January 2015

Alert
Technology & Intellectual Property

Key Technology Trends for 2015

Barry Fishley

As 2015 begins, we consider the following key technology related trends for the year:

- From the 'Internet of Things' to the 'Internet of Everything'!
- A big year for virtual currencies?
- Cyber security trends 2015
- 3D printing
- Outsourcing – growth in SIAM providers in multi-sourcing deals
- Mobile payments

From the 'Internet of Things' to the 'Internet of Everything'!

For some time we have heard of the 'Internet of Things', namely, the infrastructure consisting of billions of sensors embedded in everyday objects such as wearable technology like glasses and watches, devices which track an individuals' physical activities or smart home devices such as washing machines which are controlled remotely over the Internet. These sensors record, store and disseminate data and are connected via the Internet to other objects in a vast eco-system. We see this continuing at a pace in 2015 and beyond. The continued growth in use of social media, increasing use by employees of their own devices for work purposes, proliferation of mobile apps, growth in high speed networks and the general explosion in big data, have all driven the movement towards near-total connectivity. For example, some observers see the growth in wearable technology alone to be anything from US$5.8 billion to US$13 billion by 2018. Similarly there appears to be traction in M&A terms in this area – Google's $3.2 billion purchase of Nest Labs being one notable example.

There is a ubiquitous eco-system made up of various stakeholders including the manufacturers of the devices (such as wearable technology), the software app developers, platform providers, data aggregators, advertisers and analysts and it is likely that new business models will emerge, particularly in relation to the aggregation and monetisation of vast volumes of data.

Of course, there remain challenges in a world of total connectivity. If connected devices really are able to freely communicate with each other, one concern relates to standardisation and compatibility. The concept of an industry "standard" may be difficult, given that the concept of "Internet of Everything" theoretically permeates every device in the world. However, where manufacturers are prepared to patent their technology as "standards essential", the technology may then be made freely available on the same, fair, reasonable and non-discriminatory terms ("FRAND"). Pooling (rather than selfishly protecting) technology in this way and offering such technology to all other manufacturers on FRAND terms will both (i) foster global interoperability and (ii) boost consumer uptake of new technologies. Moreover, the cooperative implementation of standards essentials patents should minimise the risk of "patent wars", as has been endured somewhat relentlessly in the smartphone industry.

Clearly, another key challenge is data privacy. So much so that regulators such as the EU Commission has published opinions on this new eco-system, focusing on the fact that individuals are often unaware of all uses of their data, and therefore cannot be deemed to have properly consented to all uses. Indeed, the European Commission has said that both transparency of intended uses and explicit (i.e. affirmative) consent is required for lawful use of personal data.

Data ownership is another issue. As mentioned, because of the eco-system of various stakeholders, every business entering into this sector should properly understand and record ownership, related intellectual property rights and rights to exploit/monetise the data.

Alongside privacy there are obvious security concerns. With so much valuable data being produced and disseminated, effective security controls must be put in place to guard against a cyber threat but also to ensure that end users have the requisite level of confidence to adopt the various products and services. A recent survey suggested that almost 50% of smart device users do not buy mobile apps because of privacy concerns. The risk of getting this wrong could not be more dire. Not only is there increasing government and regulatory oversight in this area, but new laws are being passed, such as the European Data Protection Regulation, which will increase the powers given to European regulators to impose fines up to the higher of €100 million or 5% of a company's worldwide revenue for serious breaches.

A big year for virtual currencies?

VVirtual currencies such as Bitcoins have gained momentum in recent years and a growing number of companies, such as Dell, accept Bitcoins as a method of payment. In spite of this however, there are several key issues that still need to be addressed which could make 2015 a pivotal year.

The key aims behind virtual currencies are to allow users to transfer money globally with no transaction costs, anonymously and free from any government intervention. Bitcoins are currently the most popular digital currency, created through an algorithm that produces 25 coins every 10 minutes. Hence, the currency is immune from quantitative easing by governments. This would allow the currency to thrive under market forces alone without any government intervention whilst simultaneously avoiding inflation through a fixed rate of production. Furthermore, in theory, individuals are able to buy goods and services internationally without incurring transaction costs or exchange rate commissions.

However, there are a number of key factors which have hampered take up and it will be interesting to see how things play out in 2015:

- Cyber security: organisations that store, exchange and deal with Bitcoins are prone to attacks from hackers who wish to exploit the online security vulnerabilities of the currency. In March 2014 Mt. Gox, the largest Bitcoin exchange, collapsed after hackers managed to steal $460million worth of Bitcoins. A more recent attack in January 2015 has seen hackers steal more than $5million worth of the digital currency from Bitstamp, another major Bitcoin exchange. Bitcoins' susceptibility to security threats and hacks leads to the volatility of its value; in December 2013, the value of Bitcoins peaked at $1,240 per coin in comparison to $276 per coin in January 2015. Despite the volatile nature of Bitcoins, companies such as Microsoft still accept them as a form of payment albeit only in the US, with a non-refundable $1,000 Bitcoin daily limit that can be added to a user's Microsoft account. So, whilst large companies accept the currency in principle, the limitations perhaps illustrate their reservations.

- Regulatory and legal uncertainty: for example, the central banks have given mixed reviews and commentaries. The Bank of England currently does not see the currency as being a threat to the banking system on the whole as Bitcoins only represent a very small fraction of transactions in the economy. In contrast, the European Central Bank, alongside the Bank of France, has published reports warning the consumer of all the risks entailed when dealing with the currency. In the UK, March 2014 saw the rise of the Digital Currency Association which seeks to promote "profound improvement within society" as a whole, giving the currency backing from a variety of companies in different industries. Whilst in the US, the law is beginning to recognise it as a currency that can be regulated.

Cyber security trends 2015

2014 saw cyber security attacks providing headlines throughout the year, beginning with the fallout from the Target debacle, and more recently the political and reputational consequences arising from the attack on Sony Pictures. It seems inevitable that the number of attacks is going to grow in 2015. It is also likely that the attacks will be even more destructive.

If not before, this now means that organisations, large and small, digital and 'bricks and mortar' are (or should be) more alive to cyber security risks than ever. Possible consequences of increased attacks may include the following:

Growth in M&A

The likelihood is that the large IT and tech companies will be looking to acquire smaller players who have innovative and/or different security products so as to enhance their own product portfolios. For example, BAE Systems, Europe's largest defence company, acquired SilverSky so as to increase its share of the US cyber security market.

A tougher regulatory and legal landscape

2014 saw increasing legal and political focus on cyber security and data privacy laws and this is expected to continue and go to the next level. For example 2015 will likely see the implementation of the European Cyber Security Directive which, among other things, will require minimum security standards for public bodies and operators of critical industrial infrastructure (such as transport, healthcare, financial services and energy). There will also be an

additional obligation for relevant organisations to notify its national or designated competent authority of security incidents which have "significant impact" on the continuity of its core services. Whilst this obligation currently applies to telcos and ISPs in Europe it will also apply to a wider set of organisations.

In the US the NIST Cyber Security Framework will continue to be the defacto benchmark for cybersecurity compliance. In the US we also saw the sweep of investment firms by FINRA to assess firms' readiness to cope with cyber security threats.

The Bank of England adopted the "CBEST" framework for testing a firm's resilience to cyber attacks and the European Network and Information Security Agency reviewed 200 organisations for cyber security readiness. The recent announcement by President Obama and Prime Minister Cameron to bolster joint efforts to protect against cyber security attacks means that 2015 will likely see further proactive measures being taken by regulators and governments to assess readiness and promote information sharing on causes and best practice.

Increase in IT security spend?

Some market observers have commented that IT security budgets have reduced over recent years, but it is questionable if this trend will continue. It is likely that there will be more resource and time spent by organisations ensuring that they have in place robust technologies and measures such as a 'battle tested' cyber incident response plan to deal with cyber security attacks.

Greater boardroom scrutiny

Clearly, in light of the litigation, reputational and other risks, it is likely that boards will focus on cyber security matters and ask the relevant questions of management covering topics such as strategy, employee training and response planning.

Greater take up of cyber security insurance

There is no doubt there is more interest in cyber security insurance. Well-advised businesses will also wish to consider how insurance could reduce the risk of business interruption and other operational risks.

3D printing is here to stay and flourish

The number of 3D printers sold in 2015 is predicted to double and established companies are now using the technologies in their manufacturing processes. This has partly been instigated by the fact that a number of the underlying patents in this area expired in 2014. However, there are challenges for organisations (and their investors) which seek to protect their designs from the consequences of mass copying in a way so as not to destroy profitability and avoid the way that private copying has had a profound and long-lasting impact on the music and film industries. As with other areas of technology it is questionable whether the existing IP regime has kept up the pace. Whilst patents and European registered design rights may help confer a level of protection, copyright certainly has not kept up. For example, in the UK generally copyright law will only protect the ultimate 3D item if it is an artistic work, such as a sculpture, or a work of artistic craftmanship. Ways to mitigate this include making greater use of brands (i.e. trade marks) as a differentiator of products and considering whether it is possible to prevent the sale of 3D devices by manufacturers or ISPs who may be knowingly allowing their products/services to be used to produce or sell infringing items.

Outsourcing – growth in SIAM providers in multi-sourcing deals

We see 2015 as a year in which major organisations which outsource non-core functions such as IT and adopt a multi-sourcing model, increasingly look to engage third party service integration and management ("SIAM") providers to manage their supplier relationships.

Multi-sourcing entails the customer entering into separate contracts for each type of service (e.g. applications management and network services) against a single-source arrangement where one supplier is responsible for providing (and/or procuring) all of the services.

In the 80s and 90s many of the major outsourcings were single sourced and were often very long term (e.g. 5-10 years), often with options to extend. In recent times customers, certainly in Europe, have been more willing to take up the multi-source model with shorter term contract periods.

The benefits of multi-sourcing include (i) potential increased service quality as the customer matches suppliers with their specialist offerings; (ii) greater flexibility as the customer is not stuck with the approach of one single supplier; (iii) no supplier lock in; and (iv) greater transparency, particularly in relation to costs, for example, avoiding the scenario where a single supplier could add a profit element to underlying charges from its sub-contractors.

However, there are obvious risks when attempting to efficiently manage these arrangements, particularly where it is likely that some or all of the suppliers will be competitors. One concern is that there is no single supplier taking end-to-end responsibility for all of the services. Further, service gaps and/or overlap are more likely to occur as it more difficult to dovetail all of the arrangements and inter-dependencies. In short, integration of the entire supplier arrangements is much more difficult to achieve. All of this also means that increased customer resource and sophistication is needed in order to properly manage these arrangements.

As a result of these concerns more customers are using dedicated third party organisations to provide SIAM services and the number of these organisations is anticipated to grow this year.

The SIAM provider should manage the various suppliers (including properly identifying independencies), and work alongside the customer to ensure there are no service gaps or overlap. It should also form part of the governance structure where there are disputes.

Best practice suggests that the SIAM provider should be appointed prior to the customer contracting with the various suppliers. This will allow the customer and SIAM provider to use the pre contract process with the other suppliers as way of embedding the principles of collaboration and set up the contract governance structure. In order to aid the SIAM provider's role of facilitating cooperation between the other suppliers, the customer ought to have in place a collaboration or cooperation agreement obliging the different suppliers to communicate with each other, particularly in relation to interdependencies. The agreement should also provide a service fault process that legislates for the prompt identification and resolution of service failures before responsibility for sanctions (such as service credits) is decided.

Risk allocation will inevitably be one of the key points of contention, particularly where the SIAM provider does not exercise control over the other suppliers. Nevertheless, customers should be able to negotiate reasonable liability provisions where the SIAM supplier has failed to effectively deal with arrangements under its control such as project or change management.

Mobile Payments

A leading analyst believes that 2015 will see a double digit increase in the number of smartphones shipped worldwide. Clearly, this means that the smart phone will be even more ubiquitous and retailers, device manufacturers, mobile operators and other players will be looking to increase the use of mobile devices as a way to pay for goods and services. However, it has been estimated that 50% of consumers drop off from completing mobile purchases because they find it too difficult. All this means that 2015 will see businesses continuing to develop their technologies and processes so as to optimise the user experience including making it easier to make payments via the mobile device. The aim is to make use of a mobile device to pay for goods and services a habit. One of the challenges is that there is currently no universal payment platform or system which would greatly aid adoption. Different retailers use different technologies, perhaps in large part so that they can keep and exploit the user's valuable data. Further, businesses are grappling with ensuring that vouchers and loyalty programs are effortlessly folded into the process.

From a legal/regulatory perspective, it will be interesting to see how the regulators, such as the UK Payments Systems Regulator (which will become fully operational on 1st April 2015) will approach mobile payments given its aim for the UK to have world class payment systems that recognise the changing needs of users, but at the same time are reliable and secure.

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any member of the Technology & IP Transactions Group:

Barry Fishley (barry.fishley@weil.com) +44 20 7903 1410