Client Alert

19 June 2015

The Internet of Things: Brave New World

By Amy Collins, Adam J. Fleisher, Alistair Maughan, and Stephanie Sharron

The Internet of Things (IoT) is the network of everyday physical objects which surround us and that are increasingly being embedded with technology to enable those objects to collect and transmit data about their use and surroundings. TVs connected to the Internet and refrigerators connected to online delivery services are just the start of it. In the new world of the IoT, the possibilities are enormous, and the technology industry has so far only scratched the surface of what "machine-to-machine" (M2M) interconnectivity could achieve.

But the ingenuity and innovation which companies will apply to turn the IoT into practical reality is constrained by law and regulation. Existing issues may take on new dimensions and, as technologies combine, so will the legal consequences of those technologies.

In this Alert, we look at the prospects for the IoT.

BACKGROUND

The phrase "Internet of Things" was first coined in 1999 to mean the connection of everyday objects and devices to the Internet. The idea was that "*If we had computers that knew everything there was to know about things – using data they gathered without any help from us – we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory.*"[1]

But back in 1999, the technology required to make the IoT concept a reality was expensive, slow, reliant on dial-up Internet and limited by inadequate storage and processing power. Fast-forward 15 years, and the landscape looks very different. All the key factors have converged to create the ideal conditions to harness the power of M2M connectivity: smartphones, Wi-Fi and broadband connectivity are now ubiquitous; storage capacity "in the cloud" is growing rapidly; sensor technology has developed sophistication while becoming cheap enough to deploy in almost any location; and data handling technology makes it possible to process large volumes of data in real time.

Coupled with improvements in the ability to process and analyze vast qualities of data – *i.e.*, "Big Data" – the possible applications for Internet-connected devices are seemingly endless. Your watch now can download to your computer details of your heart rate, pulse and vital signs, your smart thermostat can turn the heating up or down depending on the weather and your instructions, your smart appliances can help you to track and replenish needed supplies, while you sleep, your baby monitor can monitor your baby's sleep habits and your wristband can now track your fitness. All of this technology is now available, although, in some cases, still at considerable cost.

[1] http://www.rfidjournal.com/articles/view?4986

The uses of the IoT in a commercial context are also exceptionally wide-ranging: ATM data can be used to provide location-specific advertising to consumers via their smartphones, logistics companies can provide real-time parcel tracking services, and car insurance providers can use telematics to monitor driving behavior in order to charge tailored premiums.[2] The IoT also looks set to revolutionize other sectors, including health care, with hospitals providing care via remote monitoring systems, and energy, with the advent of so-called "smart metering".

As with previous waves of technology revolution, the consequences for business will be significant, in ways that are both foreseeable and unforeseeable. Just as the DVD destroyed the market for VHS movie rentals, the huge rise in Internet-enabled TVs seems likely to have the same effect on DVD sales as downloadable video-on-demand becomes ubiquitous. Other outcomes of connecting physical objects in the IoT are harder to predict: not only will existing functionality of separate objects be strengthened by M2M, but new functionalities will be created.

GOVERNMENT ATTENTION

The IoT has been the focus of government attention, not just in the United States but abroad as well. In a speech in 2014 at Europe's CeBIT tech conference, UK Prime Minister David Cameron announced that the British government would be spending an additional £45 million in funding for research in areas linked to the IoT, which, following a series of other funding announcements in this area, takes the total pot to £73 million. Mr Cameron stated: "*I see the internet of things as a huge transformative development - a way of boosting productivity, of keeping us healthier, making transport more efficient, reducing energy needs, tackling climate change*" and Sir Mark Walport, the UK government's chief scientific adviser, is now expected to carry out a review into how these new technologies can be best exploited.

The EU has carried out extensive consultation on the development of the IoT, and the U.S. government, through the Federal Trade Commission, is also tracking the evolution of the market and technology in the sector.

CHALLENGES IN IMPLEMENTATION

The market for the IoT is still in its infancy and there are many challenges involved in deploying a solution. As with any eye-catching new technology, a lot of the hard work that goes into implementation often goes unnoticed.

In the case of the IoT, organizations will have to overcome significant initial hurdles in order to ensure that the solutions adopted are legally appropriate. These invariably include the typical issues confronted in putting into place any sophisticated technology solution: implementing a set of contractual relationships necessary to implement and support the technology; choosing whether to partner with a service provider in order to develop and implement a particular solution; and determining whether and how to use an external agency to harness the necessary computing power to implement fully the solution.

One key internal issue that many organizations will also have to address is the question of who within the business is actually responsible for implementation of the IoT as a product solution. A lot of the tasks required for IoT implementation will fall within the traditional roles of a business's IT leaders, even though the solution itself may be customer-facing. As a result, technology leaders within businesses will need to be heavily involved in evaluating and developing solution requirements. This will continue the progression of the CIO role from overseeing internal enterprise architecture towards an outward-facing role.

[2] For more on telematics, see our June 2013 Alert Monitoring Your Own Behaviour – Guidance for Insurers on the Use of Telematics.

Implementation of the IoT will also involve many of the operations parts of a business. The solution chosen for IoT also will need to be flexible enough to work with the types of devices and operating systems that a business has to deploy. Many of the end-to-end solutions that IoT requires involve among other features, the following key functions:

- *Device and infrastructure management platform*. The IoT requires operators to be able to operate software on devices remotely, without taking the network of sensors out of service. Clearly, where this is performed remotely, security of the device and infrastructure management platform will be crucial.
- *Data Filtering*. The IoT relies on sensors that produce vast amounts of data, but not all data will be relevant to any given application. Accordingly, a key challenge facing developers of IoT solutions is how to identify the thresholds and configurations to process only the data that is necessary for a specified purpose, and filter out the data that isn't relevant.
- *Analytics Platform*. These platforms are necessary to manage and derive the benefits to be gleaned from the huge volume of streamed data collected from remote sensors and devices and manipulate it in real time. This may well be integrated with an organization's approach to "big data" elsewhere in its business. But, whatever the platform (and whether internally provided or outsourced), it should be set up to work with data from different device types and locations and configure it in a way that is useable by the business.
- *Security and Privacy*. Dealing with issues of privacy and data security is essential. If the IoT has a weakness, it is security. Best practices emphasize designing data privacy and security into solutions early in the process of architecting a system. Precautions against unauthorized access or misuse of data need to be baked into IoT solutions from the outset.
- *Integration*. The efficiency and performance of any IoT solution will often depend on the connectors that enable applications to collect and analyze the data and engage in two way communication with the remote sensors where necessary. Effective power management, for example, requires use of communications protocols appropriate for the type of application being deployed.

Businesses also need to focus on future flexibility because the relevant technology is evolving rapidly and the relevant industry players have and will continue to change. While the first wave of solutions may well be focused on a particular application, businesses should invest wisely to ensure that the same sensor network and data infrastructure can be deployed to take on multiple applications.

The IoT has great potential to generate new sources of revenue, improve efficiencies and allow businesses to both increase profits and reduce costs. While it is the internet-enabled products that catch the eye, it is longer term investment in the underlying technology infrastructure itself that is now required and which will ultimately pay dividends.

IOT BENEFICIARIES

Apart from consumers who might soon start to see practical changes to their daily lives as a result of the IoT, a range of companies in different sectors have already targeted the IoT as a driver of future sales.

If the trajectory of the IoT proceeds in the same way as other disruptive technology developments, the initial winners seem likely to be providers of infrastructure and data center capacity, as well as microchip designers. Existing businesses focused on data security also have a key role in the IoT.

Companies that tailor their products to harness IoT capabilities and incorporate the key elements identified above are likely to be the initial front-runners. Semiconductors, for example, need to continue to evolve in terms of size and power draw as well as enabling functionality to improve connectivity between sensor devices and the cloud. With the continued addition of new devices; infrastructure providers also need to integrate their products for maximum flexibility while still ensuring significant levels of data security.

Consumer product manufacturers are perhaps the most obvious potential beneficiaries of the IoT as long as they can identify and roll-out IoT-enabled products having functionality for which consumers are willing to pay and that preserve consumer trust. But if history teaches us anything, it may be that, just as software giants became more valuable than the hardware sellers that capitalized on the first wave of the computing revolution decades ago, today's major consumer product brands may need to identify the applications that connect to their products and master and monetize those new applications and the related data that emerges, or else risk losing those opportunities to others.

Indeed, Google's $3.2 billion purchase of connected thermostat producer Nest in January 2014 shows that the real market for IoT may take shape in ways that we cannot yet anticipate. That acquisition may have been less about a smart thermostat and more about impacting the entire energy supply industry. If the Google and Nest combination can develop a product that proactively saves its users money on their home energy bills by juggling user and utility interaction and harnessing usage data, that could put Nest and its parent, Google, in a stronger position to continue its disintermediation efforts in a whole new sector.

Contact:

Adam J. Fleisher
(202) 887-8781
afleisher@mofo.com

Alistair Maughan
(+44) 20 7920 4066
amaughan@mofo.com

Stephanie L. Sharron
(650) 813-4018
ssharron@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.