The Internet of Things – ramping up privacy and security considerations

Speed read

We explain here what the Internet of Things (IoT) is, giving an example. There will be around 25 billion devices connected to the internet by the end of 2015. This is starting to have huge impact, from smart meters for electricity to remote monitoring of health signs by hospitals.

Then we address what the Federal Trade Commission (FTC) has to say about this in a 27 January 2015 report on privacy and security concerns.

There are some quite challenging issues. That report follows an EU report in September 2015 on privacy and security issues for the Internet of Things.

February 2015

The Detail

Illustrating Internet of Things issues - Fitbits

Fitbits are all the rage. This is an IoT device. The *Fitbit Surge* (pictured above), released at this year's CES show in Las Vegas for new electronic consumer products, monitors movement, steps taken, heart rate, hours slept, and can even monitor sexual activity. Pretty sensitive information. Data is uploaded from the device to Fitbit's cloud based service. It can be mixed and matched by Fitbit and others, in a way that is powerful for marketing (that is, if Fitbit choose to do that, and assuming the security is tight). The Fitbit also works with great sites like *MyFitnessPal*, so that information from the IoT device travels even further out into the cloud. Our article, *Big Data in business - father learns of teenage daughter's pregnancy from retail chain*, shows just how invasive and powerful this can become.

These are terrific innovations – and lots of people want targeted services based on matching and mixing data. The way in which Fitbit integrates with *MyFitnessPal* is terrific. But in the mix there is great risk of undue intrusion on people's personal lives.

All this use of information can be hard to track for uses of such devices with multiple platforms and providers. And there are security issues as data travels, often internationally, over the internet and the cloud.

IoT devices will become more and more pervasive over time.

What is the "Internet of Things"?

As the FTC report[1] focusses on B2C devices rather than B2B or machine to machine, we'll also focus there. But not to be overlooked is that B2C and machine to machine are also important.

As to scale, FTC note: "*Six years ago, for the first time, the number of "things" connected to the Internet surpassed the number of people. Yet we are still at the beginning of this technology trend.*

Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion."

The Internet of Things – ramping up privacy and security considerations

For B2C, the types of devices in the Internet of Things include, as FTC notes, "*Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day.*"

The EU report[2] in September has a summary of what the Internet of Things does that can't be bettered:

> *The concept of the Internet of Things (IoT) refers to an infrastructure in which billions of sensors embedded in common, everyday devices – "things" as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities. As the IoT relies on the principle of the extensive processing of data through these sensors that are designed to communicate unobtrusively and exchange data in a seamless way, it is closely linked to the notions of "pervasive" and "ubiquitous" computing.*
>
> *IoT stakeholders aim at offering new applications and services through the collection and the further combination of this data about individuals – whether in order to measure the user's environment-specific data "only", or to specifically observe and analyse his/her habits. In other words, the IoT usually implies the processing of data that relate to identified or identifiable natural persons..... The processing of such data in this context relies on the coordinated intervention of a significant number of stakeholders (i.e. device manufacturers – sometimes also acting as data platforms; data aggregators or brokers; application developers; social platforms; device lenders or renters, etc.). The respective roles of these stakeholders will be considered further in the opinion. These different stakeholders may be involved for various reasons, namely to provide additional functionalities or easy-to-use control interfaces that allow the management of technical and privacy settings, or because the user will commonly have access to his/her collected data is via a distinct web interface. Furthermore, once the data is remotely stored, it may be shared with other parties, sometimes without the individual concerned being aware of it. In these cases, the further transmission of his/her data is thus imposed on the user who cannot prevent it without disabling most of the functionalities of the device. As a result of this chain of actions, the IoT can put device manufacturers and their commercial partners in a position to build or have access to very detailed user profiles.*
>
> *In the light of the above, the development of IoT clearly raises new and significant personal data protection and privacy challenges. In fact, if uncontrolled, some developments of the IoT could go as far as develop a form of surveillance of individuals that might be considered as unlawful under EU law. The IoT also raises important security concerns, as security breaches can entail significant privacy risks for the individuals whose data are processed in such contexts.*

What are the IoT issues for B2C?

FTC noted a variety of potential security risks that could be exploited to harm consumers by:

(1) enabling unauthorized access and misuse of personal information;

(2) facilitating attacks on other systems;

(3) creating risks to personal safety; and

(4) collecting personal information, habits, locations, and physical conditions over time (such as companies using this data to make credit, insurance, and employment decisions).

Also, perceived risks to privacy and security, even if not realised, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption.

What providers should do

The FTC report proposes, among other things:

- Build security into devices from the outset: a security by design approach;
- Minimise the data that is collected and retained;
- Test security before product launch;
- Train all employees as to security;
- Retain service providers that provide reasonable security;
- Have access controls to limit unauthorised access;
- Monitor products throughout their life cycle;
- Limit data that is collected and retained (too much data and that is a target for data thieves, plus there is an increased risk of use of data that departs from consumer expectations. There will be a balancing of approach on this, to ensure protection while not stifling innovation);
- Consumer choice is important. But there is no one-size-fits-all approach as that depends on the type of information, etc.
- At least in the US, change to legislation is not yet needed.

1. *Internet of Things: Privacy & Security in a Connected World* (2015), a Report by FTC staff not the Commissioners.

2. *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (2014), EU Data Protection Working Party.

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com