How the Internet of Things Changes Everything

The next stage of the digital revolution

Kate Carruthers

UNSW Australia

Summary: The Digital Revolution Continues with the Internet of Everything

In many ways the Internet of Things will change everything, as devices and software mesh and become part of the connected fabric of the Internet. This article explores the context and potential offered by the growth of the Internet of Things (IoT). It provides an overview of this next phase of the digital revolution that is underpinned by the growth of the social web, web 2.0, and the convergence of technologies such as mobile and ubiquitous broadband. This article also attempts to provide some insight into the potential value of the Internet of Things market in the future.

The opportunities offered by the Internet of Things also raise serious questions about privacy and security in a connected world. As Umair Haque noted recently: "At some point, we should all question the value of an internet that objectifies you, tracks you, and polices you...without your consent." (Haque 2014)

Where we started – Web 1.0 and Web 2.0

The first generation of the digital revolution was about democratisation of communication, and it culminated in Web 2.0 with the development of the social web as exemplified by applications like Facebook and Twitter.

Over a number of years Web 2.0 evolved to be founded on (Dawson 2007):

1. Participation
2. Standards
3. Decentralisation
4. Openness
5. Modularity
6. User control
7. Identity

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n4.69

The combination of a reasonably sound standards framework for web protocols and application programming languages, along with cultural practices such as openness, meant that consumers were fairly well protected in the Web 2.0 world. However, issues of privacy and security were only at a rudimentary stage in the Web 2.0 world.

In the Web 2.0 landscape the average person could understand issues such as privacy and security. Governments were able to legislate to protect consumers and business regulation remained effective to protect people. Financial standards such as the Payment Card Industry Data Security Standard (PCI DSS) provided security for credit card transactions and card providers offered consumer protection for online transactions.

Changes on the horizon with the Internet of Things

The digital revolution continues with the Internet of Things (IoT). Objects that were once inanimate are now embedded with sensors and accelerometers, thus gaining the ability to communicate. Initially proposed by Kevin Ashton in 1999 (Ashton 2009), the Internet of Things (IoT) refers to identifiable objects and their virtual representation in a web like structure. Thus devices are becoming empowered by software, sensors and networking capabilities to create new information networks. The resulting information networks are creating new business models that are starting to disrupt existing business models.

A key feature of Internet of Things devices is their potential to transform a device from a single-purchase item into a service that generates recurring income. Internet of Things value is not in the devices, but in the new services related to the devices. The connectedness of Internet of Things devices is critical and relies upon mature, well-defined and well-understood wireless communications protocols such as WiFi, ZigBee and Bluetooth (Lee et al. 2007). In the Internet of Things context these technologies are supported by 4G LTE, software defined networks, and APIs.

Objects are becoming embedded with sensors and gaining the ability to operate and communicate independently of human intervention. This ability for objects to act autonomously is they key differentiator to previous incarnations of the Internet. This next generation of the Internet is being referred to as the “Internet of Things” (IoT), or “Machine to Machine” (M2M), or “Internet of Everything” (IoE).

In the Internet of Things world computing power tends to be distributed, reducing reliance on centralised platforms. Devices are able to connect via traditional commercial networks as well as using peer-to-peer connectivity that bypasses traditional regulated networks. Connections between devices are API based and allow many-to-many connections via well-defined APIs, thus reducing development overhead. And many of the applications are

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n4.69

network neutral – that is they do not care which network they use for communications as long as it is available; for example they can seamlessly switch between 4G LTE, Wi-Fi or Bluetooth networks.

Internet of Things driven by convergence

Technology Convergence

The Internet of Things is driven by the convergence of a number of technologies, and it is this convergence that gives rise to the possibilities for new business models and for new ways of enabling devices to interconnect and operate in more sophisticated ways.

Ubiquitous communications networks mean that sensor-equipped devices can be deployed in many locations that were impossible in the past. Mobile connectivity enables deployment of field devices into environments that have previously not been possible, for example devices and applications in agriculture can now be deployed using commodity technology at reasonable cost.

3D printing will enable the re-engineering of existing supply chains in novel ways. Over the next decade 3D printing is likely to shift manufacturing away from traditional factories and to enable true just-in-time production.

Sensor networks will enable devices to assess their environment and to act autonomously in response to environmental stimuli; they will also be able to direct other devices to act in response to their sensor data. There are already Internet of Things devices capable directing other devices autonomously based on sensor-derived data. With the vast amounts of data being generated by the Internet of Things devices this enables the use of big data tools and techniques to draw useful inferences and to drive new activity. The feedback loops made possible by big data will have the capacity to fuel innovation in Internet of Things.

Peer-to-peer networks provide an alternative and low cost connection mechanism for Internet of Things devices. For example, it will not be necessary to connect every device in an agricultural application to a mobile phone network to collect data. Instead the devices will be able to connect peer-to-peer and collect data for transmission by a mobile connection hub. Cloud computing provides the scalable application hosting and data storage environments for the Internet of Things. The distributed nature of Internet of Things devices, and the vast amounts of data that will be generated by these sensor-enabled devices, requires scalable and relatively cheap storage. With the evolution of cloud computing and storage solutions such as Amazon AWS and Microsoft Azure this becomes accessible for new entrants such as startups, and reduces operational costs for larger organisations.

The combination of artificial intelligence, commodity sensors and software-defined networks means that devices will be able to operate autonomously. Further, it means that the

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n4.69

supporting software-defined networks will be able to re-route data in response to environmental factors informed by sensor data and enabled by artificial intelligence algorithms.

Powered by APIs

The application ecosystem has been made possible by the evolution of API driven connectivity. APIs, or Application Programming Interfaces, have evolved from the web 2.0 phase of the Internet to act as the glue between diverse and often unrelated systems and applications. An API is a set of standardised pre-defined ways that have been defined for connecting to the program. This enables software developers to publish their API to enable external applications and systems to interact with their software. APIs became prevalent during the growth of the social web in the period from 2004 and are an important enabler of connectivity between devices in the Internet of Things.

Fuelled by the application ecosystem

The Internet of Things will be powered by software applications or applications. We have already seen a proliferation in applications for smart phones and tablets; there is no reason to assume that this will reduce.

> "*Between 2008 and 2017, Google Play and Apple's App Store will be responsible for a mind-blowing number of mobile app downloads: 350 billion.*" (Essany 2012)

On the software development or application development side of the Internet of Things market, a recent global survey of 1,400 software developers (Evans Data 2014) indicated that 17.1% of those surveyed are currently working on Internet of Things applications, and that 23% of those surveyed expect to begin work on them in the next six months. This means that there will be a substantial supply of applications and application developers to fuel development of the Internet of Things ecosystem.

This application ecosystem will be enabled by APIs and supported by the emerging standards landscape. These standards help to define how software, systems and devices can interact with each other. It is still early days from an Internet of Things standards perspective and there are a number of competing standards emerging, for example:

- Industrial Internet Consortium
- AllJoyn
- WebRTC
- Z-Wave Alliance
- Zigbee Alliance
- Open Interconnect Consortium
- Thread
- Internet of Things Consortium

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n4.69

Based upon the experience of the emergence of standards in earlier generations of the Internet it is likely take several years for the standards landscape to settle down and for the winners to emerge.

New Business Models for the Internet of Things

An important feature that changes business models for hardware and devices is that Internet of Things connected devices are transformed from a single-purchase product into a service that generates recurring income. Thus much of the Internet of Things value is not in the devices, but in new services related to the devices. This change in the ability to monetise hardware and related ongoing services means that revenue and competition in the Internet of Things space will be active.

Characteristics of the new business models

The Internet of Things lends itself to open source models, and it enables businesses to use collaboration and loose confederations rather than deep vertical integration. Agile, change-ready organisations will be able to capitalise on developing new applications and services within the Internet of Things.

The devices that form the Internet of Things are connected devices, and these connected devices are typically being controlled via smart phones or tablets and applications (also known as apps). We are seeing an explosion in applications and this is likely to continue to be driven strongly by the Internet of Things:

> "*Between 2008 and 2017, Google Play and Apple's Apps Store will be responsible for a mind-blowing number of mobile app downloads: 350 billion.*" (MacQueen 2012)

These Internet of Things applications will collect vast amounts of personal data from their users, and typically store this information in a cloud-hosting environment. Third parties who do not have a direct business relationship with the user whose data is stored often provide those cloud-hosting services. This, along with the proliferation of data being captured and stored by Internet of Things devices, means that privacy and security will emerge as key business concerns on a scale not yet seen.

Value of the Internet of Things Market

The profits that business leaders are predicting in relation to Internet of Things are enormous:

> *"The Internet of Things, I think will be the biggest leverage point for IT for the next 10 years, $14 trillion in profits from that one concept alone."* (Chambers 2013)

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n4.69

And, while Cisco research estimates that there is US $14 trillion value in the Internet of Things market (Cisco 2013), they also break it down thus:

1) Asset utilisation (reduced costs) of $2.5 trillion
2) Employee productivity (greater labour efficiencies) of $2.5 trillion
3) Supply chain and logistics (eliminating waste) of $2.7 trillion
4) Customer experience (addition of more customers) of $3.7 trillion
5) Innovation (reducing time to market) of $3.0 trillion

In addition to these kinds of estimates of market value, mergers and acquisitions provide a useful insight into the state of the Internet of Things market. Some recent Internet of Things acquisitions include:

- Google bought Nest for US $3.2 billion in January 2014 (Panzarino 2014)
- Google and Nest bought Dropcam for US $555 million (Kumparak 2014a)
- Samsung bought SmartThings for US $200 million (Kumparak 2014b)
- Vodafone bought Cobra Automotive for £115 million (Vodafone 2014)
- Zebra Technologies bought a unit of Motorola for US $3.45 billion (Crowley 2014)

With acquisitions like this it is clear that existing business leaders are positioning themselves to be significant players in the Internet of Things market.

Pervasive computing, the Internet of Things and security

Internet of Things devices are pervading every area of modern life. Wearable devices collect and transmit data about our daily habits. With the increasing prevalence of devices like Google Glass, that record and transmit everyday life, or the dashboard cameras proliferating in vehicles, we are seeing increasing personal data being tracked and stored. Home and portable devices also track our media consumption, with much of the data being recorded and stored with cloud services. This tracking and storage of usage data for Internet of Things devices and applications enables the use of big data to mine the data and determine useful insights into consumer behaviour.

Other trends that are converging with Internet of Things will power the ability to monitor user activity. Among these trends is big data, the ability to mine extremely large data sets for insights about users. Even metadata analysis provides enormous amounts of information about individual user's life. Cloud storage is another key technology that enables Internet of Things. However, cloud and device data remains vulnerable to improper access, as the recent iCloud hack demonstrates (Pauli 2014). When even large companies like Apple are unable to effectively keep user data secure, this raises concerns about smaller startups that provide similar cloud-based services.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n4.69

Much of the Internet of Things device and application data is not well secured, and users do not understand the plethora of details that are stored and transmitted about them. A good example of this is the data embedded in a tweet (Perez 2014), which reveals much more about the user than a mere 140-character message. Or the vast amount of data embedded in the images that users share so readily on social media, as shown by the *I Know Where your Cat Lives* project (Mundy 2014).

The issues that have been with us since the early days of the Internet remain – these include privacy, user control over their own data, and security. However, now due to the scale of personal data that is being collected, stored, and transmitted, these issues have increased in importance. International regulation and standards need to be addressed in a coherent and focused way. At present, Internet of Things is a bit like the Wild West.

Earlier in 2014 a family found that their home baby monitor device had been hacked (Lee 2014) and someone was yelling abuse at their baby. This is a good example of the risks of unsecured Internet of Things devices being installed in homes by users. Typically users will not consider the security implications of installing Internet of Things devices on their home networks. The question of how can users be educated about the risks inherent in these devices remains to be addressed. Further, device manufacturers and software developers have yet to recognise the issues of security and privacy that they must address in relation to the Internet of Things.

The Internet remains inherently insecure. Every week we see another bank or major retailer suffer a hack or security attack (Collins 2014). Further, recent revelations of the Shellshock and Heartbleed vulnerabilities show that some of the fundamental building blocks of the Internet remain a risk factor. This means that the Internet of Things is being constructed on the already insecure foundation of the existing Internet.

The 2014 Target attack is instructive of the kind of security problems the Internet faces. The attack vector for Target was an external third-party HVAC supplier who had access to their internal network. Existing regulations like PCI DSS did not protect them. Another good example is the recent JP Morgan hack (Bloomberg 2014); JP Morgan is protected by an inordinate amount of regulation, as are all banks, but still was hacked. Following is a summary of the existing legislation to which JP Morgan is subject to the following regulation:

- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Gramm-Leach-Bliley Act (GLB) Act
- Electronic Fund Transfer Act, Regulation E (EFTA)

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n4.69

- Free and Secure Trade Program (FAST)
- Fair and Accurate Credit Transaction Act (FACTA), including Red Flags Rule
- Federal Rules of Civil Procedure (FRCP)

The plethora of existing regulation did not protect JP Morgan or their consumers. The real question remains as to how to best protect people and organisations in this changing technical landscape. The solutions are likely to be a combination of effective standards, good business security practice and culture, and the application of appropriate security technology.

Security within the Internet of Things

If even banks are not safe then in what ways can Internet of Things users and regulators ensure that protection is in place? Traditional security approaches relied upon setting up a secure perimeter that was guarded by firewalls and similar technologies. But how does one put a perimeter defence around the Internet of Things?

We have already seen several successful attacks that launched DDoS attacks from dryers, refrigerators, and other Internet of Things devices (Greene 2014).

> *"The global attack campaign involved more than 750,000 malicious email communications coming from more than 100,000 everyday consumer gadgets such as home-networking routers, connected multi-media centers, televisions and at least one refrigerator"* (Proofpoint 2014)

And, as Bruce Schneier points out it is

> *"...often impossible to patch the software or upgrade the components to the latest version. Often, the complete source code isn't available. Yes, they'll have the source code to Linux and any other open-source components. But many of the device drivers and other components are just 'binary blobs' - no source code at all. That's the most pernicious part of the problem: No one can possibly patch code that's just binary."* (Schneier 2014)

This inability to make security patches to many existing devices on the Internet is a great challenge, and now we are adding a new layer of Internet of Things devices that are also difficult to patch. It has already been reported that Wi-Fi enabled light bulbs can be hacked and are unable to have security patches applied.

With the growth in connected medical devices the threat of malware becomes an existential one. Rather than merely stealing data the malware could actually harm a human being.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n4.69

Security is the next 'big thing' that needs to be resolved for the Internet of Things. It is important to ensure that private information remains private and that malware is unable to access critical devices.

Consumer privacy and consent

Consumer privacy faces new challenges in this age of truly pervasive computing. The very services that enable personalisation and customisation of applications and devices also require the collection and storage of personal data.

Users can be tempted to trade convenience for their data, as evidenced by the popularity of Facebook and its personal data fuelled revenue model. Users often do not understand the privacy implications of their agreement to use various software and devices.

It is not always possible to ensure that a meaningful consent can be obtained in an Internet of Things context. For example, one might question how the user of a connected motor vehicle can understand and give consent in respect of the data that their car is now collecting and reporting. A good recent example of the London agreement (Bajekal 2014) that required users to agree to give their first-born children in return for free Wi-Fi access.

From a regulatory perspective the proposed solution to this issue is 'privacy by design' (Privacy by Design 2014). However, it is unlikely that cottage industry of application developers working in bootstrapped startups around the world will ever hear about this notion.

Internet of Things and the Future

> *"We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run."- Amara's law* (Amara, undated)

The impact of the convergence of various technologies – such as big data, 3D printing, autonomous sensor networks, software defined networks, etc. – into the Internet of Things will go through the standard technology hype cycle (Gartner 2014). In the long term it is hard to predict where these new technologies will lead us. However, it is unlikely that anyone can stop the changes in computing and business models that are enabled by the Internet of Things.

The most interesting developments in the Internet of Things are likely to happen at the interstices between the API ecosystem and other emerging technologies, such as 3D printing and remote sensor networks. Yet many of these emerging technologies face some 'wicked problems' (Rittel & Webber 1973) before they are ready for general commercial adoption. For example, self-driving or autonomous cars seem to be an obvious new product in the Internet

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n4.69

of Things. However, some of the technical challenges in getting them ready for the public roads mean they will not be viable in the short term (Ross 2014). Instead, autonomous vehicles may proliferate in closed or controlled environments like mining sites well before they appear on our public roads (Diss 2014). Therefore the Internet of Things will not be just a consumer phenomenon; it will enable a significant change in the way industrial work is done as well.

What is absolutely clear about the future of this market is that both large companies, like Cisco or GE, and startups see the future of the Internet of Things as critical to growth. The possibilities inherent in the Internet of Things are encouraging large players to cooperate so as to share competitive advantage across industry sectors. The recently announced deal between GE, Verizon, Cisco and Intel is an example (Dignan 2014) of this phenomenon. The Internet of Things is the next stage in the digital revolution that is reshaping our world and we can expect to see it drive changes in the way we socialise, work, and consume media and other products.

References

Amara, Roy. 'Amara's Law, http://en.wikipedia.org/wiki/Roy_Amara; accessed 14 October 2014

Ashton, Kevin. 2009. 'That 'Internet of Things' Thing: In the real world, things matter more than ideas.' *RFID Journal*, 22 June 2009. Available at: http://www.rfidjournal.com/articles/view?4986; accessed 14 October 2014

Bajekal, Naina. 2014. 'Londoners Unwittingly Exchange First Born Children For Free Wi-Fi', *Time*, September 29, 2014. Available at: http://time.com/3445092/free-wifi-first-born-children/; accessed 4 October 2014

Chambers, John, Cisco Chief Executive Officer. 2013. 'All Things D Conference interview', May 2013. Available at: http://allthingsd.com/20130529/ciscos-john-chambers-and-boxs-aaron-levie-the-full-d11-interview-video/; accessed 31/8/2014

CISCO. 2013. White paper 'Embracing the Internet of Everything for your Share of $14 trillion'. Available at: http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf; accessed 14 October 2014

Collins, Keith. 2014. 'Data Breaches in the US', *Bloomberg* 4 September 2014. Available at: http://www.bloomberg.com/infographics/2014-08-21/top-data-breaches.html; accessed 4 Sep 2014

ISSN 2203-1693.

http://doi.org/10.7790/ajtde.v2n4.69

Crowley, Amy-jo. 2014. 'Why Zebra's buyout of Motorola's enterprise business will fuel IoT growth', *CBR Online*, 17 April 2014. Available at: http://www.cbronline.com/news/tech/networks/networking/why-zebras-buyout-of-motorolas-enterprise-business-will-fuel-iot-growth-4216325; accessed 14 October 2014

Dawson, Ross. 2007. 'Launching the Web 2.0 Framework', May 30, 2007. Available at: http://rossdawsonblog.com/weblog/archives/2007/05/launching_the_w.html ; accessed 31 August 2014

Dignan, Larry. 2014. 'GE, forges Internet of things alliances with Verizon, Cisco, Intel', *ZDNet*, 9 October 2014. Available at: http://www.zdnet.com/article/ge-forges-internet-of-things-alliances-with-verizon-cisco-intel/; accessed 14 October 2014-12-07

Diss, Kathryn. 2014. 'Robotic trucks taking over Pilbara mining operations in shift to automation', *ABC*, 26 April 2014. Available at: http://www.abc.net.au/news/2014-04-25/computer-controlled-trucks-taking-over-in-pilbara-mining-wa/5412642; accessed 14 October 2014

Bloomberg. 2014. Editorial. 'Why the JP Morgan hack is scary' *Bloomberg*, 6 October 2014. Available at: http://www.bloombergview.com/articles/2014-10-06/why-the-jpmorgan-hack-is-scary; accessed 14 October 2014

Essany, Michael. 2012. 'The Decade of 350 billion app downloads', *Mobile Marketing Watch*, November 19, 2012. Available at: http://www.mobilemarketingwatch.com/the-decade-of-350-billion-app-downloads-26932/

Evans Data Corporation. 2014. Survey, July 2014. Available at: http://www.evansdata.com/press/viewRelease.php?pressID=212; accessed 4 October 2014

Gartner. 2014. Gartner Hype Cycle. Available at: http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp; accessed 14 October 2014

Greene, Tim. 2014. 'Bot Herders Launch DDoS attacks using IoT Devices', *Network World*, 24 September 2014. Available at: http://www.networkworld.com/article/2687169/security0/bot-herders-can-launch-ddos-attacks-from-dryers-refrigerators-other-internet-of-things-devices.html; accessed 14 October 2014

Haque, Umair. 2014. Twitter 2 September 2014. https://twitter.com/umairh/status/506546721007370240; accessed 2/9/2014

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n4.69

Lee, Jin-Shyan; Su, Yu-Wei; Shen, Chung-Chou. 2007. "A Comparative Study of Wireless Protocols: Bluetooth, U WB, ZigBee, and Wi-Fi," Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE, vol., no., pp.46, 51, 5-8 Nov. 2007 doi: 10.1109/IECON.2007.4460126. Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4460126&isnumber=4459874; accessed 4 October 2014

Kumparak, Greg. 2014a. 'Google and Nest Acquire Dropcam', *TechCrunch* 20 June 2014. Available at: http://techcrunch.com/2014/06/20/google-and-nest-acquire-dropcam-for-555-million/; accessed 14 October 2014

Kumparak, Greg. 2014b. 'SmartThings acquired by Samsung', *TechCrunch* 14 August 2014. Available at: http://techcrunch.com/2014/08/14/smartthings-acquired-by-samsung-for-around-200-million/; accessed 14 October 2014

Lee, Adriana. 2014. 'Another connected home hack emphasizes the need for stronger passwords', *Read Write Web*, 30 April 2014. Available at: http://readwrite.com/2014/04/30/connected-home-hackers-stop-yelling-at-babies-foscam#feed=/tag/internet-of-things&awesm=~oEe6yipkTkz40o; accessed 14 October 2014

MacQueen. David. 2012. 'App Download Forecast 2008 – 2017', November 08 2012. Available at: http://www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&a0=7934; accessed 31/8/2014

Mundy, Owen. 2014. Online project, I Know Where Your Cat Lives. Available at: http://iknowwhereyourcatlives.com/about/; accessed 31 August 2014

Panzarino, Matthew. 2014. 'Google just bought connected device company Nest', *TechCrunch* 13 January 2014. Available at: http://techcrunch.com/2014/01/13/google-just-bought-connected-device-company-nest-for-3-2b-in-cash/; accessed 14 October 2014

Pauli, Darren. 2014. 'JLaw, Kate Upton exposed in celeb nude pics hack: 100 women victimised as Apple iCloud accounts reportedly popped', *The Register*, 31 Aug 2014. Available at: http://www.theregister.co.uk/2014/08/31/jlaw_upton_caught_in_celeb_nude_pics_hack/; accessed 31/8/2014

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n4.69

Perez, Sarah. 2010. 'This is What a Tweet Looks Like', April 19, 2010, *ReadWrite*. Available at: http://readwrite.com/2010/04/19/this_is_what_a_tweet_looks_like; accessed 31/8/2014

Privacy by Design. 2014. Available at: http://www.futureofprivacy.org/privacy-by-design/; accessed 14 October 2014

Proofpoint. 2014. Media Release, 'Proofpoint Uncovers Internet of Things (IoT) Cyber attack', January 16, 2014. Available at: http://investors.proofpoint.com/releasedetail.cfm?ReleaseID=819799; accessed 14 October 2014

Rittel, Horst W. J; Webber, Melvin M. 1973. 'Dilemmas in a General Theory of Planning', *Policy Sciences* 4: 155–169, 1973. Available at: http://link.springer.com/article/10.1007%2FBF01405730; accessed 14 October 2014

Ross, Philip E. 2014. 'Self-Driving Cars Face Serious Roadblocks, Experts Say', *IEEE Spectrum*, 10 September 2014. Available at: http://spectrum.ieee.org/cars-that-think/transportation/self-driving/future-of-self-driving-cars-detroit-panel; accessed 14 October 2014

Schneier, Bruce . 2014. The Internet of Things Is Wildly Insecure - And Often Unpatchable, *Wired*, Jan 2014; accessed 10 October 2014

Vodafone. 2014. Media release, 'Vodafone completes acquisition of Cobra Automotive Technologies', Vodafone 8 August 2014. Available at: https://m2m.vodafone.com/cs/m2m/insight_news/2014-06-18-vodafone-completes-acquisition-of-cobra-automotive-technologies; accessed 14 October 2014

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n4.69