Deloitte.

The Deloitte Consumer Review

Digital Predictions 2017

March 2017

Contents

About this report
In this publication, references to Deloitte are references to Deloitte LLP, the UK member firm of DTTL.

Please visit http://www.deloitte.co.uk/consumerreview for additional content related to the Consumer & Industrial Products industry.

Foreword

Welcome to the latest edition of the Deloitte Consumer Review. In this report we look at how six digital technology trends will accelerate disruption in the consumer market in 2017. In doing this we draw upon the Deloitte Global 16th annual Technology, Media & Telecommunications Predictions report and consider the implications for consumers and the businesses that serve them.

These trends involve technologies that are either improving localised consumer experience on mobile devices, or the infrastructure that enables them. As a result consumers are more and more empowered and sitting at the centre of the virtual economy.

The trends include:

1. Fingerprint, the biometric trailblazer
2. Unleashing the power of machine learning in mobile devices
3. The last frontier: indoor navigation made possible
4. Automatic braking system: the road leading to self-driving
5. 5G: the promise of a big bang in connectivity
6. Increase in the severity of DDoS attacks

The consumer market continues to be disrupted by consumers' usage of an expanding range of ever more powerful, faster-connected and better-specified digital devices. Innovation and integration across digital, physical and biological ecosystems are accelerating. The term 'exponential disruption' has been coined to capture a change that is no longer linear, leading to the fourth industrial revolution.[1]

This growing harmonisation and integration of technologies are transforming both the way consumers behave and how businesses need to operate.

User-centric design, exploiting the near omnipresence of the mobile platform, plays an increasingly important role in driving innovation. Mobile technologies have been transformed into powerful engines for change. Dedicated machine-learning capability in the smartphone is supporting the shift from the era of digitalisation to the era of cognitive automation and augmentation, with intelligent speech interfaces that enrich our interactions 'beyond the glass' touchscreen.

For businesses, this fourth industrial revolution is seeing the emergence of smart organisations where virtual and physical systems cooperate in an agile and flexible way. Finally, as well as the exponential pace, these emerging technologies and innovations are converging and resulting in the emergence of new competitors, meaning it is now more important than ever to experiment and understand their implications.

We hope this report gives you 'food for thought' in such exciting and disruptive times and we welcome your feedback.

Phil Neal
Digital Transformation Lead,
Consumer and Industrial Products

Fingerprint: the biometric trailblazer

The active base of fingerprint reader-equipped devices will top **1 billion** **for the first time in early 2017.**

90% of devices will be **smartphones** and **tablets**.

Businesses should consider how best to leverage the growing number of individuals who have become accustomed to using biometric sensors on their phones.

Unleashing the power of machine learning to mobile devices

Over **300 million smartphones** sold in 2017 will have on-board neural machine-learning capabilities. This will allow smartphones to **perform machine** learning tasks…

…even when **not connected** to a network.

As AI and machine learning are more skilfully integrated into devices, the ability to anticipate consumer needs will improve as will user experiences.

The last frontier: indoor navigation made possible

At least a **quarter** of human and machine uses of digital navigation will include or exclusively be **indoors by 2022**.

This is due to an increase in **Wi-Fi hotspots**, **dense cellular networks**, **beacons**, **LED lighting**, **ultra-wide broadband (UWB)** and **magnetic positioning**.

Precise indoor navigations will save time for consumers and improve productivity for consumer businesses. Examples where this could have an impact include shopping centres, airports and entertainment venues.

Automatic braking system: the road leading to self-driving

By 2022 automatic emergency braking (AEB) will contribute to a **reduction of annual US motor vehicle deaths** by **6,000**, a **16% decline** compared to 2017.

Overall expected price which consumers are willing to pay for future automotive technologies

2014 = £677

2016 = £375

AEB is the top technology for over 20,000 respondents across 17 countries according to Deloitte's recent Global Consumer Auto Survey.

5G: the promise of a big bang in connectivity

Over **200 mobile networks** will include elements of **5G network** architecture by the end of 2017.

These will be found among **upgraded 4G (LTE-A and LTE-A Pro) networks**, which will provide a steady progression to the full launch of 5G in 2020.

Faster connectivity will allow consumers and brands to interact more and more in a real-time basis and while on the move.

Increase in the severity of DDoS attacks

10 million Distributed Denial of Service (DDoS) attacks, and **at least one** Terabit DDoS attack expected **per month** during 2017.

The average size of attack is increasing year on year

300 Gbit/s	*400 Gbit/s*	*500 Gbit/s*	*1 Tbit/s*
2013	2014	2015	2016

Consumer businesses should consider a range of options to mitigate the impacts of DDoS attacks including decentralisation, dynamic defence, geographic filtering and certification marks for connected devices.

The digital consumer

The UK user base for smartphones is approaching a peak at 81 per cent. No other personal device has had the same commercial and social impact and at present no other new device seems likely to. The smartphone permeates our lives as it incorporates ever more functionality and gets even faster.

The adoption of digital technologies, such as smartphones or voice-controlled devices, continues to drive a revolution in the way consumers behave and engage with the companies serving them.

Digital devices have become an increasing part of our world, listening to us, anticipating our needs and helping us unprompted. The consumer sector so far has been one of the main beneficiaries of a revolution that has made consumers' lives more efficient and more productive.

This digital revolution is challenging businesses. They must change how they interact with their consumers – and also increase the speed at which they transform their operations, if they are to compete. New business models are threatening what used to be 'safe' market shares for well-established incumbents. For example, in the UK retail sector Amazon's entry into the grocery sector is forcing the big four to rethink how to continue to compete. The move to purchase Argos would suggest Sainsbury's believes diversification is the way to prosper.

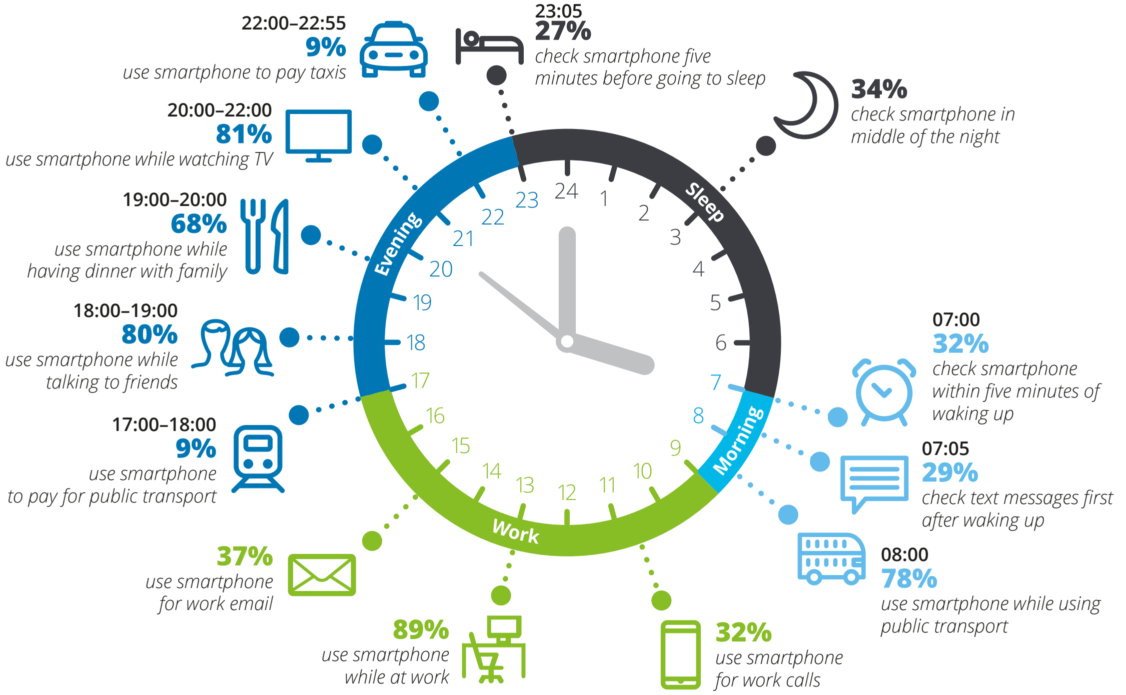
Digital devices have become an increasing part of our world, listening to us, anticipating our needs and helping us unprompted.

Something in it for everyone

Furthermore, with the development of new business propositions delivered via mobile devices, the line between consumers and organisations is blurring. Businesses are increasingly enrolling consumers in real-time via their mobile device enabling the consumer to provide rich behavioural data, or help businesses with some of their enterprise challenges. Digital has catalysed the fast growth of so-called 'contingent working' or crowdsourcing business models that are a sign of things to come. Contingent working or the more recent term 'gig economy' describes a labour market characterised by the prevalence of short-term flexible contracts or freelance work, as opposed to permanent jobs. An individual can instantly switch between being a consumer or a contingent worker by simply swapping apps on their mobile device.

Businesses such as Deliveroo use the gig economy to sell and deliver restaurant meals to the household or office. Their technology platform optimises food ordering and delivery. It integrates web and mobile orders with a restaurant tablet-based point-of-sale and optimises logistics via a delivery driver smartphone software. Streetbees is a crowdsource business that connects brands and consumers through a mobile app at the exact moment a consumer experiences the brand, allowing the consumer to share data about his experience in real time.[2]

Figure 1. A day in the life of a smartphone



Note: Respondents for which a particular activity does not apply have been excluded from this analysis (e.g. respondents who do not work have not been asked if they use their phone at work).
Weighted base: Respondents who own or have access to a smartphone (3,251)
Source: UK edition, Deloitte Global Mobile Consumer Survey, May–Jun 2016

Crowdsourcing is growing and has been used by over 25 per cent of Fortune 500 companies and is due to increase to 75 per cent by 2020.[3] According to Deloitte, almost half of the executives surveyed (42 per cent) expect to increase or significantly increase the use of the gig economy in the next three to five years.[4]

The digital revolution is driven by three trends: increasing digital device ownership, more and more powerful devices and faster connectivity speeds.

This digital revolution is challenging businesses. They must change how they interact with their consumers – and also increase the speed at which they transform their operations, if they are to compete.

The true domination of the smartphone

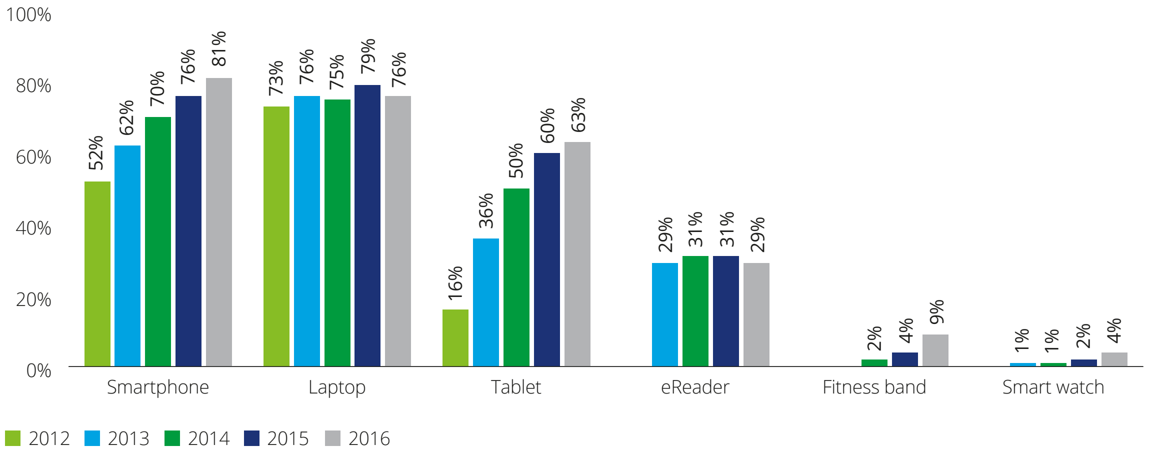
The smartphone is the ever-present companion of most smartphone owners (see Figure 1). It is both useful and entertaining, both functional and invasive. It facilitates creativity and consumption. It fosters productivity – and offers distraction. It is more and more an all-in-one device.

Today, according to Deloitte research, 81 per cent of UK consumers own or have access to a smartphone. Among 18-44 year olds the rate of ownership is reaching a plateau at 91 per cent (see Figure 2).[5] The growth in the ownership of tablets continues to decelerate and for the first time smartphone ownership has overtaken that of laptops.

The tablet was the future once. It has triumphed insofar as nearly two-thirds of people in the UK have access to one but it has not managed to usurp the desktop PC, laptop or the smartphone, and appears unlikely to do so in the medium term.

The impact of the smartphone is likely to become more pronounced still. Greater connectivity speeds are likely to unlock a whole range of new applications, in addition to live streaming as a mainstream activity. Once components such as fingerprint readers become available in the majority of devices, smartphones may become increasingly accepted as a proof of identity. Smartphone penetration may be approaching a peak, but with a growing range of new applications and ever more cognitive abilities, consumers' concentration of power in one single device is increasing, hence the smartphone's impact should continue to grow over coming years.

Figure 2. UK digital devices owned or accessed



Source: Deloitte UK, Global Mobile Consumer Survey, May-Jun 2016
Base: All UK respondents, n=4,003

Consumer Internet of Things: some way to go

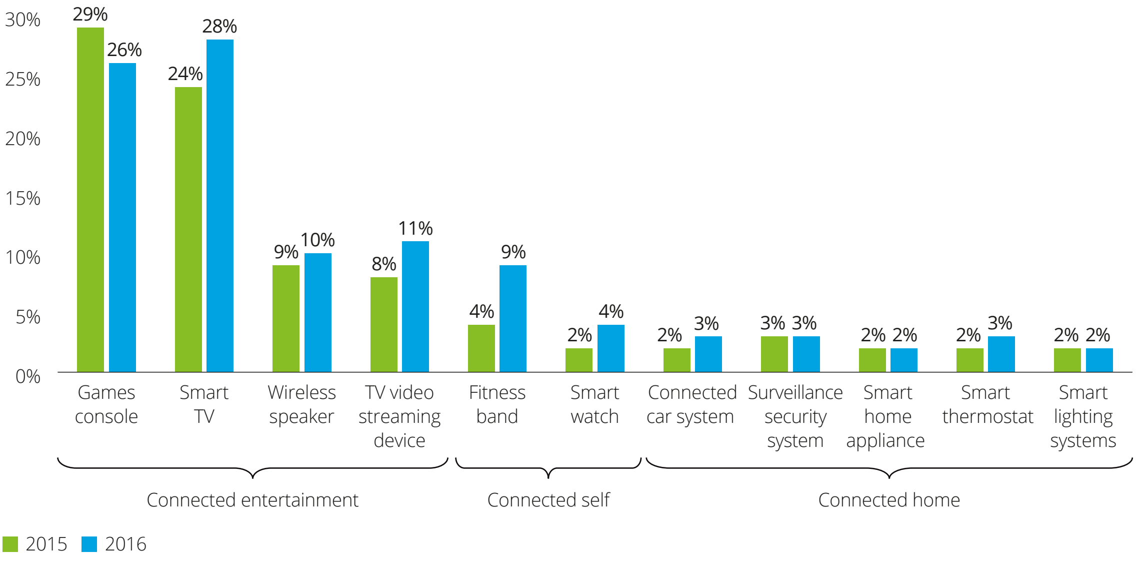
The connected-self category of the Internet of Things (IoT), fitness bands and smart watches, have enjoyed a doubling in adoption over the past year. Despite this, neither device yet boasts penetration in double figures. Just nine per cent of UK adults own a fitness band, and only four per cent have a smart watch. This is very low when compared to 81 per cent smartphone penetration (see Figure 3).

Overall, ownership of connected home devices has barely changed in the last year. Ownership of smart lights and smart appliances remains at two per cent and connected surveillance systems at three per cent. These products have been relatively niche since launch.

While UK consumers are aware of the potential benefits of IoT, perceived high prices and scepticism about the technology are deterring them from buying more connected devices. The era of IoT device ownership across multiple categories is likely to dawn when its benefits align with mainstream consumer behaviour.

Our research suggests that we will see a gradual uptake in IoT devices for the home – not overnight adoption. One of the biggest drivers for adoption will be the replacement cycle. The majority of new TV models are now 'smart-ready' and we will continue to see other home devices offer connected features as standard. As consumers replace their old kettles, ovens, fridges and lighting in coming years, we will see a gradual rise in IoT adoption. Through targeted promotions and marketing and in-store demonstrations, retailers may be able to speed up the replacement cycle.

Figure 3. Other connected devices adopted by adults in the UK



Source: Deloitte UK, Global Mobile Consumer Survey, May-Jun 2016
Base: All UK respondents, n=4,003

Fingerprint: the biometric trailblazer

Deloitte predicts that the active global base of fingerprint reader-equipped devices will top one billion for the first time in early 2017. Additionally Deloitte expects each active sensor will be used an average of 30 times a day, implying over 10 trillion aggregate presses globally over the year.[6]

Deloitte further predicts that about 40 per cent of all smartphones in developed countries will incorporate a fingerprint reader as of end-2017. This compares to 26 per cent as of mid-2016.[7] Deloitte expects that at least 80 per cent of users with a fingerprint reader-equipped smartphone will use this sensor regularly; this compares to 69 per cent of users in mid-2016.[8]

Over 90 per cent of active devices with fingerprint readers are likely to be smartphones and tablets.[9] By the end of the decade Deloitte foresees that fingerprint readers will have become as ubiquitous as front-facing cameras on smartphones. By this time fingerprint sensors for identification and authentication are likely to have been incorporated into a range of other devices, from laptop computers to remote control devices.

The smartphone fingerprint reader's success is due to its ability to provide a rapid and discreet way, relative to passwords, of unlocking phones and authenticating transactions. It is a challenge for most people to remember multiple strong passwords and by 2020 the average user may have 200 online accounts.[10, 11]

The main purpose for the trillions of aggregate uses of fingerprint readers in 2017 is likely to be for unlocking phones and tablets – typically dozens of times per day. As the ubiquity of the fingerprint reader grows, Deloitte expects a growing proportion of apps and websites to support the technology, primarily as an alternative to password entry.

Billions of smartphones and tablets are expected to be capable of processing and collecting multiple types of biometric inputs, including face recognition, voice pattern and iris scan in 2017, but usage of fingerprints is likely to lead the way. Deloitte expects, as of end-2017, that the percentage of smartphone or tablet owners using facial, voice or iris recognition for authentication will be less than five per cent compared to 40 per cent for fingerprint readers.[12]

The usage of biometrics is millennia-old but its large-scale adoption in modern technology has taken place only in recent years and is likely to become increasingly sophisticated and effective in 2017 and in years to come.[13]

This prediction has focused mostly on the use of fingerprint readers but the smartphone's presence in all aspects of our daily lives lends itself well to combined use of other data unique to us, such as typing patterns and location information. Deloitte would expect blended usage of various biometric inputs, known as multi-factor authentication, to become increasingly popular.[14] It would still provide more robust authentication. For example, a banking app could use both fingerprint and voice recognition, with the fingerprint providing initial access and voice inputs additional verification.

> The smartphone fingerprint reader's success is due to its ability to provide a rapid and discreet way, relative to passwords, of unlocking phones and authenticating transactions. It is a challenge for most people to remember multiple strong passwords and by 2020 the average user may have 200 online accounts.

Case study: Mastercard rolling out fingerprint and 'selfie' payment technology[15]

Mastercard is rolling out its 'Identity Check Mobile', a new payment technology app that uses biometrics like fingerprints or facial recognition to verify a cardholder's identity, across Europe. The aim of the technology is to eliminate the need for cardholders to recall passwords and to simplify the process of online shopping, by allowing consumers to confirm their identity by taking a 'selfie' photograph or using the fingerprint scanner on their smartphone.

Biometric systems are already gaining prominence in the retail space with quicker checkouts and easier payment systems. The retail biometric market is set to reach $1.6 billion in 2020 from $625 million in 2015.

Bottom line

Organisations should consider how best to exploit the growing base of fingerprint readers and the large number of individuals who have become accustomed to using them on their phones.

Biometric systems are already gaining prominence in the retail space with quicker checkouts and easier payment systems. The retail biometric market is set to reach $1.6 billion in 2020 from $625 million in 2015.[16] In particular, facial recognition, a technology mainly employed by airport security, border agents and casinos, is now being used by retailers. In its commercial retail application, the faces of individuals caught on camera are converted into a biometric template and cross-referenced with a database for a possible match with past shoplifters or known criminals. All this has been made possible by the arrival of networked, high-resolution security cameras and rapidly advancing analytical capabilities.

The same technologies used to identify thieves, however, can also be used to track customers. Indeed, video surveillance is increasingly doing double duty to help stores improve sales. Many of the companies providing facial recognition capabilities also offer sophisticated analytics applications that capture in-store 'dwell times', responses to product displays and traffic flow. For traditional brick and mortar retailers, this sort of information has helped level the playing field with online retailers, who routinely track and profile their customers through cookies. In the UK, a 2015 survey of 150 retail executives suggested that a quarter of them use facial recognition in-store.[17]

Applications to provide rapid and secure authentication could include:

- check-in and security: Already some airports have either implemented or are trialling biometric technologies to facilitate check-in and security. For example, while some airports' e-gates at security are now fully functioning, using a 'chipped' passport and advanced facial recognition technology to compare the passenger's face to the digital image recorded in their passport, Schiphol airport and KLM are trialling facial recognition as an alternative to boarding passes and passports.[18] Hotels are also starting to invest in biometric technologies for their check-in process. In the Kube hotel in Paris, guests have to use their fingerprint to get into their rooms, thus avoiding the need for keys or magnetic cards.[19]

- e-commerce checkout: the ability to make fast and secure payments using a fingerprint reader to provide a one-tap checkout will be attractive to most online shoppers, especially if it offers improved payment security.

- in-store payment: in-store payment apps can use near-field communication (NFC) technology to enable the user to authenticate a payment by putting their finger on a sensor and holding the phone near the NFC reader. This eliminates the need to enter a PIN.

- 'your account' data: biometrics could be used as an alternative to entering a password to get access to any account or public services information and data such as health records.

- online subscription services: providers of music, premium news, television or other content held behind a paywall could control illicit sharing of user IDs and passwords by requiring users to authenticate themselves using fingerprints. A single-user account could be tied to one set of fingerprints and the prints would be far harder to share than a password.

Case study: Apple Pay[20]

Apple Pay functionality has now arrived on the web. Consumers can make purchases using Apple Pay and the Touch ID fingerprint scanner in the Safari internet browser using an iPhone, iPad or a Mac running macOS Sierra. With the Mac, the consumer authenticates its purchase via a hook-up with an iPhone or an Apple Watch.

Every payment generates a randomised string of numbers, a so-called Device Account Number, which is transmitted via a secure chip in Apple devices. As a result consumers no longer need to share credit or debit card numbers with an online retailer. Actual card numbers are not stored on the device, nor on Apple servers, making it very secure.

Unleashing the power of machine learning in mobile devices

Deloitte predicts that over 300 million smartphones, or more than a fifth of units sold in 2017, will have on-board neural network machine-learning capability.[21, 22] These are computer models designed to mimic aspects of the human brain's structure and function, with elements representing neurons and their interconnections. They will allow smartphones to perform machine-learning tasks even when not connected to a network.

This functionality will enhance applications including indoor navigation, image classification, augmented reality, speech recognition and language translation even where there is little or no mobile or Wi-Fi connectivity, such as in remote areas, underground or on an airplane. Where there is connectivity, on-board machine learning – the process by which computers can get better at performing tasks through exposure to data – may allow tasks to be done better and faster, or with more privacy.

Machine learning on-the-go will not just be limited to smartphones. These capabilities are likely to be found over time in tens of millions (or more) drones,[23] tablets, cars,[24] virtual or augmented reality devices,[25] medical tools,[26] Internet of Things (IoT) devices[27] and unforeseen new technologies.

Historically, having gaps in connectivity was not a big deal: if our phones could not provide image classification or indoor navigation, we managed to do without. But as our phones have become more powerful and ubiquitous, they are becoming critical devices in our daily lives and need to be able to perform machine-learning tasks all the time. A smartphone-enabled medical device or vehicle-driving application that works all the time may be a matter of life or death, rather than just convenience.

As mobile devices become more capable of performing machine-learning tasks, there are some interesting implications.

Reducing data transmission

It may reduce the amount of data that needs to be transmitted. Reducing the amount of data to be transferred (and latency) is particularly important in potential IoT applications and analytics.[28] Furthermore, carrying out machine learning on-board is inherently more private and secure.[29]

Moving to the edge

Smartphones are increasingly becoming a critical tool for most people. At present the mobile machine-learning device must connect to data centres – but can only do so provided the mobile network is working. Mobile devices able to perform machine-learning tasks without heavy reliance on connectivity to the cloud would be a significant gain.

Machine learning will power IoT

In the near term, most of the on-board machine-learning capacity will be on consumer devices such as smartphones and tablets. But over time the applications for IoT devices may be more transformative. Autonomous vehicles will need to have machine-learning capacity all the time, not just when cell signals are strong. At the speed cars travel on highways, making decisions on-board would offer vitally lower latency: at 80 miles per hour (MPH), or 36 meters per second, every millisecond counts. Achieving lower latency could also be a reason to use mobile machine-learning chips or software in jet engines, medical devices, or even oil and gas pipelines.

Preventing malware attacks

Another of our 2017 predictions looks at the role of compromised IoT devices (for example, webcams) in Distributed Denial of Service (DDoS) attacks.[30] We discuss this in more detail later in this report, but on-board machine learning has the potential to protect the proliferation of devices in our lives and might even help turn the tide against the growing wave of cyberattacks.

Case study: Netflix is a great example of artificial intelligence (AI) and machine learning in action today

Netflix tries to predict what you want to watch next. The more you watch, the more valuable the service. Depending on the amount of data collected about a member's viewing habits, Netflix can say with 85 to 90 per cent confidence what else a member is likely to enjoy watching.

Bottom line

Thanks to a surge in the availability of consumer data, brands can already make better inferences about consumer wants and needs, but as AI and machine learning are more skilfully integrated, insights will only get better, as will the ability to anticipate consumer needs – and even to make decisions on customers' behalf without their input. Machine learning, by looking for patterns of data such as consumer behaviour, and via statistical inferences, creates self-learning algorithms to make better decisions and optimise user experiences.

This will open up a whole new world for brands and marketers by helping them more accurately target consumers. Machine learning and AI will do the hard work of looking for patterns in consumer preference and behaviour data. This also means it will require less input on the consumer's part as long as she or he is comfortable sharing their consumption pattern data. This seems unlikely to be difficult as consumers start to see the gains, such as recommendations and proposed products and services that are more and more relevant and personalised, helping consumers save time and become more efficient.

IoT and machine learning will also open up a new realm of opportunities for manufacturers. IoT products with in-built machine learning will automatically action a solution when a problem occurs with the machine itself. It will also allow one machine to talk to another if the two can work together better – such as an alarm clock telling your coffee machine when to prepare you a fresh cup of coffee.

One prediction we can confidently make is that it will become more difficult to secure fair consumer protections in a world of highly connected, data-rich, and increasingly intelligent devices. Machine learning may not always produce predictable results. If individuals act on the basis of such results it may raise issues of responsibility and accountability. Similarly, as businesses build more comprehensive data sets on consumers, and engage with them based on richer inferred insight, the 'value exchange' – what they get back in return for the potential privacy intrusion – needs to be seen as fair and transparent. Policy that keeps pace with the technology, with appropriate 'opt outs' will be key if consumers are not to feel exploited.

Case study: North Face experiments with AI[31]

The outdoor apparel, equipment and footwear retailer, North Face, launched a new interactive online shopping experience powered by artificial intelligence. Customers can now use natural conversation as they shop online via an intuitive, dialogue-based recommendation engine and receive clothing recommendations that suit their needs – just as if they were being assisted by a sales assistant in a store.

The last frontier: indoor navigation made possible

Deloitte predicts that as of 2022 at least a quarter of all human and machine uses of precision digital navigation will include an indoor leg or be for an entirely indoor journey. This compares to less than five per cent of all uses in 2017. Growth will be stimulated by sustained improvements in the accuracy of indoor navigation over the medium term, permitted by an array of positioning data, improved analytical tools that interpret multiple indoor location datasets in parallel, and more high-quality indoor maps.

Satellite-based digital navigation, accompanied by the digitisation of street maps, has revolutionised how people and objects are located and guided. However, satellite navigation has one fundamental blind spot – its signals, sent from a height of 24,000 kilometres, are often too weak to penetrate solid roofs by the time they reach ground level.[32] Consequently their signal may not be visible to receivers indoors, such as smartphones, unless the user is close to a window or below a glass roof. Yet people spend over 90 per cent of their time indoors.

Realising the promise of indoor navigation requires, just as with outdoor navigation, two core components: real-time communication of location, and digital maps.

Existing indoor location data sets: Wi-Fi and mobile networks

As of 2017, indoor location can be ascertained from two principal sources: Wi-Fi routers and mobile base stations.

Wi-Fi networks can, with sufficient network density, be accurate to a few meters, and are currently the richest source of indoor positioning data.[33]

This degree of accuracy enables people to be guided to a store within a shopping centre and then a department within it, to a staircase within a stadium, to a meeting room on an office floor, or to the right carriage on a train.

As of the start of 2017, there were significantly more Wi-Fi routers than mobile base stations. One forecast estimates that there will be 340 million Wi-Fi hotspots (shared routers) globally by 2018, a sevenfold increase on the 50 million base as of 2015.[34]

Positioning via mobile networks is a by-product of the provision of connectivity. This approach provides localisation accuracy of, at best, a 50 metre radius on a 4G network. Accuracy should steadily improve as network density increases.

Network cell density should increase over the next decade, firstly via 4G networks, and then via 5G.

In addition to the existing data sets that can be used to estimate location, there are several more that are in early or nascent stages of deployment. Over the medium term, beacons, LED lighting, ultra-wide broadband (UWB) and magnetic fields could be used to complement existing data sets.

Beacons can provide location to within a metre, enabling them to be used for a wide range of indoor navigation applications. A beacon is a small, inexpensive (circa £4) Bluetooth Low Energy (BLE) equipped module. As of 2016, there were an estimated seven million beacons installed globally, covering a much smaller area than Wi-Fi routers or mobile networks.[35]

Deploying beacons just to provide location might be a hard business case to make, but the returns from proximity marketing – sending offers to customers within a specific area – may pay for the deployment on its own.

Beacons can interface with the majority of smartphones, but Bluetooth must be switched on and an app downloaded.

LED lighting can be used to provide accuracy to half a metre.[36] As at the start of 2017, deployment was still at an early stage.

LEDs, increasingly ubiquitous, generate a pulsing light signal. Each LED light can send a unique identifier to a receiving device, most commonly a smartphone.[37]

In a retail environment, it may be that the business case for deployment of an Ethernet-powered lighting and sensor network would cover the entire cost of installation, and that user navigation would come as a zero-cost additional benefit. Retailers are constantly striving to understand better customer behaviour, and this may be the primary reason for deploying the lighting system.

The approach requires the user to download and open an app, and for the smartphone's front camera to be on and in line of sight of the light.

Ultra-wide broadband (UWB) can provide indoor accuracy to 5-10 centimetres.[38] UWB indoor positioning works by measuring range and/or angle estimates from a set of fixed points to a tag positioned on an object. The set of measurements is then used to calculate position. UWB sensors are typically positioned on the ceiling of a building.

This approach is currently deployed in factories and warehouses as a way of enabling objects to be located faster. This method, however, requires a separate chip to work and is used mostly today in manufacturing environments.

Magnetic positioning only uses the magnetometer (compass) on the person's phone and tries to evaluate the disturbances in the gravitational field caused by metal structures inside the building.[39]

These magnetic disturbances create a unique gravitational footprint for every building. This footprint can be recorded by extensive mapping, and can estimate location within two metres.

Exploiting smartphone sensors

A smartphone's internal array of inertial measurement unit (IMU) sensors can be used in tandem with satellite positioning and internal positioning data to determine a user's location.[40]

Digital Indoor Maps

An improvement in indoor positioning accuracy requires a commensurate increase in indoor mapping for its benefits to be exploited fully.

There are likely to be multiple players that see significant benefit in generating indoor maps. A shopping centre could use indoor maps to enable people to find stores, departments and even aisles faster.

Google offers indoor maps as an extension to its outdoor maps. As of end-2016, there were hundreds of sites around the world whose indoor maps were available.[41] Site owners are invited to upload their maps and are provided with an app to help increase their accuracy.[42] Google has also created a backpack-mounted digital cartography instrument that enables maps to be created by someone walking through a venue. The backpack features Simultaneous Localisation and Mapping (SLAM) technology.[43]

Case study: Harrods launches new navigation tool[44]

Harrods, the luxury department store, has launched a pioneering in-store mapping tool in the Harrods app. With 1 million square feet of retail space spread over seven floors, Harrods has developed an innovative way of helping customers navigate the store, made possible by a network of over 500 iBeacons that have been installed on the ceilings of their 167-year-old building. The new in-app tool marks a first in Europe for a major department store by supporting customers' shopping experiences with a live digital mapping solution.

The Mobile Store Guide detects the location of a customer's device via Bluetooth, and highlights their location on the interactive map. As well as browsing maps, customers can locate brands, services and restaurants using a searchable store index, and find routes to their favourite departments.

The new feature is available on Apple devices (iPhone and iPad) and can be accessed by downloading the iOS version of the Harrods app from the App Store.

Bottom line

Precise indoor navigation's potential is significant, and could be transformative, and is likely to benefit vertical sectors most, and have impacts on government, business and consumers alike. However, it will be challenging to deliver and the precision of information yielded is likely to be inconsistent in the short run.

Consumers' growing power has been facilitated by easier access to information and products in the digital space. New indoor mapping capability will further enhance consumers' shopping experience by completing the seamless loop consumers take to get to what they want. For example, through a simple web engine search on a mobile device, a consumer can quickly skim through an array of goods to find the product they are after, indoor navigation will then take them directly to where the product is stocked or located. This has the potential to reinvigorate the physical space's ability to compete with online commerce.

Retail time is wasted when shoppers cannot find a store within a shopping centre, or when they need to be directed to a floor and an aisle, or to a less busy check-out area. Staff could find goods more quickly on the shop floor and in stock rooms with precise indoor guidance. Location data can also be used to send geographically-targeted marketing messages to customers. Robots could be also be used to fetch items from the stock room. The availability of precise indoor navigation is likely to become a differentiator for shopping centres in the medium term. This benefit may well encourage shopping centre owners to encourage mobile networks, Wi-Fi network providers and other providers of infrastructure to deploy their infrastructure on their premises.

In entertainment venues attendees could find their way to their seats more readily, rather than rely on guides. Indoor navigation could also guide people to the refreshment stall with the shortest lines, or guests could order snacks from their seats, with vendors using indoor guidance to locate hungry customers. This could improve the productivity of waiting staff.

Travel: late arrival at an airport gate can be costly for an airline and stressful for a passenger. Over 30 airports worldwide host more than 20 million passengers per year.[45] Existing services, such as app-based taxi hailing, could become more precise with indoor navigation, and pickups at subterranean shopping-centre parking lots or under hotel canopies could take place more easily and not have to rely on spoken instructions between driver and passenger. Tagging suitcases with location sensors may be more useful with indoor navigation.

For trade fairs or conventions: attendees and exhibitors can find their way to stands or to meeting rooms using an app, rather than relying on (often poor or non-existent) signage.[46] There were over 67 million attendees of trade fairs in Europe alone in 2015.[47]

In the medium term, precision indoor navigation is a facility that consumers and business are likely to take for granted. In the interim, significant research is likely to be required to harness all the many technologies and data sets available which, collectively, should enable indoor localisation. The effort required will be substantial. The rewards should be too.

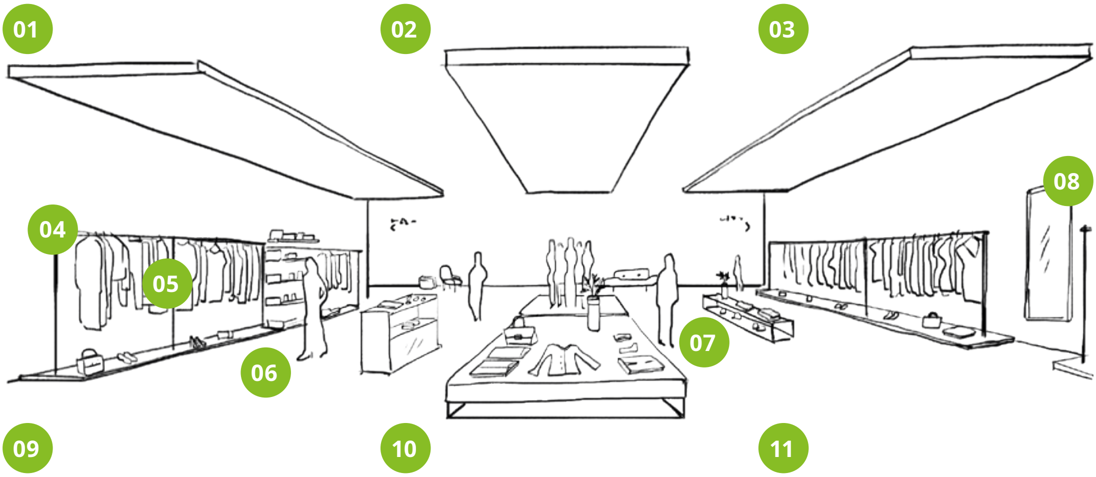
Satellite-based digital navigation, accompanied by the digitisation of street maps, has revolutionised how people and objects are located and guided.

Realising the promise of indoor navigation requires, just as with outdoor navigation, two core components: real-time communication of location, and digital maps.

Case study: Deloitte's connected store proposition

With digital technologies such as indoor navigation entering the physical space, retailers have an opportunity to build a new type of store. Through a 'connected store' environment, retailers could generate insight that will help increase conversion, enrich customer interactions and boost store productivity.

Deloitte has developed a space to help retailers better understand the strategic value of in-store technologies by bringing the experience to life. The Deloitte 'connected store' helps clients think and visualise what digital transformation in the consumer environment can mean for them.



01. Sensors near the shop frontage tell when customers are getting drawn in

02. Connected low-energy lighting gives energy efficiency, collects and transmits data via Visual Light Communications (VLC), low energy Bluetooth and Wi-Fi

03. Connected supply chain allows an on-demand model across production, buying and distribution to be responsive to changing demands and trends

04. Sensors on rails and shelves track stock density and 'browse' behaviour by shoppers

05. Connected labels or tags enable targeted pricing and mobile checkout (as well as security tracking)

06. Shopper's use of the store app on smartphones makes paying easier and gives new potential to wish lists and loyalty schemes

07. Staff smartphones connect them with management teams, give them real-time information about shoppers, stock and new offers, and help them prioritise tasks and increase productivity

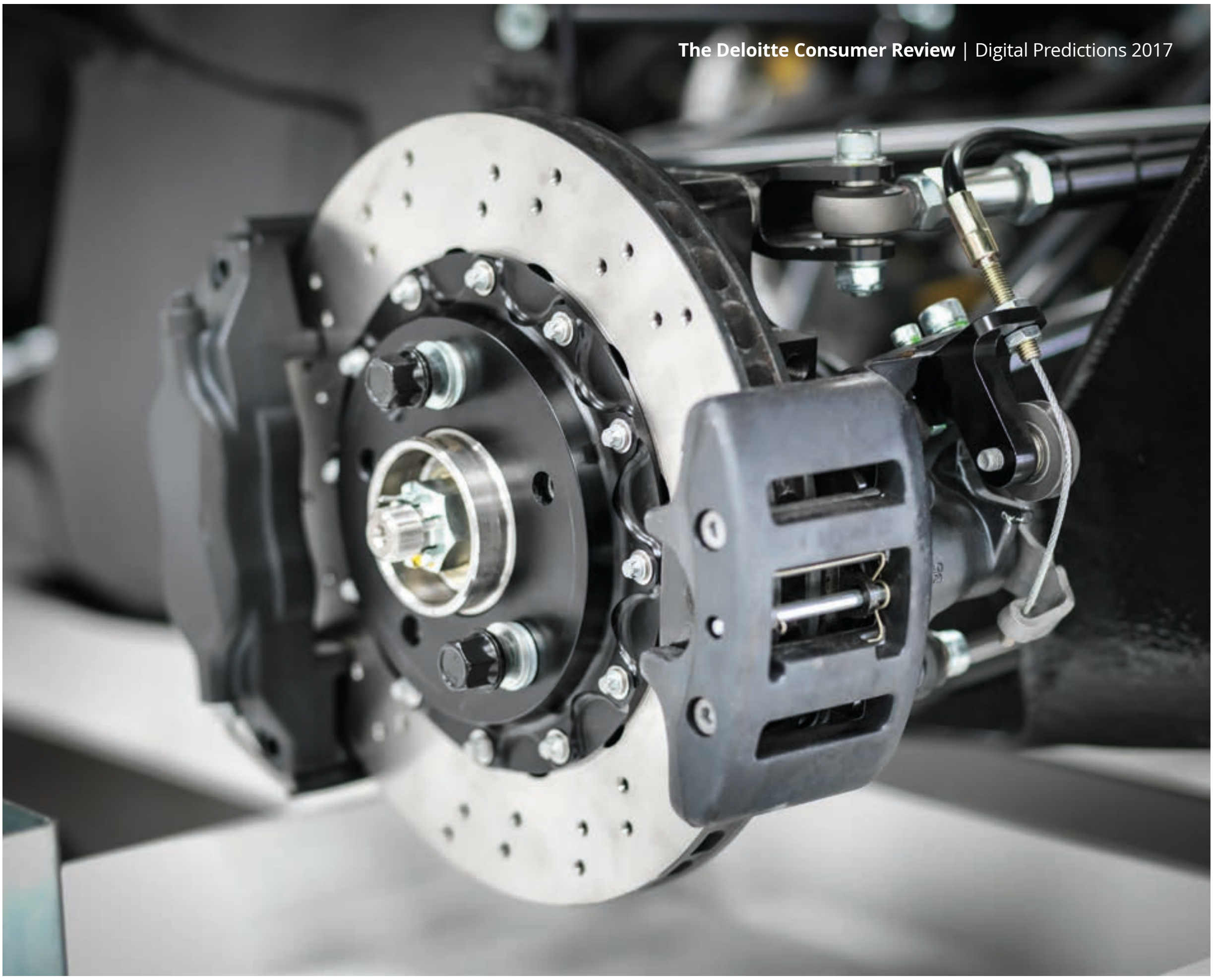
08. Smart mirrors, screens and connected signage give shoppers personalised information

09. Floor sensors measure footfall throughout the store and tell staff when areas are particularly busy

10. Camera systems not only provide loss prevention security, but also track shoppers' faces and physical journeys through the store

11. Connected baskets and trolleys help let staff know dwell time around the store for those shoppers not using smartphones

Source: Deloitte Digital



Automatic braking system: the road leading to self-driving

Deloitte Global predicts that by 2022, annual US motor vehicle fatalities could fall by 6,000, a 16 per cent decline on the likely death toll in 2017.[48] The greatest factor is likely to be automatic emergency braking (AEB) technologies, a safety feature that takes into account the traffic conditions and automatically brakes the car if the driver fails to respond. Already low-speed AEB technology has led to a 38 per cent reduction in real world rear-end crashes.[49]

Quantifying the impact of a motor accident

The number of people who will die in motor vehicle collisions in 2017 worldwide is forecast at over 1.25 million, making it the ninth leading cause of death worldwide, and the leading killer for those 15-29 years of age.[50, 51]

How AEB makes cars safer

The average driver takes a couple of seconds to see an obstruction, recognise it as a problem, and react to it by hitting the brakes.[52] If travelling at 70 miles per hour (MPH), this would mean that the vehicle could still be going at full speed for two seconds and travel a further 63 meters before the brakes are applied.

In contrast, a vehicle with AEB technology could react in a millisecond or two. This, in many cases, might prevent a collision entirely; in other cases it will reduce the severity. For example, the two seconds gained could allow the vehicle to decelerate to around 30 MPH, a 56 per cent reduction in speed. A collision at this speed would still be serious and would be likely to cause major damage to the vehicle, but deaths would be significantly less likely.

As AEB technology becomes more widely adopted, there could be a significant increase in lives saved if one car has the technology – and an even greater increase if both cars have it in a collision involving two cars.

Case study: HexScore and HexMotor

HexScore is a Deloitte cognitive insight platform that has the potential to disrupt many industries. Its current focus is in quantifying risks across dynamic physical environments, including roads, buildings, marine and aviation.

It generates better intelligence by integrating technologies such as machine learning, cloud computing and distributed search engines, and mining numerous dynamic data sources (e.g. IoT sensor data, unstructured data, social media, roadside cameras, satellite and drone imagery and open data).

HexScore technology has enabled disruptive new products such as HexMotor, a mobile-based motor insurance product with an option of pay-per-mile which is based on where, when and how much someone drives. At purchase, customers have an option to enable a pay-per-mile tariff. Customers who choose the option have their trips tracked through their smartphone and may obtain a discount if their usage is low.

As AEB technology becomes more widely adopted, there could be a significant increase in lives saved if one car has the technology – and an even greater increase if both cars have it in a collision involving two cars.

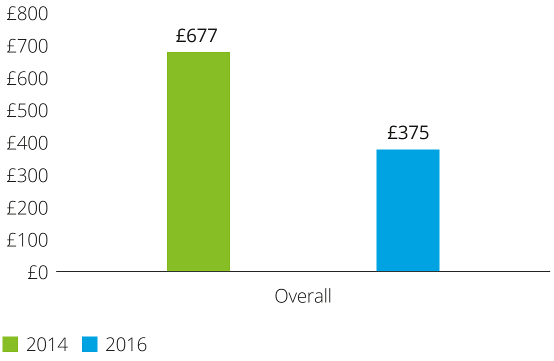
The survey says... safety, safety, safety

According to Deloitte's recent Consumer Auto Survey, AEB is the top technology for over 20,000 respondents across 17 countries.[53] When asked to rank over 30 different advanced automotive technologies, consumers' top choice was a technology that "recognises presence of objects on road and avoids collision".

This was the case by generation and by gender. In most demographic groups, AEB also ranked higher than self-driving technology – even though it is considered part of a suite of technologies that will eventually be part of autonomous vehicles.

Affordability also favours AEB: the amount respondents in the Deloitte survey were willing to pay for future automotive technologies is more or less in line with the likely cost of AEB in the next year or two (see Figure 4).

Figure 4. Overall expected price which consumers are willing to pay for future automotive technologies, 2014 and 2016[54]



Source: Deloitte's Global Automotive Consumer survey, January 2017

The cost per vehicle of providing AEB is falling. It is currently estimated to be about $460, depending on the mix of attendant equipment.[55] In 2017, cameras and radars will be fairly low-cost technologies, but laser-imaging is still likely to cost tens of thousands of dollars.[56] In the near term, affordable AEB is most likely to come through the use of cameras and radars but by 2022 it is expected that Light Detection and Ranging (LIDAR) technology will be much more affordable.[57]

Case study: The connected car[58]

Financial services firm Visa is turning the car into a mobile payments solution – in the same way people use their smartphone or a traditional credit card. The company's concept app will let drivers pay for fuel, parking and drive-through food without leaving their car.

The app, which can be accessed via the car's dashboard, will tell a driver when they are running low on petrol and navigate them to the nearest filling station. Once parked next to a pump, the app can calculate the cost of filling up and a person can pay for the petrol and even convenience store items using it. The app can also let people pay the exact price for a parking spot.

By 2020, there will be an estimated quarter of a billion connected vehicles on the road.[59] People will therefore be carrying out an increasing number of tasks using their car's dashboard.

Next: driverless cars

Autonomous driving is expected to be commercially available first in areas where vehicle owners can recoup the higher costs, such as road freight and ride-hailing. AEB has already been standard in commercial vehicles in Europe since 2013 and various fleet platooning technologies are likely to hit the market in the next two to five years.

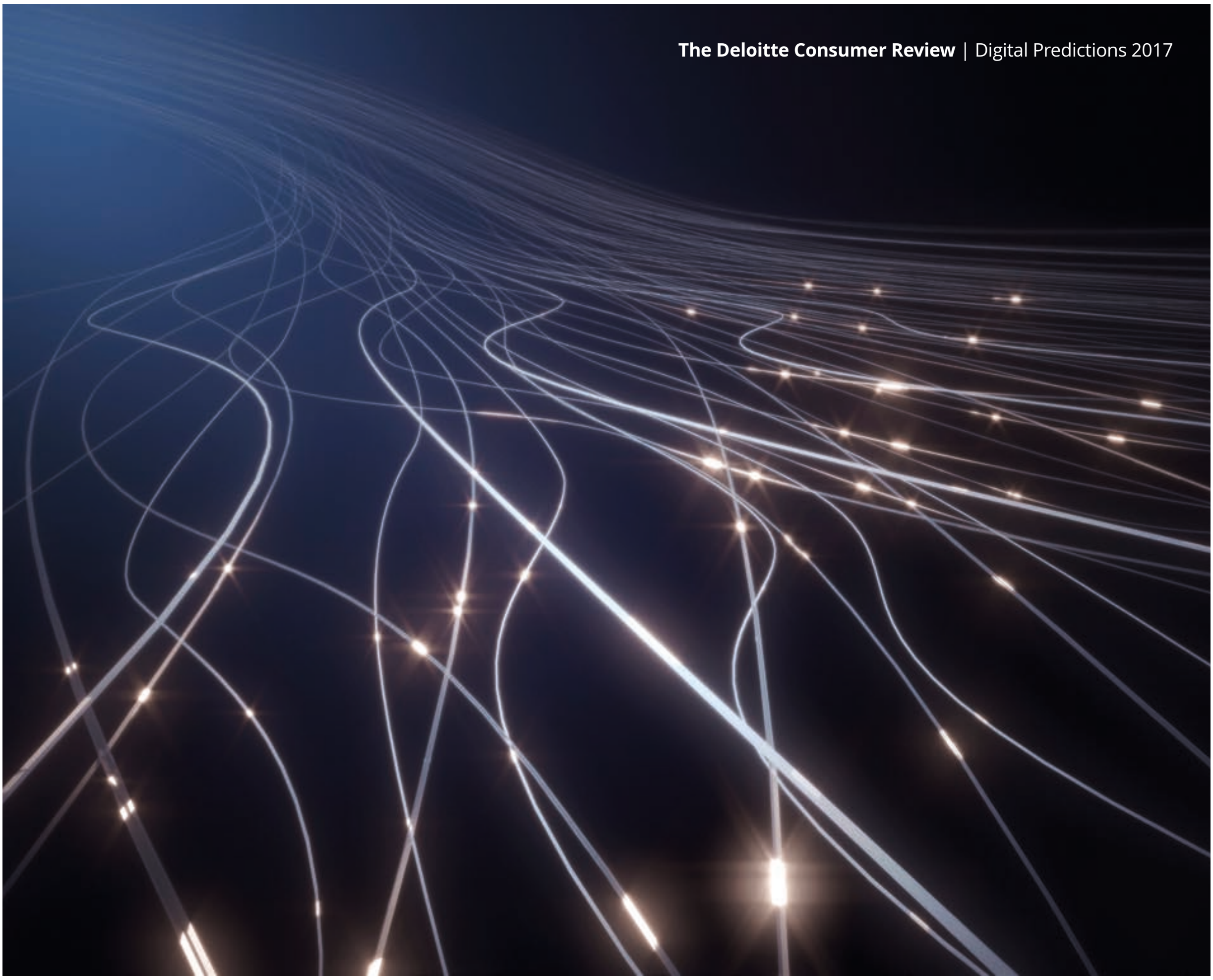
The UK will launch a truck platooning challenge later in 2017 on the M6 in Cumbria. Truck Platooning comprises a number of trucks, equipped with state-of-the-art driving support systems, which closely follow one another. The trucks, driven by smart technology and mutually communicating, form a platoon. As following trucks brake immediately, with zero reaction time, platooning can improve traffic safety. Platooning is also a cost-saver as the trucks drive close together at a constant speed. This means fuel consumption and CO^2 emissions are reduced. Finally, platooning improves traffic flow by reducing tailbacks and the short distance between vehicles means less space is taken up on the road.

Consumers will benefit most from the improved safety that driverless cars offer: fewer humans driving should mean fewer accidents. They will also reap the benefits of cheaper transportation across all sectors: the cost per mile is expected to drop once humans (and their wages) are removed from haulage, taxis, mass transit and more. This should make mobility accessible to more segments of the population, and easier and cheaper for the elderly and the disabled and those on low incomes to get around. The extra time freed up from not having to drive will make commuting both more productive and more enjoyable.

Case study: Driverless commercial delivery[60]

Otto, a self-driving start-up acquired by Uber, announced that its self-driving semi truck, in conjunction with Anheuser-Busch and Volvo, delivered a shipment of Budweiser beer from Fort Collins, Colorado, to Colorado Springs. The Volvo truck relied on a series of radar and sensors, plus cameras, to complete the drive. The driver, who was present for safety, monitored the truck on the road. It should be added that the whole trip was not done autonomously. Otto's system is meant to reduce the strain of highway driving. When it comes to tight, urban driving, the driver is still needed.

Already low-speed AEB technology has led to a 38 per cent reduction in real world rear-end crashes.



5G: the promise of a big bang in connectivity

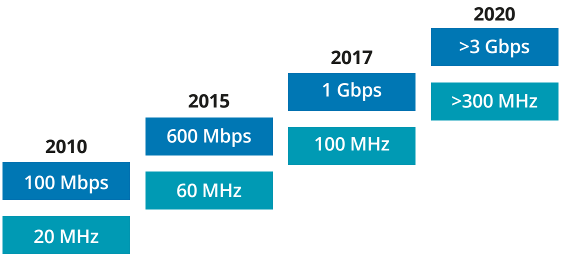
Deloitte predicts that significant tangible steps towards the launch of 5G, the fifth generation of mobile networks, will take place in 2017. Enhanced 4G networks, namely LTE-Advanced and LTE Advanced Pro, which incorporate many of the core 5G network components, will be commercially available. By end-2017, over 200 carriers are likely to be offering LTE-A across some of their network, and over 20 should have LTE-A Pro networks.[61]

With 5G technology, challenges such as smart transportation, autonomous driving, automated traffic control systems, smart grid, IoT and virtual reality take on a whole new meaning. In the future, 5G will guarantee a significant increase in speed and ultra-short response times. Additional benefits will include greatly reduced energy consumption to operate networks and end devices – promising a completely new ecosystem for business models.

Moreover 5G could power the rise of further new technology phenomena like smart cities, smart device adoption, telemedicine, smart homes, in-car infotainment systems, IoT based insurance, virtual reality, automation and even wearables. Autonomous cars would consume 4,000 gigabytes of data per car per day; such levels and quality could only be provided by 5G.

> With 5G technology, challenges such as smart transportation, autonomous driving, automated traffic control systems, smart grid, IoT and virtual reality take on a whole new meaning.

Figure 5. LTE-Advanced Pro data rate and bandwidth[63]



Source: Nokia Networks

Gigabit speeds over mobile networks

By end-2017, Deloitte expects tens and possibly hundreds of millions of LTE-A users to be able to access maximum speeds in the hundreds of Mbit/s (megabit per second), although in some everyday ('real world') environments, the speed attained might be in the tens of Mbit/s – still fast, and equivalent to speeds attainable over many fixed broadband connections.[62]

By the time wider 5G launches around 2020, a significant proportion of users should have become accustomed to obtaining and expecting connectivity speeds of over 100 Mbit/s, and in some cases significantly higher (see Figure 5).

Case study: Swisscom and Ericsson launch '5G for Switzerland' programme

Swisscom and Ericsson are getting set for the new mobile generation with their '5G for Switzerland' programme. Applications are being devised and tested with industrial partners in various sectors, such as smart transportation and virtual reality. The research results will support the definition of international standards for 5G, with completion planned for 2019.

Swisscom and Ericsson will work with industry partners to understand how 5G can innovate their business and develop industrial applications to implement and trial. The results will be incorporated into the definition of international standards for 5G, with completion planned for 2019.

'5G for Switzerland' is part of Ericsson's European '5G for Europe' programme designed to strengthen the competitiveness of Switzerland and Europe. Swisscom aims to extend its network with 5G by 2020.[64]

Bottom line

5G is likely to have a big-bang impact. Its long fuse, which incorporates interim milestones in the forms of LTE-A and LTE-A Pro, has already been lit. Connectivity is a core enabler of the modern economy; 4G is estimated to have accounted for up to $150 billion in economic growth and up to 771,000 jobs in the US alone.[65]

Consumers dominate bandwidth consumption and will be one of the main beneficiaries of 5G. Connectivity has often been a barrier to consumers exploiting fully the capabilities of their devices. For example, the Internet-of-Things has yet to deliver on its promises and 5G will help drive adoption. From wearable devices to connectivity within the home consumers will see devices that currently rely on Wi-Fi or Bluetooth being offered as directly connected services that require no user configuration or setup.

Mobile first becomes a reality

Faster connectivity will allow consumers and brands to interact more and more on a real-time basis and while on the move. Businesses will increasingly differentiate on an engaging, high-quality mobile user experience as part of a seamless omni-channel experience. As connectivity speeds increase, some industries will exploit the opportunity to move to an entirely mobile platform. In the travel sector consumers increasingly want to research and book their next stay or trip while on the move. This need also applies to part of the retail sector, where consumers want to see stock in real time, compare prices, or navigate to the product whilst in store.

Increasingly demanding consumers will expect richer content and more engaging user experiences from businesses with the use of video and 3D content expected to grow exponentially.

Augmented or Virtual Reality (AR/VR) on the go will become more likely with 5G. This could revolutionise marketing. Consumers may be offered immersive marketing experiences – virtually visiting branded events like fashion shows, or virtually touring plants like whiskey distilleries as brands try to build stronger consumer relations through AR/VR technologies.

Lower latency

LTE-A Pro additionally offers vastly lower latency (the time taken for a data packet to travel from one point in a network to another). LTE-A Pro has 600 microsecond latency compared to eight milliseconds (8,000 microseconds) for standard LTE.[66]

Lower latency enables more responsive applications but more critically makes machine control, such as of fast-moving machines, far more viable. This will be of particular value to the automation of tasks in areas such as distribution and delivery.

Mobile applications will continue to evolve

Enterprises should start experimenting with new products and services based on higher speeds, greater capacity and a lower cost per Gigabyte.

Companies should also consider how faster, lower-cost downloads, allied to larger capacity smartphones, might change usage habits.

For example, 4G's greater speeds relative to 3G unlocked latent demand for streaming music into cars and for watching video on public transport.

App downloads that complete in seconds rather than minutes may encourage more people to use apps rather than mobile-optimised websites.
For retailers, this would enable a higher functionality user experience, including the ability to offer indoor navigation or one-touch check-outs using fingerprint readers. However, most users have only around 25-30 apps on their phones and use only a handful on a daily basis. Higher speeds from 5G may not alter that "limited shelf space" attitude.[67]

A major new capability unlocked by iterations of 4G and 5G will be in the enterprise IoT space, and much experimentation will be required to identify the optimal applications.

From wired to wireless connectivity

5G opens the door for truly wireless connectivity everywhere. Operators may also want to evaluate whether some consumers might consider LTE-A Pro (and in a few years, 5G) as alternatives to fixed broadband connections. Fixed networks are getting steadily faster but mobile networks are keeping pace. Using 5G could be significantly cheaper than installing fibre.[68] In some markets LTE speeds are now competitive with fixed line networks accessed via Wi-Fi.

Consumers dominate bandwidth consumption and will be one of the main beneficiaries of 5G. Connectivity has often been a barrier to consumers exploiting fully the capabilities of their devices.

Increase in the severity of DDoS attacks

Deloitte predicts that in 2017 Distributed Denial-of-Service (DDoS) attacks, a form of cyberattack, will become larger in scale, harder to mitigate (increasing the severity of impact), and more frequent. Deloitte expects there will be on average a Tbit/s (terabit per second) attack per month, over 10 million attacks in total, and an average attack size of between 1.25 and 1.5 Gbit/s (gigabit per second) of junk data being sent.[69, 70, 71] An unmitigated Gbit/s attack (one whose impact was not contained), would be sufficient to take many organisations offline.[72, 73]

The largest attacks in 2013-2015 were respectively 300, 400 and 500 Gbit/s; 2016 witnessed the first two Tbit/s attacks. The anticipated escalation in the DDoS threat is primarily due to three concurrent trends:

- the growing installed base of insecure IoT devices (such as connected cameras and digital video recorders) that are usually easier to incorporate into botnets than PCs, smartphones and tablets[75]
- the online availability of malware methodologies, such as Mirai, which allow relatively unskilled attackers to corral insecure IoT devices and use them to launch attacks
- the availability of ever higher bandwidth speeds which means that each compromised device in a botnet can now send a lot more junk data.

Content Distribution Networks (CDNs) and local mitigations may not be able to scale up readily to mitigate the impact of concurrent large-scale attacks, requiring a new approach to DDoS attacks.[76]

How a DDoS attack works

A DDoS attack is aimed at rendering a website or connected device (for example, a server) unusable, meaning that an e-commerce site may not be accessible by shoppers, a government site may not be able to process tax returns or a news site may not be able to share news.

The most common type of DDoS attack congests access to a website or connected device. A DDoS attack is equivalent to hundreds of thousands of fake customers converging on a traditional shop at the same time. The shop quickly becomes overwhelmed. The genuine customers cannot get in and the shop is unable to trade as it cannot serve them.

How a DDoS attack works continued.

A botnet is a large quantity (currently hundreds of thousands) of connected devices that have been infected with malicious code and which can be instructed to act disruptively by a third party. Botnets can be used to effect a flood attack, currently the most prevalent form of attack.

A second approach is an amplification attack, which is based on injecting malicious code into a server, and getting it to create multiple fake IP addresses (also known as 'spoofing').This sends a large volume of commands to a website, causing it to become overwhelmed.[77] As each compromised machine can spoof thousands of fake IP addresses, amplification attacks can cause massive disruption with a relatively small quantity (thousands) of infected servers.

The standard mechanism for mitigating a DDoS attack is to divert traffic to a third party specialised in filtering out malign requests to a website – the equivalent of separating the real customers from the fake ones. Each third party specialised in mitigating an attack has a large, but finite, capacity for containing it, and each of these providers is typically mitigating multiple attacks concurrently on behalf of its clients. The cumulative volume of attacks against clients might at times be greater than the third party's capacity to deal with the attacks, resulting in service disruption for some clients.

Insecure IoT devices

The first trend contributing to the impact of DDoS attacks is the growth in the base of insecure connected IoT devices (that is, vulnerable to being taken over by malign third parties), from video cameras to digital video recorders and from routers to appliances.

Compromising a connected device remotely, such as an IoT device, often requires knowledge of its user ID and password. This knowledge enables the device to be taken over, and to be used potentially for malign purposes. The majority of users are familiar with the need to change user ID and passwords before using a device for the first time, and at regular intervals thereafter. But approximately half a million of the billions of IoT devices worldwide – a small proportion of the total, but a relatively large absolute number – reportedly have hard-coded user IDs and passwords. They cannot be changed, even if the user wants to.[78]

The greater vulnerability of insecure IoT devices relative to generally better protected PCs, tablets and smartphones is likely to encourage hackers to focus on the former when creating botnets and launching DDoS attacks.

In October 2016 a huge attack on global internet access blocked some of the world's most popular websites, such as Twitter, PayPal and Spotify, and is believed to have been unleashed by hackers using common devices like webcams and digital recorders. Users complained they could not reach dozens of internet destinations, including Mashable, CNN, the New York Times, the Wall Street Journal, Yelp and some businesses hosted by Amazon. The attacks were coming from millions of internet addresses, making it one of the largest attacks ever seen.[79]

Bottom line

While DDoS attacks threaten the reputation and the profitability of businesses, they also threaten consumers. In many cases a DDoS attack is launched as a lure to hide the real intentions of the hacker – which is to steal corporate intellectual property and financial data, as well as consumer data.

Companies should consider a range of options to mitigate the impacts of DDoS attacks:

- **decentralising:** organisations can design and implement architectures that disperse critical capabilities physically and logically to mitigate DDoS recognising this is a trade off with centralised efficiency

- **oversubscription:** organisations often lease a significantly larger bandwidth capacity than they need in order to allow for commercial growth and for DDoS attack mitigation

- **testing:** should be used to proactively test the effectiveness of DDoS attack detection or mitigation

- **dynamic defence:** by adopting agile defensive techniques, including deceptive approaches that establish a false reality for adversaries it makes it harder to plan DDoS attacks vs static, predictable behaviour

- **fall-backs:** online streaming media companies may need to consider whether to offer an offline mode; for example, by enabling customers to preload content to watch later

- **protecting**: device vendors should be encouraged, or even mandated, to obtain secure certification for their products, and for this to be labelled on the packaging. Changing credentials should be made simple and secure for consumers[80]

- **detecting**: Explore possibilities for more granular traffic filtering – for example, by geography

- **repelling**: telecommunications companies could be asked to filter at the DNS (Domain Name System) level, possibly tracking traffic from other countries (or major Internet Exchange Points) if required.

With the ever growing level of threat, consumers will be looking for reliable ways to protect their personal data. Opportunities exist for intermediaries to step in and offer gateways to store and protect consumers' details. These intermediaries can invest in appropriate levels of security to ensure consumer protection from fraudulent attacks.

Some organisations may have become a little blasé about DDoS attacks. However, these attacks are likely to increase in intensity in 2017 and beyond, and the attackers are likely to become more inventive. Unfortunately it may never be possible to relax about DDoS attacks. The DDoS genie is out of the bottle, and is unlikely to pop back in.

Case study: Behavioural biometrics for enhanced fraud detection[81]

Nuance has partnered with behavioural biometrics firm BioCatch to incorporate BioCatch's behavioural biometrics data within its voice and facial biometrics platform. This added layer of protection will help organisations flag potentially fraudulent activity based on inconsistencies in the way a person interacts with a device or an application. By learning how a person typically uses their keyboard, mouse or mobile device screen, BioCatch builds a unique behavioural user profile that can identify anomalies, generating an alert that an unauthorised person may be accessing the device.

While DDoS attacks threaten the reputation and the profitability of businesses, they also threaten consumers. In many cases a DDoS attack is launched as a lure to hide the real intentions of the hacker – which is to steal corporate intellectual property and financial data, as well as consumer data.

Endnotes

1. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

2. http://blogs.deloitte.co.uk/innovation/2016/11/the-power-of-the-crowd-easy-access-to-affordable-data-anywhere-in-the-world.html

3. http://www.cio.in/opinion/crowdsourcing-force-multiplier-deliver-digital-transformation

4. Global Human Capital Trends 2017, February 2017. See also: https://dupress.deloitte.com/dup-us-en/focus/human-capital-trends.html

5. UK edition, Deloitte member firms' Global Mobile Consumer Survey, May-Jun 2016. See also: http://www.deloitte.co.uk/mobileuk/

6. Deloitte Global analysis based on conversations with industry experts, a variety of publicly available sources and results from the Deloitte's Global Mobile Consumer Survey data across 23 countries (Argentina, Australia, Belgium, Brazil, Canada, China, Finland, France, Germany, India, Ireland, Italy, Japan, Luxembourg, Mexico, Netherlands, Norway, Poland, Russia, South Korea, Sweden, UK, and US). For more details, see Deloitte's Global Mobile Consumer Survey: www.deloitte.com/gmcs

7. This data is from Deloitte's Global Mobile Consumer Survey across in 15 developed countries (Australia, Belgium, Canada, Finland, France, Germany, Ireland, Italy, Japan, Luxembourg, Netherlands, Norway, Sweden, UK, and US). For more details, see Deloitte's Global Mobile Consumer Survey: www.deloitte.com/gmcs

8. Ibid.

9. There are also likely to be fingerprint readers available in laptops, but on a scale far smaller than found in smartphones and tablets, at least in 2017. Other examples will also exist, such as in airports, for national ID programs and for building access

10. Passwords have inherent limitations. Ideally they should get steadily stronger over time, as the digital tools used to crack them become ever more powerful. A stronger password is longer and composed of a blend of numbers, letters and special characters, in a sequence that does not resemble a word. 'Pa$$w0rd' is easier to remember but not ideal. Those blessed with an exceptionally precise memory could create ever longer passwords for a growing range of services. However, for most people, between five and nine characters is the limit. When people are asked to create strong passwords for a rising number of services, and to refresh them every three months, their typical response is to use the same password for multiple accounts

11. A world beyond passwords: Improving security, efficiency, and user experience in digital transformation, Deloitte University Press, Deloitte Development LLC, 25 July 2016: http://dupress.com/articles/moving-beyond-passwords-cybersecurity/

12. Deloitte Global analysis based on conversations with industry experts, a variety of publicly available sources and results from the Deloitte's Global Mobile Consumer Survey data across 23 countries. For more details, see Deloitte's Global Mobile Consumer Survey: www.deloitte.com/gmcs

13. Chapter 1, Fingerprint Sourcebook, International Association for Identification, et al., July 2011: http://www.nij.gov/publications/pages/publication-detail.aspx?ncjnumber=225320

14. For example, see HSBC launches biometric security for mobile banking in the UK, Computer Weekly, 19 February 2016: http://www.computerweekly.com/news/4500273410/HSBC-launches-biometric-security-for-mobile-banking-in-the-UK

15. https://fashionunited.uk/news/retail/mastercard-rolling-out-fingerprint-and-selfie-payment-technology/2016100522032

16. Global biometric market in the retail sector, 2015: http://rynkologia.pl/wp-content/uploads/2016/01/Global-Biometrics-Market-in-the-Retail-Sector-2016-20202.pdf

17. New CSC Research Reveals Where Shoppers and Retailers Stand on Next Generation In-store Technology, September 10, 2015: http://www.csc.com/uk/press_releases/133753-new_csc_research_reveals_where_shoppers_and_retailers_stand_on_next_generation_in_store_technology

18. KLM, Schiphol airport pilot facial recognition-based boarding system, February 7, 2017: http://www.biometricupdate.com/201702/klm-schiphol-airport-pilot-facial-recognition-based-boarding-system

19. Technology and innovation in the hospitality industry, 29 June, 2016: http://www.winhotelsolution.com/en/blog/hotel-technology/technology-innovation-hospitality-industry/

20. http://www.techradar.com/news/internet/web/apple-pay-has-landed-on-the-web-just-in-time-for-macos-sierra-1328679

21. Deloitte Global expects 300 million units of premium smartphones, mainly costing $500 or more, from a range of manufacturers to incorporate hardware that enhances neural network machine learning. This number may be higher if aggregate sales of premium models is higher than expected, or if neural network machine learning capability is introduced into lower cost phones. It may also be the case that some models of smartphone incorporate neural network machine learning capability, but this is not publicly known

22. Smartphone shipments are expected to reach 1.45 billion in 2016 and 1.49 billion in 2017 (a 3.4 per cent year-on-year growth rate). See: 4G Smartphones to Surpass 1 Billion Mark in Shipments for 2016 as Emerging Markets Play Catch Up, According to IDC, IDC, 29 November 2016: http://www.idc.com/getdoc.jsp?containerId=prUS41962716

23. For more information on machine learning in drones, see DJI launches new era of intelligent flying cameras, DJI, 2 March 2016: https://u.dji.com/en/articles/19

24. NVIDIA boosts IQ of self-driving cars with world's first in-car artificial intelligence supercomputer, NVIDIA, 4 January 2016: http://nvidianews.nvidia.com/news/nvidia-boosts-iq-of-self-driving-cars-with-world-s-first-in-car-artificial-intelligence-supercomputer

25. Lenovo and Google partner on new project tango device, Lenovo, 7 January 2016: http://news.lenovo.com/news-releases/lenovo-and-google-partner-on-new-project-tango-device.htm

26. For more information, see Machine learning + wearable medical devices = a healthier future for all, SAS, as accessed on 23 November 2016: http://www.sas.com/en_ca/insights/articles/big-data/machine-learning-wearable-devices-healthier-future.html

27. The internet of things and machine learning, Forbes, 16 March 2016: http://www.forbes.com/sites/moorinsights/2016/03/16/the-internet-of-things-and-machine-learning/#7e6cb06483e3

28. Internet of Things, Deloitte University Press, Deloitte Development LLP, 21 January 2016: https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/internet-of-things-iot-adoption-edge-analytics-wireless-communication-networks.html

29. The iBrain is here and it's already in your phone, An exclusive inside look at how artificial intelligence and machine learning work at Apple, Backchannel, 24 August 2016: https://backchannel.com/an-exclusive-look-at-how-ai-and-machine-learning-work-at-apple-8dbfb131932b#.zcxe6jnoy

30. One example of IoT devices that can be hacked are security cams.

31. https://internetretailing.com.au/the-north-face-experiments-with-artificial-intelligence/

32. The ability to pass through roofs depends on the material used as well as environmental conditions.

33. Wi-Fi Trick Gives Devices Super-Accurate Indoor Location Fixes, MIT Technology Review, 16 October 2015: https://www.technologyreview.com/s/542561/wi-fi-trick-gives-devices-super-accurate-indoor-location-fixes/

34. For more information, see The Global Public Wi-Fi Network Grows to 50 Million Worldwide Wi-Fi Hotspots, iPass, 20 January 2015: https://www.ipass.com/press-releases/the-global-public-wi-fi-network-grows-to-50-million-worldwide-wi-fi-hotspots/

35. Proximity Marketing in Airports and Transportation – The Q3 Proxbook Report 2016, Unacast, 9 November 2016: http://unacast.com/proximity-marketing-airports-transportation-q3-proxbook-report-2016/

36. Bringing the power of GPS indoors, Philips, as accessed on 30 November 2016: http://www.lighting.philips.com/main/systems/themes/led-based-indoor-positioning.html#form_white_paper

37. Ibid.

38. What's The Difference Between Measuring Location By UWB, Wi-Fi, and Bluetooth?, Electronic Design, 6 February 2015: http://electronicdesign.com/communications/what-s-difference-between-measuring-location-uwb-wi-fi-and-bluetooth

39. See Performance Analysis of Magnetic Indoor Local Positioning System, Western Michigan University, June 2015: http://scholarworks.wmich.edu/cgi/viewcontent.cgi?article=1620&context=masters_theses

40. The principal sensors are: accelerometers and gyroscopes and magnetometers

41. Indoor Maps availability, Google, as accessed on 30 November 2016: https://support.google.com/maps/answer/1685827?hl=en&ref_topic=3280760

42. Use indoor maps to view floor plans, Google, as accessed on 30 November 2016: https://support.google.com/maps/answer/2803784?hl=en&visit_id=0-636159492056420879-831623605&rd=1; also see: Google Maps Floor Plan Marker, Google, as accessed on 30 November 2016: https://play.google.com/store/apps/details?id=com.google.android.apps.insight.surveyor

43. See Making of Maps: The cornerstones, Google, 4 September 2014: https://maps.googleblog.com/2014/09/making-of-maps-cornerstones.html

44. http://www.pointrlabs.com/blog/press-release-harrods-launches-new-navigation-tool-for-knightsbridge-store-just-in-time-for-christmas/

45. This data is for 2015, see International Passenger Traffic for past 12 months, Airports Council International, 11 April 2016: http://www.aci.aero/Data-Centre/Monthly-Traffic-Data/International-Passenger-Rankings/12-months

46. For example see The Proxbook Report: The State Of The Proximity Industry, Unacast, as accessed on 28 November 2016: https://unacast.s3.amazonaws.com/Q2_Proxbook_Report_-_Sports_and_Events.pdf

47. Trade Show Statistics 2015 for Europe, Exhibit in Europe, 30 October 2016: http://www.exhibit-in-europe.com/tips/trade-show-statistics-2015/

48. Deloitte Global analysis based on conversations with industry experts, the Deloitte Global estimate that one sixth of cars are expected to have AEB by 2022, and other factors including other safety technologies such as lane keeping, vehicle-to-vehicle communications. Changes in other forms of distracted driving could have large effects on the death rate. Future fuel prices and employment levels also have strong effects on fatalities: historically, as more people drive, and drive further, fatalities also rise

49. Connected and Autonomous Vehicles, SMMT, February 2017

50. See global status report on road safety 2015 (page 9), World Health Organization, 2015: http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/

51. See global status report on road safety 2015 (page 12), World Health Organization, 2015: http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/

52. See Driver Reaction Time, Marc Green PhD, as accessed on 5 December 2016: http://www.visualexpert.com/Resources/reactiontime.html

53. See Deloitte Global's annual Global Automotive Consumer Insights Platform: Future of Automotive Technologies survey, Deloitte Global, January 2017: www.deloitte.com/autoconsumers

54. Ibid.

55. For more information, see Automatic Emergency Braking: A Soon-to-Be Standard on New Vehicles, Bolt Insurance Agency, 1 August 2016: https://www.boltinsurance.com/automatic-emergency-braking-a-soon-to-be-standard-on-new-vehicles/

56. The $75,000 problem for self-driving cars is going away, The Washington Post, 4 December 2015: https://www.washingtonpost.com/news/innovations/wp/2015/12/04/the-75000-problem-for-self-driving-cars-is-going-away/

57. Cheap Lidar: The Key to Making Self-Driving Cars Affordable, IEEE, 22 September 2016: http://spectrum.ieee.org/transportation/advanced-cars/cheap-lidar-the-key-to-making-selfdriving-cars-affordable

58. https://usa.visa.com/visa-everywhere/innovation-centers/dubai/the-inside-edge/technology/connected-car.html

59. Connected Cars Will Form a Major Element of the Internet of Things, January 2015, http://www.gartner.com/newsroom/id/2970017

60. https://www.bloomberg.com/news/articles/2016-10-25/uber-self-driving-truck-packed-with-budweiser-makes-first-delivery-in-colorado

61. As of October 2016, LTE-A had been introduced by 166 operators around the world. As of October 2016, 12 operators had launched LTE-A Pro services. 4G market and technology update, Global Mobile Supplier's Association, 26 October 2016: http://gsacom.com/wp-content/uploads/2016/10/161027-GSA-Evolution_to_LTE_report_October_2016-001.jpeg

62. Fixed broadband speeds vary significantly. The technology used and distance from the exchange are two factors that affect the speed attainable. For each type of technology there are multiple tiers of performance. A speed of about 50 Mbit/s would be consistent with an entry-level cable connection using DOCSIS 3.0 technology, or a Fibre to the Cabinet (FTTC) connection using a copper connection between a street-based cabinet and the home

63. Nokia Networks white paper, LTE-Advanced Pro: Pushing LTE capabilities towards 5G, as accessed on 1 December 2016: http://resources.alcatel-lucent.com/asset/200176

64. https://www.swisscom.ch/en/about/medien/press-releases/2016/06/20160616-MM-5G-for-Switzerland.html

65. The impact of 4G technology on commercial interactions, economic growth, and U.S. competitiveness, Deloitte Development LLC, August 2011: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-impactof-4g-060612.pdf

66. From “Leading the Path Towards 5G with LTE Advanced Pro” (page 19), Qualcomm, 19 January 2016: https://www.qualcomm.com/documents/leading-path-towards-5g-lte-advanced-pro

67. Deloitte’s Global Mobile Consumer Survey, conducted in 15 developed countries. For more details, see Deloitte’s Global Mobile Consumer Survey: www.deloitte.com/gmcs

68. According to Verizon’s CEO, installation costs of home broadband via 5G would be significantly lower than for fibre. The cost of the 5G router would be less than the combined cost of a fibre router and optical network terminal (ONT). Additionally 5G capabilities could be added to existing 4G small cells. See Verizon CEO details ‘wireless fiber’ 5G deployment trials, FierceTelecom, 27 July 2016: http://www.fiercetelecom.com/installer/verizon-ceo-details-wireless-fiber-5g-deployment-trials

69. The average attack size in the first half of 2016 was 968 Mbit/s, and was forecast at 1.15 Gbit/s for all of 2016. For more information, see Arbor Networks releases global DDoS attack data for 1H 2016, Arbor Networks, 19 July 2016: https://www.arbornetworks.com/arbor-networks-releases-global-ddos-attack-data-for-1h-2016

70. For more information, see The zettabyte era—trends and analysis (figure 22), Cisco, 2 June 2016: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

71. The first recorded Tbit/s attack was in September 2016, see Record-breaking DDoS reportedly delivered by 145,000+ hacked cameras, Ars Technica, 29 September 2016: http://arstechnica.co.uk/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

72. Arbor Networks releases global DDoS attack data for 1H 2016, Arbor Networks, 19 July 2016: https://www.arbornetworks.com/arbor-networks-releases-global-ddos-attack-data-for-1h-2016

73. This document refers to attack dimensions in Gbit/s, but there are other metrics, including requests per second. For more nformation, see Say cheese: a snapshot of the massive DDoS attacks coming from IoT cameras, Cloudflare, 11 October 2016: https://blog.cloudflare.com/say-cheese-a-snapshot-of-the-massive-ddos-attacks-coming-from-iot-cameras/

74. The zettabyte era—trends and analysis, Cisco, 2 June 2016: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

75. IoT devices being increasingly used for DDoS attacks, Symantec Corporation, 22 September 2016: http://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks

76. As an example, one of the major mitigation providers has 10 Terabit/s capacity, see Cloudflare, as accessed on 22 November 2016: www.cloudflare.com

77. For more detail on amplification attacks, see Technical details behind a 400Gbps NTP amplification DDoS attack, Cloudflare, 13 February 2014: https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/

78. A scan as of October 2016 found 515,000 vulnerable IoT devices. For more information, see Hacked cameras, DVRs powered today’s massive internet outage, KrebsOnSecurity, 21 October 2016: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

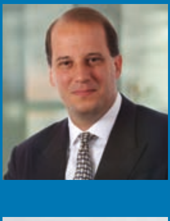
79. https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service

80. See Europe to push new security rules amid IoT mess , KrebsOnSecurity, 8 October 2016: https://krebsonsecurity.com/2016/10/europe-to-push-new-security-rules-amid-iot-mess/; EU pushes IoT security regulations, TechWeek Europe, 10 October 2016: http://www.techweekeurope.co.uk/security/european-commission-push-iot-security-regulations-198826

81. https://www.biometricupdate.com/201702/nuance-adds-behavioral-biometrics-for-enhanced-fraud-detection

Contacts

Leadership team



Nigel Wixcey
UK Industry Leader, Consumer & Industrial Products
+44 (0)20 7303 5007
nigelwixcey@deloitte.co.uk

Phil Neal
Digital Transformation Lead, Consumer & Industrial Products
+44 (0)20 7007 4065
pneal@deloitte.co.uk

Authors

Céline Fenech
UK Research Manager, Consumer & Industrial Products
+44 (0)20 7303 2064
cfenech@deloitte.co.uk

Paul Lee
Partner, Technology, Media & Telecommunications
+44 (0)20 7303 0197
paullee@deloitte.co.uk

Contributors

Justine Bornstein
Research Senior Manager, Industrial Products & Automotive
+44 (0)20 7303 2569
jbornstein@deloitte.co.uk

Deloitte.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000
Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. J11120