracker information and then use it against you in a court of law. That's what happened to Chris Bucchere, a San Francisco cyclist who struck and killed an elderly pedestrian. Bucchere was charged with manslaughter, carrying a potential penalty of six years in prison, after prosecutors obtained his data from his GPS-enabled fitness tracker to show he'd been speeding before the accident. Bucchere's own self-monitoring became a piece of evidence against him.

Sifting data for evidence is nothing new. Police in the UK already identify residential marijuana growers by monitoring the total energy consumption of a home and comparing it to averages in the area. This approach is made easier by the roll out-out of smart meters, as these remotely-readable devices autonomously collect electricity usage information from residential addresses in the UK.

A current strand of academic research is in the use of Non-Intrusive Load Monitoring Algorithms (NILMAs), which make use of the data collected by smart meters. NILMAs are able to split the total energy used by the home into constituent parts and inform observers which devices in the home are being used and at what times.

SO COULD A FITNESS TRACKER REALLY SOLVE A MURDER?

The simple answer is yes, it could. Yet there are many challenges to overcome before we can say with certainty that it actually can.

A fitness tracker can use GPS to pinpoint its location, but that's not enough to constitute evidence of a person's location. As well as monitoring location, you need to monitor the activity of the fitness tracker itself at that point. Was it simply left at home? Painting a full picture and spotting patterns of odd behaviour relies not only on accurate data collection, but the accurate interpretation of the data.

Making use of data of this kind presents many hurdles for law

“Using data to solve crime”

enforcement bodies. Not only do they need to get hold of the data, they need to prove it's the correct data, clean the data, process and store the data and - for all of this - they need the right processes and tools to do this accurately and effectively, and within the law.

As the IoT environment matures, we'll see a significant increase in the number and variety of IoT devices and the data these generate. When it comes to analysing the data from a crime scene, there are a number of different approaches to performing analytics on such high data volumes, and one way would be to utilise big data platforms. The data can then be stored in data centres and subsequently analysed by police investigating the crime in question.

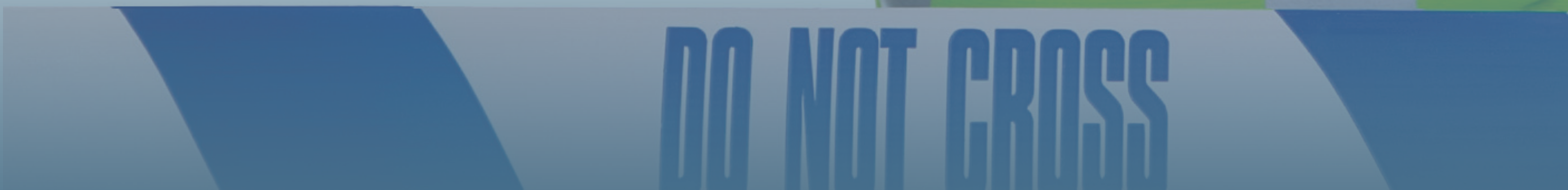
Although there are obvious advantages to law enforcement agencies being able to access this data, a disadvantage is that, in reality, a large percentage of the processed data is likely to be uninteresting, but then processed regardless.

Another challenge for law enforcement authorities is the lack of widely adopted open standards for storing and communicating information on and between IoT devices. This presents the difficulty of analysing data stored in proprietary formats, and the challenges posed from connecting to a range of devices using proprietary interfaces.

Moreover, given the insecure nature of most IoT devices, it is not even possible to determine the provenance of the data, casting doubt on the credibility of the information from a forensic perspective.

To solve this will require government and international body collaboration to drive the adoption of common interfaces, in turn driving competitive efficiencies for the consumer – and common interfaces for law enforcement authorities

Roke is investing in an internal IoT testbed for to understand the opportunities that IoT devices offer. This involves extensive research and structural analysis of these devices, carried out by Roke security experts, to uncover any vulnerabilities and work with the manufactures to secure them.



WHO OWNS THE DATA?

Analysing such a vast sea of complex data is only one challenge in the world of IoT. There are also several others to overcome when it comes to data privacy.

In most physical environments, such as your home, workplace or a train station, multiple individuals will be present and interacting with the environment, many of whom will not be relevant to an investigation. This results in privacy and data protection constraints.

Law enforcement agencies have a responsibility to protect the privacy of individuals other than those under investigation, and in the IoT world that means their data, which may be stored on the same server as a subject of interest.

Then there's the tricky debate about ownership. We already give up a certain amount of data every time we buy a fitness tracker, but who owns this data? Who should have access to it and what constitutes this need?

At the moment, data can be obtained through court on a case-by-case basis, but this relies on law enforcement agencies knowing what data they could get, what they need, and how to go about asking for it.

Roke is actively involved in shaping the future of IoT security through its membership with the Internet of Things Security Foundation (IoTSF), a collaborative, non-profit, international response to the complex challenges posed by security in the expansive hyper-connected world. Together, this group of organisations is establishing principles for IoT security, to inform industry, government and legal sectors.

Whether we are prepared or not, it's an undeniable fact that the IoT era is upon us and it's creating a data-rich environment for law enforcement. Law enforcement agencies must now learn how to manage this data to realise its full value. The challenge lies not only in developing novel data management technologies, but also in law enforcement agencies being supported in understanding what data is available and having the relevant technical knowledge and skills to realise the full potential of connected devices.

Mark West
Practice Area Lead for Information Security

Mark is an expert in cyber security and currently heads Roke's Information Security practice. He plays a central role in Roke's partnership with the Cyber Security Challenge and the University of Southampton's Cyber Security Academy where he is Visiting Professor. He specialises in Internet standardisation as well as EU and UK/US collaborative research programmes, also providing consultancy to commercial, defence, national security and Open Government Data projects.

Owing to Mark's knowledge of Internet protocols and architecture, he has been chosen as technical authority on many diverse projects for the UK Government, where he has been responsible for the design and evaluation of secure systems.

Mark has more than 25 years of experience as a software engineer.

Tel: +44 (0)1794 833311

Mark.West@roke.co.uk

MEDIA CONTACT
LINDSAY COMPTON

Email: lindsay.compton@roke.co.uk
+44 (0)1794 833205