Challenges for an increasingly-connected world--the Internet of Things

20/07/2015

IP&IT analysis: How is the advent of the Internet of Things (IoT) likely to impact the everyday lives of people and businesses? Sarah Pearce, partner, and Leo Spicer-Phelps, associate, at Cooley (UK) LLP, consider the various legal aspects underpinning the IoT.

What is the IoT?

It is projected that the creation of an IoT, essentially the creation of a 'connected' world through the addition of sensors and devices to enable communication from everyday products to other products, applications and wider information networks--could have an economic value of up to $25 trn to the global economy by 2025.

The scope of products and services incorporated by the term IoT is incredibly broad, ranging from demand prediction and automatic production in factories to wellness monitoring through wearable devices.

While it is clear that the IoT will have a huge impact on the way the world operates--it can be a pretty nebulous term and its implications, both legally and commercially, remain unclear.

How is the IoT changing the tech sector?

Already incredibly important and valuable to all businesses (particularly in the tech sector), data will reign supreme across all industries. The importance of data processing software and the integration of technology into everyday products is likely to dramatically expand the reach of what we consider to be the 'tech sector' at the moment.

The IoT provides access to an increased amount of data, collected from many more sources to many more people. It is envisaged that, where they do not already, virtually all products will include sensors and communication devices to collect and send that data to be used in a very practical manner--to your fridge, your watch, your car, the list is endless.

Advertising, media and retail companies and the like have all been using technology to predict human behaviours based on the data they are able to collect. However, a McKinsey report on the IoT found that, in many areas, only 1% of data collected is currently being put to meaningful use. The challenge is going to be making this 'big data' meaningful and optimising the opportunities it presents.

Over the last few years, innovators seem to have been focusing more on 'machine to machine' communications? What does this mean and what are the key issues that may arise?

Machine to machine communication is exactly what it sounds like--one device talking to another. The reason it is being focused on so much is because the IoT means many more devices will communicate in this way.

Machine to machine communications will be key to creating integrated systems which create an effective data sharing network. Classic examples include driverless cars talking to other cars, intelligent utility monitors communicating with weather meters and intelligent white goods.

Take a white goods example--your fridge knows that you are running low on milk. The fridge is linked to your wearable device which tells that device to send you a notification. The notification explains that milk has been added to your next scheduled food delivery. This is a pretty simplistic model--but even here the data collected in this process could be useful to many other services or products outside of the obvious ones playing a role in the chain.

The IoT allows you to expand this data sharing network. Dairy producers would want to know how people consume milk throughout the year--your wearable health monitor might want to know whether you've been ordering whole milk as that could explain the elevated cholesterol levels it's picking up. Your private health care provider may also be interested in this information if you had selected a novel 'monitored healthy eating gets you a discounted premium' medical insurance model.

The user would probably agree that the initial application of the data was useful, as may be the second use, but they might not be happy with the third. The role of data protection and privacy is going to be paramount.

What are the legal challenges around data use in the IoT?

There are multiple legal challenges:

- liability for malicious attacks
- litigation around cyber insurance policies
- criminal responsibility for driverless cars etc

The principal cause of all these issues is likely to be friction with legal and regulatory frameworks which do not address the pace of developments in the area.

For example, the forthcoming General Data Protection Regulation (GDPR) is likely to create a requirement that data privacy is embedded by design and default into all systems and processes operated by companies--how does this square with businesses' desire to expand data sharing to provide novel or improved services to consumers?

To really exploit the full value of the IoT for businesses and to make it as useful as possible to users, a great deal of data is going to be shared and used, probably for purposes other than those for which it was initially collected. The key issue here is going to be the consent of the user to the use of their data within the ever expanding networks created by the IoT.

This idea of 'repurposing' data raises major issues around consent to the use of the data, issues that are likely to be heavily debated as and when the GDPR becomes the harmonised law across the EU. Among many other methods designed to protect data security, the GDPR is very likely to require data controllers operating in this area to get explicit, unambiguous consent to collection and processing of personal data--and the burden of proof will be on the data controller to demonstrate that they obtained that consent.

Lengthy legal terms that are not frequently read will be tough to rely on as evidence of effective, informed consent under the GDPR. This means businesses and legal practitioners will have to work to build new customer-facing communications and agreements in order to get this consent.

Interviewed by Alex Heshmaty.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor