WORLD
ECONOMIC
FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

White Paper

Realizing the Internet of Things: A Framework for Collective Action

In collaboration with the Massachusetts Institute of Technology

January 2019

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

This white paper has been published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum, but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Contents

Foreword

Jeff Merritt, Head, Internet of Things, Robotics and Smart Cities, World Economic Forum

Sanjay Sarma, Professor of Mechanical Engineering and Co-Founder, Auto-ID Lab, Massachusetts Institute of Technology, USA

At the World Economic Forum Annual Meeting 2017, global leaders highlighted the development of the internet of things (IoT) as one of the most significant emerging technologies, harbouring the potential for massive societal impact. Recognizing this opportunity, the World Economic Forum, the Auto-ID Lab at the Massachusetts Institute of Technology (MIT) and GS1, the global standards organization, collaborated to help define a path forward while ensuring a shared understanding of the pressing challenges facing the development of IoT.

Over the course of 2017 and 2018, the Forum, the Auto-ID Lab at MIT and GS1 organized calls and workshop meetings to gather input, case studies and insights from experts and key stakeholders. Roundtable events were also held at the Forum's Annual Meeting of the New Champions 2017 and Annual Meeting 2018.

This White Paper presents the findings and outcomes of this work. It includes a framework for analysing the space, the opportunities for impact and the challenges facing the IoT ecosystem. A series of recommendations are also put forward to help government, the private sector and civil society organizations work together to advance the development of IoT in the public interest.

Executive Summary

The ability to sense the environment, and to formulate and execute an action in response, is central to all vertebrates and increasingly so to all things artificial. This is the driving force behind the internet of things (IoT). Homes, businesses, governments and systems that deploy sensors, gather data to inform intelligent decisions and respond to the environment can enable a safer, more sustainable, more comfortable, healthier and more economically viable world for humanity.

IoT fulfils these needs, and the growth expected is staggering. Gartner predicted that IoT spend in 2016 would exceed $2.5 million per minute, and projects 1 million IoT devices to be installed hourly by 2021.[1] HP similarly estimates an 18% compound annual growth rate in machine-to-machine connections, reaching 27 billion by 2024.[2] A chorus of predictions by blue chip companies, such as McKinsey and Cisco, echoes the same message: IoT will see astronomical growth in the next decade.

The rise and expansion of IoT

IoT owes its growing potential in recent years to several parallel developments over the last decade.

Hard-wired industrial automation goes back over 100 years. Over the last 50 years, automation has transformed businesses, and the economic, performance, safety and quality benefits are well understood. Automation needs connectivity, and modern networking principles entered the industrial realm in fits and starts with the likes of the manufacturing application protocol/technical office protocol more than 35 years ago – and later with Modbus, Lonworks, CANbus and ethernet – but adoption in heavy industries such as manufacturing favoured dedicated “hardened” systems due to understandable concerns about performance. These systems, meant to control factories and plants, are referred to as Supervisory Control and Data Acquisition (SCADA). In automotive systems, the CANbus standard has dominated and become the foundation for on-board diagnostics. However, the incredible advances in sensing, networking and data analysis currently occurring in home automation and consumer applications is only slowly affecting the industrial world. But that change will accelerate tremendously in the years ahead.

Many advances recently have been driven by consumer demands for voice and data, combined with innovator demands for ad hoc data networking – such as, say, a flexible sensor and actuator system for watering plants in a greenhouse – and have led to new paradigms in networking, sensing and actuating outside the industrial automation realm. As is often the case, the “lower” expectations for performance in non-critical applications have allowed more innovation and architectural creativity, leading in the end to a dazzling set of systems and components, at lower costs and, in many respects, with better performance. Today, a broad palette of connectivity approaches is available to engineers, including everything from low-power radio-frequency identification (RFID) to 5G, and the alphanumeric soup in between, whether a LPWAN (low-power wide-area network) or 6LowPAN (IPv6 over low-power wireless personal area networks).

While connectivity is a key element of IoT, computation and sensors are two other key legs of the stool. The smartphone combines all three and has driven a two-pronged revolution. On the one hand, smartphones are the magic wand of IoT, turning dumb objects into smart objects by their very presence, by adding handy displays and controls where needed, and by providing computation at a pinch. Uber, for example, converts any old car into a connected vehicle that can be tracked and located by a consumer (and vice versa).

On the other hand, the cellular industry has brought about a stunning commoditization of sensor components – be it cameras or gyroscopes, accelerometers or touch displays. Batteries have become more stable, longer-lasting and cheaper. Unbundled sensor modules are now easier to embed in other devices such as thermostats and smoke alarms. Embedded computation packs more bang for the buck today. Radio chips are now more ubiquitous. And the growth of RFID brings ubiquitous, disposable sensors much closer to reality. This has snowballed now with the growth of other industries, such as autonomous vehicles, robotics, wearables and drones. Suddenly, LiDAR (light detection and ranging) is going solid-state, infrared cameras are becoming affordable and galvanic skin response sensors are becoming commoditized.

While technologies are enabling to IoT, human capital is paramount. The growth of talent that can manipulate the various levels of the computational stack, and the hacker/maker culture further fuelled by the rise of systems such as the Raspberry Pi, have made the innovation in IoT an irresistible force. Few household or industrial products today – be it a home lock or a doorbell, a heating, ventilation and air conditioning system or an elevator – have resisted the inexorable force of IoT-based rethinking. These innovators are now bringing their unconventional ideas back to more mature industries – such as industrial automation and vehicles networking. Tesla, for example, supports CANbus, but really uses in-vehicle ethernet, enabling a more flexible IoT approach.

So, while automation is not new, it is the amorphous, pervasive (and often publicly) connected, ad hoc, distributed, easy to design, easy to deploy, easy to “mashup” and massively commoditized nature of the sensing, computing and actuating enabled by IoT that makes it a new and explosive capability. And it is now impacting the industrial sector where it all started. Whether a new building or a new oil rig, a retrofitted power plant or a retooled manufacturing line, IoT is becoming an inevitable part of the thinking – a *lingua franca* of sorts.

IoT is a new design language

Much has been written about the opportunity created by IoT,[3] but fundamental questions may confuse the issue in the minds of business leaders. Is IoT a technology that can be purchased? Is IoT a business practice? A communications technology? How might one best think about IoT? Until these fundamental doubts are resolved, discussions about IoT will vacillate between arcane questions about standards and technology, such as 6LowPAN versus Wi-Fi, and speculative guesses of the return on investment (ROI) of IoT. This section presents a way to think about IoT.

IoT may be thought of as a new design language. Consider the business of designing buildings before the widespread availability of electric power. Buildings had to be lit with candles and, later, with gas.[4] Running water was difficult to deliver to upper floors without steam pumps and overhead tanks. Elevators and escalators were rare because they needed to be powered by hand or animals. Fire provided heat, and cooling was impractical. The invention and adoption of electricity and the subsequent development of pumps, electric lights, elevators, escalators and modern heating, ventilation and air conditioning systems together heralded a whole new design language for architects. Buildings, and the business of construction, were transformed.

Similarly, IoT is best thought of as a new design language for organizations, which helps them more effectively meet the needs that their customers or constituents want. Consider car rentals: the typical rental complex is usually near an airport and houses hundreds of cars ready for pick up. The reason is simple: keys need to be distributed and collected, and mileages and fuel levels must be recorded. With IoT, however, keys can be transferred electronically, and mileage and fuel levels can be accessed remotely. Suddenly, cars can be positioned where customers want them: at the parking lot across the street from their apartment, or in office parking lots. This was the new rental paradigm invented by Robin Chase and Antje Danielson when they founded Zipcar,[5] which was quite possibly the first consumer-facing IoT company. What Chase and Danielson did was rethink the car rental business by using the affordances of IoT's new design language.

The new vocabulary

So, what are the elements of this new language? The four key components of such language are presented next. Clearly, connectivity is one. Connectivity, implicit in the "I" in IoT, enables remote device operation and data collection. Whether a remotely operable lock,[6] so a homeowner can let a visitor into her online rental property, or a thermostat that can be monitored from a phone or controlled by a cloud platform to activate when a family member approaches the vicinity of home,[7] or a compressor driving the pneumatics in a construction site that can report the vibration it is sensing in the motor, connectivity is a powerful capability. However, it is only one of several capabilities enabling the IoT.

Computation, or intelligence, is a second capability. Intelligent systems afford a level of customization for the user's experience impossible with connectivity alone. Smart, connected thermostats can sense usage patterns and suggest alternate heating and cooling schedules that reduce energy consumption. Modern smartphones and voice-controllable devices can implement new apps and skills to make the user's experience more satisfying. Analytics of the compressor can detect an issue and prevent a breakdown – transforming maintenance from a scheduled or preventative paradigm to a predictive one. A general-purpose computation platform that can morph and enlist local or cloud-based resources to provide intelligent, adaptive functionality can strengthen the relationship between the customer and the vendor, and also provide insights previously unavailable in conventional static products.

The third affordance of IoT's design language is recruitment. A single device may not have the functionality to create an experience, but it may recruit other devices. Laptops can be unlocked by a user when she is nearby wearing a smart watch.[8] A coffee machine may activate when a user has woken because her wearable fitness device signalled it.[9] The smart thermostat in the earlier example recruits a phone's GPS to figure out when to turn up the heat and may also recruit a comfort sensor on the user's body to fine-tune its setting.[10] The compressor in the previous example can recruit a local sensor to also record ambient temperature and help diagnose the overheating problem.

The fourth and most seamless design component within IoT is immersion, where connectivity, intelligence and recruitment occur automatically and fluidly. As a user walks from her home office to her deck on a balmy Friday evening, a connected, immersive music system follows her from room to room all the way to the deck;[11] lights dim and the music changes as her wearable detects a lowering heart rate.[12] Her car sees a calendar event and pulls out to the driveway in anticipation of an upcoming dinner.[13] Returning to the compressor example, a maintenance engineer entering a jobsite is guided to the compressor unit. A message to her mobile phone has informed her of the impending issue, and replacement parts have been ordered for her and are waiting for her to conduct a quick maintenance operation before the next shift begins. As she leaves, she informs the job foreman of the higher than rated temperature of the jobsite and upsells him on the appropriate compressor unit that has better cooling.

Rethinking Business and Government in an Era of IoT

As highlighted in the previous section, IoT forces us to question the traditional concepts of products, services user-interfaces and capabilities. Does a coffee machine need its own app store?[14] Should a mattress detect sleep patterns?[15] These ideas may seem outlandish but they rethink the customer experience using the new design language of IoT.

The rethinking may also involve a reimagination of the business model of an industry. Uber and AirBnB are examples of two-sided markets that have disrupted the business models of the transportation and hotel industries, respectively. Amazon Prime unbundles the shopping list of the consumer and enables a form of streaming supply that is exploited by the Amazon Conversational Commerce family including Dash, Echo and Dot. Ring, recently acquired by Amazon, is an IoT doorbell that works off a subscription service.[16] It is hard to imagine a subscription for a doorbell – but the Ring product uses a connected camera and image-processing to offer greater value to the customer.

Governments and citizens, in many ways, have the most to gain from IoT in pursuit of comfort, convenience, safety, security and sustainability. Whether it is water quality or detecting leaky water pipes, traffic safety or emissions reduction, plant performance or equipment maintenance, sensors and intelligent actuation can have a significant impact. However, where to start and how to fund these activities remain critical, even paralysing questions. In the end, these systems need to interoperate. The trade-offs between starting too early and building disconnected islands, or starting late and foregoing benefits are difficult to negotiate. Yet progress must be made, especially in the face of pressing goals – whether the United Nations Sustainable Development Goals (SDGs) or economic imperatives.

An era of convergence

The vocabulary of this new design language is more expansive than IoT alone, though it is often the glue that holds things together. Is a self-driving car an example of IoT? Is it a robot? Does it involve the cloud? Is it an example of machine learning? Does it rely on computer vision? Or is it all of the above? Clearly, the answer is the latter – this is an era of convergence, one in which the new language of business is becoming more and more powerful. The ubiquity of the smartphone makes IoT even more real and imminent as an opportunity – and a threat – for businesses. Even blockchain and related technologies are a part of this new language. Supply chain tracking using transponders, recorded in distributed ledgers, has been suggested as a way to assure provenance and product integrity.[17] [18]

The convergence has a snowball effect. New ways to collect, process and interpret the flow of data are emerging – whether they be voice or video, temperature readings or traffic sensors. Computation is evolving by blending cloud computing with ground-level edge computing – also called fog computing.[19] Each of these new concepts add a new noun, verb or adjective to the growing vocabulary of the new design language that the people designing products, services and, more importantly, experiences can leverage.

The risks of IoT

For all its opportunities, IoT has challenges. Consider connectivity: there are myriad standards ranging from ZigBee to Z-Wave, from Wi-Fi to Bluetooth, from a number of LPWAN standards (LoRA, SigFox, NB-IOT) to RFID. The inevitable rise of 5G will become a driving force in IoT and the Fourth Industrial Revolution. Fragmented standards can be challenging, though the dream of total technical convergence may be misplaced. It can be argued that different standards are here to stay and serve different goals. LoRA addresses long-range, ultra-low power and low bandwidth communications whereas Wi-Fi addresses low-range, higher-power and high-bandwidth communications. Standards at other areas of the IoT must be carefully assessed in terms of cost and performance trade-offs across many dimensions. Computation, intelligence, scale and accessibility create new cybersecurity challenges. The growth of software on a cyberphysical system creates terrible new possibilities like those exploited by Stuxnet[20] and the Mirai Botnet.[21] In cyberphysical systems, the failure modes are more widespread and coupled with common tasks and jobs – does a technician replacing an instrumented valve in a power plant also need to be a cybersecurity expert? Protocols and training are needed to ensure security. Trojan-horse hardware and software pose another challenge; the consequences are greater when the physical world is involved.[22]

This is the brave new world that awaits businesses in the 21st century – one of great opportunity but also threats, both competitive and malicious. In the sections that follow, the key issues faced by business and government in an era of IoT are laid out and a framework is offered for how the global community can take on these challenges for the greater good of society.

Five Pillars Shaping the Development of IoT

The many uncertainties in the future development of IoT may be organized into five categories, or pillars, summarized below.

1. Architecture and standards

Scalable, future-proof and cost-effective architectural choices are essential to IoT's long-term success.[23] Architectural choices today may lock companies into long-term trajectories that can make or break IoT businesses. Reference architectures provide precompetitive frameworks and serve to enable two purposes: a) enable the development of standards with dependable interface and touchpoints, which in turn are necessary for a healthy vendor ecosystem; and b) enable best practices that ensure both widespread adoption and a healthy ecosystem that is relatively free of performance or safety issues. Architecture and standards are important not just for software and communication – data require careful thought as well.

2. Security and privacy

Security and privacy must be designed in from the start. According to a Cisco/Jasper study, a mere 9% of consumers trust their data to be secure when stored online, with only 14% agreeing that companies provide appropriate transparency and clarity in explaining their data usage and sharing policies.[24] Despite the largely negative sentiment, 42% of consumers are unwilling to disconnect their lives from the internet, in part due to the pervasive integration of the technology into various beneficial services.[25] Clearly, consumers are uneasy with their IoT presence and they perceive increasing security and improving transparency as must-haves. For all its benefits, IoT increases the attack surface of systems and connects two hitherto unrelated concerns: cybersecurity and safety.

3. Shared value creation

The anticipated benefits of new technologies in the early days are often rather bleak.[26] In a Dell report, 48% and 27% of survey respondents list budgetary constraints and unclear financial benefits as barriers to IoT investment, respectively.[27] Investment in IoT will therefore require leadership and vision. For cash-strapped cities and governments, though IoT investments can lead to significant upsides in operational expenses and consumers benefits, the initial investments can be daunting. Public infrastructure may therefore lag in adoption. Value created must also be shared – consumers must see the benefits of a smart meter installed by a utility system rather than feeling as if they are the victims of pricing games.[28] Buy-in across the value chain is necessary to ensure that IoT is seen as a tide that lifts all boats rather than a technology for changing the dynamics between players.

4. Organizational development

IoT is not IT. Using and benefiting from IoT often require a fundamental rethinking of the business, and "speaking the new design language". GE Aerospace famously claimed to be in the business of thrust, not engines. This was predicated in part on the idea of instrumenting engines and monitoring them remotely – an early example of IoT. Such rethinking requires three components: executive leadership, a realignment of incentives across the organization and, perhaps most importantly, a massive upskilling of the organization to learn the new design language.

5. Ecosystem governance

New technologies often create new ecosystems with little governance, either self or external. This cycle tragically repeats itself and usually involves competing technologies, competing vendors, varying public opinion and national and, increasingly, international regulators. Simply put, IoT needs a governing group. A number of questions in the IoT space, including standards, privacy, security, architectures, business cases, etc. – as discussed previously – urgently require collective attention in the form of the development of industry best-practices and self-governance.

Key Challenges and Opportunities

The continuously evolving ecosystem of IoT presents unique and impending challenges that must be addressed not in an ad hoc and piecemeal manner, but by considering the bigger picture. With this in mind, issues related to the five pillars more holistically are examined below.

IoT challenges are society-wide and enterprise-wide. As society grapples with a range of issues – such as sustainability, security and demographic shifts – the ability to sense, communicate, infer and act become necessary and indispensable in building a smarter, more efficient and more comfortable world. The growing acceptance of technology, which is now becoming a hunger for dazzling new functionality, is fuelling new categories of companies with novel offerings with creative revenue models – ones that the existing business and technical lexicons can barely describe. With the rise of payment technologies, such as cryptocurrencies,[29] and the newly minted IoTa,[30] even payment *methods* are reaching far into uncharted territory. However, there are issues with growing such a pervasive technology so broadly and in as decentralized a way. Challenges facing the IoT ecosystem include implementation, interaction and intrinsics. Some challenges stem from technical issues, others policy issues or organizational dynamics, and still others might be governance-related, all impeding the realization of the greatest benefits or the prevention of downside.[31] [32] [33] A broad viewing angle is necessary to ensure an optimal outcome for society at large.

Architecture and standards

Successful architectures are not always obvious. For example, alternating current, or AC, which made the modern electric grid possible, was a counter-intuitive idea pioneered by Tesla in the face of ferocious competition from direct current (DC) and its formidable backer, Edison. Packet-switched networks, cellular telephony and the World Wide Web are other examples of architectural breakthroughs.

IoT is in pressing need of a breakthrough reference architecture. Several questions are unanswered. Should the communication be peer-to-peer? Should the computation be local? Others pertain to where the computation will occur: at the device, at the edge or in the cloud?

Two key patterns are emerging. The first is the concept that was initiated contemporaneously as Cloud Things,[34] Digital Twins[35] or digital mirroring. The basic idea is that IoT objects in the real world will be mirrored in the cloud with virtual equivalents. In some ways the concept predates even the two technical references above – the iTunes account attached to an iPod being one of the earlier commercial examples. However, the extent of the mirroring, combined with the additional functionality in the cloud and the ability to control, drive and protect the IoT object through its guardian in the cloud, is the area where a great deal of progress is occurring.[36] Furthermore, the communication itself can occur between the cloud instances rather than between the actual IoT devices unless the latency cannot be tolerated (which, in a surprisingly large proportion of applications, it can). This enables a new form of security in which the digital twin, with its vastly superior resources in the cloud, can enable a new form of security that is referred to as the Cognitive Firewall. The Cognitive Firewall is a self-learning system capable of evaluating commands for safety in context and only allowing those safe commands to pass from the Cloud to the end device for execution.[37]

The second pattern is what is variously captured by so-called edge computing and fog computing. The basic idea is that some computation can and needs to occur locally to ensure responsiveness and to save bandwidth when that is important. On the other hand, some heavier-weight computation needs to occur in the cloud. A simple example of this form of distribution of computation occurs in voice assistants such as Alexa, Siri, Google and Cortana. The detection of the wake word, such as “Hey Google” or “Alexa”, occurs at the edge with an always-on signal processing system but the actual heavy lifting of understanding and routing the query string, such as “read me the news” occurs in the cloud.

Evolving the ideal architecture requires iteration and refinement. A test bed is extremely effective, and often a necessary precondition, for evolving good architectures. ARPANET is a prime example of a government-initiated test bed. Successful architectures become references – so called reference architectures – that others can adopt with confidence of success. In IoT, the Industrial Internet Consortium (IIC) has led a series of activities around test bed creation with use cases and business needs.[38]

Architectures and standards are closely interrelated. The architecture defines the touchpoints and the interfaces where standards may be defined. In the World Wide Web, the hyperlinking architecture drove the two new and key standards: HTTP and HTML. In the IoT world, Wi-Fi, Bluetooth, Zigbee, 6LowPAN and RFID are jostling for last-meter LAN connectivity. At the same time, new approaches, such as LPWAN, are enabling unprecedented levels of connectivity at long ranges with low-power objects. LPWAN is intended not for real-time control at all, but for relatively infrequent status updates at low bandwidths and at very low battery levels. Each of these protocols occupies a different point in the multidimensional space, consisting of axes for power consumption, bandwidth, range and latency. For example, Wi-Fi is designed for high bandwidth, low-latency but relatively high-power applications, such as video cameras, while LPWAN is meant for relatively infrequent communications with, say, a tank level sensor. The absence of a dominant standard has driven IoT into a wild-west status.

Intellectual property, licensing and the ability to use standards freely are key measures of the effectiveness of a standard. Too often standards are burdened by intellectual property rights and require cross-licensing. Stipulations, such as Reasonable and Non-Discriminatory (RAND) licensing, can help mitigate the friction in standards adoption but require careful construction of IP agreements. Understanding which standard is best for which application, and which architecture, will be necessary to lay out the relevance of various standards under development, and where to play.

Other related questions on architectures and standards revolve around how the data are generated, how the data are made portable across applications/devices and how data reuse is supported. Data portability and reusability are critical to reducing operational costs and enhancing application and service capabilities. McKinsey states that interoperability is necessary to unlock more than $4 trillion in unrealized economic impact in IoT by 2025 (36% of the maximum $11.1 trillion economic benefit from the same study).[39] For example, individual car brands can collect their own traffic data – or better data can be aggregated by the entire fleet, using crowdsourcing.[40] Building on such an example, connected products may fundamentally change the way in which traffic management, road maintenance, autonomy, vehicle warranty services and maintenance are delivered. Yet today, such standards are rare.

Security and privacy

Security and privacy are related but apply to different concerns. Privacy deals with issues – intent, policy and procedures – related to personally identifiable information (PII). As with many computing and networking systems, IoT has a large impact on both issues: privacy and security. A cloud-backed home security camera may track a person's movements. The privacy questions are around what the homeowner's rights are over the data, as opposed to that of the cloud provider. The security question relates to the protection of the device and the cloud from hacking by a third party.

IoT fundamentally expands the PII reach of computer systems and the size of the attack surface. An industry study by Dell notes that the scale of IoT creates unexpected opportunities for hacking.[41] While 75% of respondents to a Forrester survey indicated that security was important or very important, 60% identified the area as a significant challenge.[42] Building and maintaining an IoT system is complicated. There are no clear and agreed upon architectures to simplify development. Systems may be secure independently, but by the time glue layers are developed to link dissimilar systems, weak links and new attack surfaces have been introduced.[43] The next war will likely be fought through the cyber-takedown of a country's infrastructure. Hacked power grids and exposed citizens are hardly the signs of a responsible industry.

As physical and digital systems converge, unintended consequences become an increasing and significant risk in IoT ecosystems.[44] This includes challenges hitherto unseen in the technology world, such as Trojan-horse hardware and software (for example, a webcam innocently brought into a factory, in which lurks malware that can infect the SCADA system), the confluence of even simple workflows with IoT functionality (an innocent valve may tomorrow have an embedded computer), and the attendant need to upskill, and so on. A default password can be all a malware needs to take residence inside an installation. Uniquely in this new world, safety considerations and cybersecurity considerations converge. What might have been an unintended safety lapse in the pre-IoT world can become a weapon in the hands of a remote malicious party in the IoT world. For example, the automotive staple CANbus may be inadequate for the challenges of security in a more interconnected world and new security solutions for IoT are being explored. A series of security holes has illustrated the need for rethinking.[45]

Security and privacy must be considered at the very start of the IoT journey.[46] Meanwhile, many who may think they have not started the IoT journey are probably already unwitting participants in the IoT ecosphere. If a system has electronic control, and it has even the most indirect connection to the internet, it is vulnerable to an IoT hack.[47] [48] This is a very significant problem – a 2014 World Economic Forum report estimated that by 2020, cybersecurity issues may result in as much as $3 trillion in loss.[49] The reality is that, with the events witnessed in 2016 and 2017,[50] [51] that number may underestimate IoT's potential risk exposure. Here is another difficulty in addressing security: there are no adequate IoT test beds, nor, as noted earlier, stated best practices in the form of reference architectures. And, sadly, the repercussions for insecurity are not sufficient.[52] A new approach to security and privacy, such as the Cognitive Firewall, is needed.

Individuals and businesses often resist IoT adoption due to a lack of confidence in today's privacy-preserving measures. Identity and trust are fundamental to ensuring sustainable growth. For example, an IoT valve being installed on a network must be able to show that it is certified for that installation, and the person installing the valve should be able to show that he or she is authorized to do so. This is a complex chain of actions, and one that goes well beyond our current conception of security protocols. Immediate, thoughtful community attention is needed to take on these issues. GS1 numbers can be used to identify products before they are using carriers such as barcodes and electronic product code (EPC) RFID. In a network, the Media Access Control address can be used to uniquely identify a device, and the Internet Protocol address can be used to communicate with the device. However, in IoT, identification is also needed for people to identify who is authorized, for example, to set up which device, when and how. This "soup" of identification has not been clarified and is resulting in different work practices, yielding potential security risks.

As indicated previously, voice, video, gesture and other similar interface standards create a whole new class of privacy questions. Voice can be used to "jump the air-gap", i.e. communicate without using the network at all. A recent Burger King commercial on TV simply asks Google Home to read out a longer description of its products.[53] Could this capability be used to unlock a smart door? The

Amazon Echo, meanwhile, erroneously recorded a man's conversation with his wife and sent it to an employee.[54] Is it okay for a voice-based device to detect the mood of the person and market accordingly? It is not unlikely that an AI engine will one day be capable of recognizing a disconsolate user and market liquor. Brain interfaces or neural interfaces, the stuff of science fiction, are also now becoming a reality.[55] Wearables can create a ubiquitous human-machine connection. These capabilities are powerful but, in addition to obvious privacy threats, also create security threats.

Fortunately, there is much research on privacy that can be brought to bear on these questions. Several of the solutions are technical.[56] [57] While the research on privacy is too extensive to describe here, the work of Sweeney on k-anonymity[58] and that of Dwork in differential privacy are starting points.[59] The extensive work in academia and research labs can be applied on this important topic.

One of the issues with IoT is the number of invisible connections that can proliferate between systems. Visualization tools can help end users to understand the flow of their data: what is shared, with whom, and for what purpose. For example, an augmented reality device that can help see which device is talking when and to which other device can build both understanding and trust.[60]

In addition to privacy and security are the questions related to policy. During the development of the EPC suite of RFID standards, the industry adopted a number of new principles, including notice and choice. The new General Data Protection Regulation from the EU has created specific guidelines that raise the bar for privacy protection. Security deals with the ability to protect systems from intrusions. IoT may trigger new regulation – which may be good or bad depending on whether it is thoughtful, reactive or an overreaction.

Shared value creation

In many ways, the apparently logical search for value seems to be one of the more paralysing aspects of IoT adoption. Consider first the individual organization. ROI calculations are extremely difficult to construct in the early days of any new technology for a large number of reasons. First, many such calculations are necessarily conservative. The myriad uses of enabling technologies, such as computers, the World Wide Web and mobile phones, could not have been, and were not, anticipated. The anticipated benefits of these technologies in the early days were often rather bleak.[61] As referenced earlier, in a Dell report, 48% and 27% of survey respondents list budgetary constraints and unclear financial benefits as barriers to IoT investment, respectively.[62] Second, early ROI analyses tend to be limited to silos of benefit – whereas a holistic view of a technology such as IoT can lead to broader benefits.[63] [64] As mentioned, IoT can be transformative; yet many analyses only consider the incremental benefits of IoT. Third, issues such as customer engagement and unintended upsides are inherently difficult to calculate, and so are often ignored. Making matters more complicated are the rapidly changing perceptions of customers today. What was innovative a year back may become today's table stakes. As consumers become more used to voice assistants, traffic-aware navigation systems, smart watches and self-driving cars, their base expectations for the value of IoT often increase more rapidly than companies can recognize.

A second stumbling block for IoT is the appropriation of value *across* the ecosystem. Ultra-high frequency (UHF) RFID fell into a trap that illustrates this point. Ideally, RFID was intended to make the entire supply chain more efficient. However, when retailers mandated suppliers to tag their products, a new dynamic emerged: suppliers complained that while they paid all the costs for tagging products, it was retailers that would reap the benefits in terms of better inventory management and reduced costs. This tension paralysed progress in RFID adoption for nearly a decade. Eventually, progress was made in RFID not because of cross-partner coordination, but in closed-loop implementations, where the entity bearing the price of tagging also reaped the benefits. So, for example, instead of a supplier tagging a shirt, and using that tag to improve its own supply chain as well as that of the retailer, the retailer would apply the tag and benefit from that information only in its own half of the supply chain. This was suboptimal – and another form of siloing of business cases. IoT could suffer from the same problem without openness to information-sharing and shared value. Avoiding this pitfall also requires an ecosystem view that seeks out the greater good, documents successes and establishes best practices – thereby giving courage and precedent to early adopters who wish to make the leap.

The issue is particularly pronounced for government infrastructure. Today, the value of everything from smart grids to instrumented water supplies depend on critical investments in the underlying IoT infrastructure. Yet few governments have the wherewithal to make these investments. Public-private partnerships (PPPs) are a powerful and economically sustainable way for cities and governments to draw investment and expertise to upgrade facilities for the better of society. Templates and best practices for PPPs are needed to ensure orderly and beneficial adoption. For example, many cities and countries will likely benefit from IoT investment in smart street lights, say, or smart parking meters.[65] [66] Rate-base investments from private entities can create the investment pipeline desperately needed.

The ultimate benefit of IoT will be sustainability. According to an analysis by the World Economic Forum in partnership with IoT Analytics, 84% of IoT deployments are currently addressing, or have the potential to address, the SDGs.[67] Indeed, many of the technologies described above affect several of the SDGs. This will ensure that the value of IoT is shared across all of society, and indeed humanity. A robust, smart grid that is two-way, and that can absorb power from homes, as well as supply power to homes, will contribute to the reduction of greenhouse gas emissions. This requires a great deal of IoT infrastructure, ranging from phase measurement units to sensors and switches in homes. The shepherding of this grand future requires broader systemic thinking across industries and nations than is currently occurring.[68]

Organizational development

IoT will create ripples that cascade across the organizations with positive and negative consequences. Almost one-third (30%) of business leaders believe IoT will unlock new revenue opportunities with 23% believing that IoT will change their company's models of operation, including internal operations.[69] Specifically, IoT can be leveraged as a boon to business innovation, as cited by 53% of respondent organizations in IDG's study, as well as reduced costs, cited by 50%.[70] Benefits will be disproportionate across organizations and will therefore require a single-minded focus on overall company success. For example, a change in business model from a one-time sale approach to a subscription or service approach will likely change sales patterns, with traditional sales metrics taking a hit. Handling these changes will require organizational determination. Corporate leadership will become essential in the face of these challenges, and tolerance of failure will be a defining factor. For all the success of Amazon Echo, consider this: by any standard, the Amazon Fire Phone was an abject failure.[71]

IoT is also expected to affect the business models of companies. Currently, Ford Motor Company is confronting a new future in which products are replaced by services in much the same way as GE did: by testing the transportation as a service market through its acquisition of Chariot.[72] Initiatives such as these will change incentives, practices and skills across the company, requiring further executive leadership and a steady hand on the tiller.

IoT will exacerbate the skills gap facing many organizations and even nations.[73] This will be especially challenging in the emerging gig economy, in which workers are more likely to be freelancers and possibly transient. Traditional IT skills translate only partially to the IoT sphere. Knowledge of protocols, hardware, security, privacy and the cloud are a starting point for IoT implementers. General rank and file employees will also need to upgrade their skills to deal with IoT, just as they have had to with basic computers. In response to the question: "Does a plumber have to become an IoT expert?", the answer, to some extent, is "yes." The plumber needs to have enough knowledge to know how to ensure that security protocols are followed, ensure that the device is authorized, to initiate the IoT valve, to test it, and to monitor it during use. This level of retraining is unprecedented, and the new reality. Employee upskilling, whether through online courses or virtual/augmented reality, through apprenticeship or traditional classes, will possibly be the clarion call of the IoT age.

The emergence of IoT also involves the development of new manual protocols, systems, checks and balances. For example, the checklist required to change an IoT-equipped valve will be very different than a traditional valve. At the same time, the data from the valve, and the signal sent to control the valve, must be handled differently to extract maximum performance without compromising safety. The development of these new procedures will require an extensive new activity, parallel to the training activity described above. In many ways, this is the curriculum for the training. However, the new normal will be the continuous updating of these protocols and procedures as technology evolves rapidly. For example, the sensor on the valve may have a battery that lasts one week today but may increase to one month in a few years as battery technology, as well as power electronics, improve. This will require an update to the protocols. Deploying hardware that can be updated via software in the field will become the new normal.

New technologies also require new behaviour patterns by customers. For example, an electric car in the hands of the customer may not perform very well if the customer does not charge it appropriately. A connected car may deliver a great deal more benefit if connected to the home of the customer (to turn the thermostat on, as discussed previously, for example). In other words, the company's product offering is now part of a larger ecosystem, and integration with that ecosystem becomes more important. This will require, on the one hand, a new class of engineering – ecosystem engineering – which makes the ecosystem foolproof and the products responsive to real-time use and user demands[74] and, on the other hand, a new class of marketing functions that includes educating the customer.

A central theme in this coming revolution is upskilling. There is a great deal of worry across the world about the future of work. Yet IoT presents both a challenge and a massive opportunity. Leveraging new educational approaches (e.g. online), combined with new educational paradigms (e.g. intense, short, in-person programmes at community colleges and companies across the world, new virtual/augmented reality-based worker training/assistance programmes and new credential schemes), it is possible to create a new cadre of employees and creators who can have gainful, productive employment in this new world.

Ecosystem governance

The IoT ecosystem suffers from an odd problem: too little governance at a holistic level and yet too many competing governance mechanisms at the level of individual standards. There is a dire need to collaborate, self-govern, self-certify, establish best practices, develop cross-border agreements and even self-police. As recent events from the social media and cryptocurrency world show, there is often a wild-west approach when new industries emerge. Other technology revolutions have had to face similar issues. In the case of the internet, it was the Advanced Research Projects Agency (ARPA) that acted as the "sheriff", guiding convergence, a shared sense of purpose and an aspiration for the greater good. For the World Wide Web, the W3C consortium served a similar purpose.[75] Creative Commons similarly promoted and brought order to the sharing and reuse of creative works.[76] In the case of EPC UHF RFID, it was the Auto-ID Centers, first at MIT, then at Cambridge, ETH Zurich, the University of Adelaide, Keio University in Japan and Fudan University in China, all backed by over 100 sponsor companies and GS1, that were collectively able to drive a unified standard. The Auto-ID work was then absorbed into GS1, which took on the mantle of creating shared guidelines for everything from standards to privacy. (A co-author of this document, Sanjay Sarma, was a key part of this effort.)

The wild-west nature of IoT has manifested itself in many ways: the security and privacy issues listed earlier, the balkanized standards, the lack of anonymized data-sharing for the greater good and sudden shifts in standards. The selection of NB-IoT is one such example.[77] Another path forward is possible, however. A salutary lesson on cross-industry standards, digital rights management and consumer reactions in a non-IoT environment can be found in the case of Keurig's approach to coffee pods.[78]

Recommendations

IoT must be thought of not simply as a method to seek incremental improvements but rather as a new design language to rethink and transform organizations and business. Leadership in such situations is most effective coming from the top – both in individual organizations and across organizational, industry and even national boundaries. Multistakeholder collaboration, including the creation of channels between academia and industry to share research and explore collaboration, will be vital to ensure the development of scalable, sustainable and effective architectures that benefit the world at large.

The journey to transformation will not be linear. Organizations must be ready to experiment, learn, refine, engage. Opportunities to get a head start exist by leveraging existing standards, policies and initiatives. Small, safe experiments can be used to build expertise. Consider, for example, the Industrial IoT Safety Protocol.[79] Safety is a relatively straightforward win with IoT.

Architecture and standards

- IoT use cases will evolve; therefore it is critical to ensure that the chosen architecture is future-proof and extensible. Businesses should consider industry-wide use cases to ensure a full appreciation of where the industry may go. Meanwhile, it is necessary to ensure that the chosen architecture is not brittle and will permit an evolution of the overall system as well as maintenance and upkeep.

- When planning the architecture of IoT systems, it is important to consider if the physical object should have a digital twin, and how much of the computation and communication should be edge versus on the cloud.[80]

- Communication standards should be used and matched to specific needs: range, power, latency, bandwidth. It is important to standardize data as much as communication.

Security and privacy

- Reference architectures should be created on which to base security approaches.[81] It is essential that security and privacy are planned for from the very beginning. For example, it is important to ensure that all systems can be updated seamlessly and over the air.

- New security and privacy approaches will be needed as the cyberworld and physical worlds intersect. Joint research efforts with major universities and industries can help ensure continuously evolving thinking.

- Clear, user-centric policies are needed for identification, access control, authentication, data ownership and use.

- It is critical to always think beyond the first installation. What happens when a device fails? What are the technical and people protocols for replacing the device? What are the protocols for protecting against malicious players, including employees and consultants, and against Trojan-horse hardware and software? New privacy protection technologies can be of significant benefit in the realm of IoT.

Shared value creation

- Cross-industry, cross-sector and cross-organizational use cases should be documented and included in roadmaps. It is important to look for shared value creation across all partners including end consumers.

- Incentives are needed for vendors to create interoperable hardware, software and data standards so that all members of the ecosystem can benefit. Misplaced aspirations of lock-in will self-limit industry expansion.

- Public-private partnerships can bring together the best of government and industry. There are more stakeholders in IoT than in many conventional industries due to its broader reach, large scale and extensible utility.

Organizational development

- IoT will bring significant changes to organizations and ecosystems. This will result in changing business models, individual incentives and organizational boundaries. Steady leadership will be central to navigating these changes.

- Strategies are needed to develop the human capital for the coming IoT revolution. A new design language is emerging – but do you have people who speak IoT? Organizations should consider new technologies, such as virtual and augmented reality, to help train new workers and to cope with an increasingly transient gig economy workforce.

- The emerging skills gap will require a massive retraining effort. Radical new approaches to upskilling should be considered, including online courses, intensive workshops and so on.

Ecosystem governance

- A governance council for the IoT ecosystem is greatly needed. Sustainability and ensuring shared value creation should be a key focus and goal for the council. It is also vital that a security observatory be established to share guidelines, standards, reference architectures, test beds, best practices and timely warnings across industries and sectors.

- A comprehensive philosophical framework should be established for thinking about security, privacy and safety in the IoT context. This is probably best done in partnership with academia, from where the modern principles of cyber (IT) have come – but they need to be rethought for cyberphysical (IoT) applications.

- Precompetitive consensus roadmaps should be developed, as was done in the semiconductor industry by SEMATECH[82] and in the RFID industry using Pelotons.[83] Close collaboration with industry groups such as the IIC and GS1 are key to a multistakeholder approach.

- New cross-industry training standards, certifications and credentials should be encouraged and developed to support shared learning and advancement.

Conclusion

IoT is a game-changing opportunity that may substantially affect business and society. It is an ecosystem opportunity – one with the potential to change businesses and governments from within, as well as externally in society at large. This document provides a framework to examine IoT's potentially transformative set of technologies through the lens of the five pillars described.

Quantifying IoT's value is difficult but, no matter the precise numbers, the impact – economically and socially – could be massive. With partnerships in place, elevating society as a whole can be lucrative and enriching for all parties. IoT, done right, could make everyday living safer, more efficient and more convenient, and could make the world at large more sustainable, happier and friendlier. This paper suggests IoT can be a new design language, where connectivity, computation, sensing and actuation pair with recruitability and immersiveness to enable a better life for humans – in ways sometimes visible and sometimes unseen and seemingly magical. Every smart thermostat has the potential to reduce energy wastage, every smart parking meter to reduce traffic, and every sensor to improve safety.

Nevertheless, IoT is currently a multifaceted, multiparty space with a largely uncoordinated group of stakeholders. Technological advances from labs, start-ups and larger companies in this space, while exciting, are somewhat inchoate and even chaotic – and run the risk of premature, heavy-handed regulation. Even where regulation does not result, the move to launch quickly and gain a first-mover advantage can be detrimental to industries, where ill-conceived roll-outs result in burned bridges for partnerships and consumer perception problems. In many cases, the IoT space must anticipate and avoid versions of a principal-agent problem through collaboration. For example, government officials in cities may want extensive standardization while technology vendors may favour proprietary approaches. More than ever, IoT requires the engagement of a large number of stakeholders in and across organizations. This includes other companies, industries, governments, standards bodies and the citizenry at large.

Major questions related to privacy, security, trust, sustainability and consumer guidelines need to be addressed, not in a piecemeal fashion, nor jurisdiction by jurisdiction. The melding of digital and physical systems, which could occur at great economic and geographic scale, needs the trust and empowerment of end users. Beyond designing robust hardware or conventional cybersecurity alone, the richness of IoT data makes it critical to be transparent and progressive in allowing participants insight and control over their data ownership and sharing. Leaders need to rethink norms and embrace IoT's potential for change in a safe, scalable and effective way. The organizations best poised to leverage IoT will form a clear vision and make it a CEO and C-suite priority, and will realign around new, bolder visions for the future. Organizations must come together internally and as members of a larger global community to develop IoT as an ecosystem play. Corporate roles will change, and having adaptable teams and a willingness to pioneer new and evolving visions are a must. Organizations will need to adapt to become worldlier and more cross-discipline, leveraging others' competencies and marketing their own internal excellence to partner organizations.

Industry bodies such as GS1[84] and the IIC[85] are major forces in converging thinking in the retail and industrial sectors. However, a cross-sector council is needed to wrestle with the problems and issues outlined in this document. The World Economic Forum provides such a platform, as well as an opportunity for broad consensus-building along these lines.

IoT has the potential to change the way people work, live and play, buy and sell, and interact. This paper argues that it is a new design language – the plumbing of a better future – and that it can take the old and make it new and fresh in a manner that is safe and secure. Our job must be to devise the appropriate vocabulary and grammar to make sure that the language achieves its greatest potential without unnecessarily introducing the potential to cause harm – whether intentional or not.

Contributors

The World Economic Forum acknowledges the dedication and valuable contributions of the following authors and staff who made this publication possible.

Massachusetts Institute of Technology
(Co-authors)

Joshua Siegel
Research Scientist
USA

Sriram Krishnan
Research Affiliate
USA

Brian Subirana
Director, MIT Auto-ID Lab
USA

Sanjay Sarma
Professor of Mechanical Engineering and Co-Founder, MIT Auto-ID Lab
USA

World Economic Forum

Jeff Merritt
Head, IoT, Robotics and Smart Cities
Centre for the Fourth Industrial Revolution

Lauren Joseph
Community Lead, Electronics Industry
Centre for Global Industries

Rodrigo Arias
Content Lead, Technology, Media and Digital Industries
Centre for Global Industries

This White Paper benefited from the input of many experts and diverse stakeholders who shared case studies, insights and lessons learned through a series of workshops, conference calls, meetings and roundtable events over the course of 2017 and 2018. A supplemental list of experts and partners is included in Annex 1.

Annex 1: Workshop participants

The Forum is grateful for the substantive contributions received from the workshop participants listed below, as well as from the many companies and organizations that participated in related conference calls, meetings and roundtable events.

These partners include, but are not limited to, American Tower Corporation, AT&T, BCG Digital Ventures, BSI Group, BT, Cisco, Dell, Ericsson, Fujitsu, Google, GS1/Vaspar Strategies, Harvard University, HCL, Hewlett Packard Enterprise, Huawei, IEEE, Infosys, IoT Impact Labs, Kaiser Permanente, Kudelski Group, Microsoft, Nokia, Object Management Group, Qualcomm, Royal Philips, Thomson Reuters, Tibco, UL, United Nations and VIA Technologies.

"Aligning the IOT Ecosystem towards Sustainable Adoption" Workshop participants

Alexandra Amouyel, Executive Director, Solve, Massachusetts Institute of Technology, USA
Mikael Bäck, Vice-President, Technology and Emerging Business, Ericsson, Sweden
Joel Barbier, Director, Thought Leadership, Cisco, USA
Tilman Buchner, Director, Engineering, BCG Digital Ventures, Germany
Sri Chandrasekaran, Director, Standards and Technology, Institute of Electrical and Electronics Engineers (IEEE), India
Edmund DiSanto, Executive Vice-President, Chief Administrative Officer and General Counsel, American Tower Corporation, USA
Jamshed Dubash, Chief Executive Officer, Vaspar Strategies, Vaspar, USA
Hod Fleishman, Partner, BCG Digital Ventures, USA
Matilda Gennvi-Gustafsson, Director, Sustainability, Ericsson, Sweden
Todd Glover, Director, Global Product Security and Services Program, Royal Philips, USA
Becca Gould, Senior Vice-President, Public Affairs, American Tower Corporation, USA
Haizhou Gu, Associate Officer, Information Systems, United Nations Counter-Terrorism Committee Executive Directorate (CTED), New York
Patrick Hauert, Vice-President, Programme Development, Kudelski Security, Kudelski Group, Switzerland
Ellis Lindsay, General Manager, Customer Experience Solutions, Nokia, Canada
David O'Brien, Senior Researcher, Berkman Klein Center for Internet & Society, Harvard University USA
Danielle Osler, Public Policy Counsel, Google, USA
Chris Rezendes, Managing Director, IOT Impact Labs, USA
Andreas Rohnfelder, Head, Industry 4.0 Competence Center, Fujitsu, Germany
Sanjay Sarma, Professor of Mechanical Engineering and Co-Founder, Auto-ID Lab, Massachusetts Institute of Technology, USA
Alpesh Shah, Senior Director, Global Business Strategy and Intelligence, Institute of Electrical and Electronics Engineers (IEEE), USA
Joshua Siegel, Research Scientist, Massachusetts Institute of Technology, USA
Richard Soley, Chairman and Chief Executive Officer, Object Management Group, USA
Brian Subirana, Director, Auto-ID Lab, Massachusetts Institute of Technology, USA
Michael Sutten, Chief Technology Officer, Kaiser Permanente, USA
Michael Tennefoss, Vice-President, Strategic Partnerships, Aruba Networks, USA
Dave Weller, Chief Enterprise Architect, Thomson Reuters, USA
Ethan Wood, Vice-President, Global OEM Solutions and IoT Marketing, Dell Technologies, USA
Epan Wu, President, Embedded Systems and IoT Business, VIA Technologies, Taiwan, China

Endnotes

1. Gartner. “Top Strategic Predictions for 2016 and Beyond: The Future Is a Digital Thing”, 2 October 2015. https://www.gartner.com/binaries/content/assets/events/keywords/symposium/sym26/gartner_top_strategic_predictions_2016.pdf (accessed 8 January 2019).

2. Hewlett Packard Enterprise. “Smart cities and the Internet of Things”. HPE business white paper, 2016.

3. Manyika, James et al. *The Internet of Things: Mapping the Value Beyond the Hype.* McKinsey Global Institute, 2015.

4. Henley, Jon. *Life before artificial light,* 31 October 2009. https://www.theguardian.com/lifeandstyle/2009/oct/31/life-before-artificial-light (accessed 11 January 2018).

5. Zipcar. n.d. http://www.zipcar.com (accessed 11 January 2018).

6. Ho, Grant et al. “Smart Locks: Lessons for Securing Commodity Internet of Things Devices”. *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security.* New York: ACM, 2016. 461-472.

7. If This Then That (IFTTT) (User: Bocovich). *Geofencing for the Nest.* n.d. https://ifttt.com/applets/194273p-geofencing-for-the-nest (accessed 11 January 2018).

8. Apple. *How to unlock your Mac with your Apple Watch.* n.d. https://support.apple.com/en-us/HT206995 (accessed 11 January 2018).

9. Davies, Chris. *Smarter’s WiFi Coffee Maker adds caffeine to IoT*. *Slashgear,* 5 January 2015. https://www.slashgear.com/smarters-wifi-coffee-maker-adds-caffeine-to-iot-05361984/ (accessed 11 January 2018).

10. Feldmeier, Mark and Joseph A. Paradiso. “Personalized HVAC control system”. *2010 Internet of Things conference.* Tokyo, Japan: IEEE, 2010.

11. Trajectio. *Inexpensive follow me lighting and music at home*. *Kickstarter.* May 2017. https://www.kickstarter.com/projects/1109816630/trajectio-motion-powered-hue-and-sonos-smart-home?ref=nav_search (accessed 11 January 2018).

12. Adib, Fadel et al. “Smart Homes that Monitor Breathing and Heart Rate”. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.* Seoul: ACM, 2015. 837-846.

13. Krumm, John and Eric Horvitz. “Predestination: Inferring Destinations from Partial Trajectories”. *International Conference on Ubiquitous Computing.* Springer, 2016. 243-260.

14. Nestle. *NESCAFÉ Coffee Machine,* 10 November 2017. https://itunes.apple.com/mx/app/nescaf%C3%A9-coffee-machine/id1239418048?l=en&mt=8 (accessed 11 January 2018).

15. Eight. *Eightsleep*, 2018. http://www.eightsleep.com (accessed 11 January 2018).

16. Endgadget. “Amazon acquires Ring’s smart doorbell business”. *Endgadget news,* 27 February 2018. https://www.engadget.com/2018/02/27/amazon-acquires-ring/ (accessed 5 March 2018).

17. IBM. “Trust in trade”. White paper. *IBM Institute for Business Value*, 2016. https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03771usen/gbe03771usen-00_GBE03771USEN.pdf (accessed 4 January 2019).

18. Forbes. “IBM Blockchain Is Tracking Diamond Rings Across the Globe”. *Forbes.com*, 26 April 2018. http://fortune.com/2018/04/26/ibm-blockchain-diamonds-helzberg/ (accessed 1 June 2018).

19. National Institute of Standards and Technology (NIST), US Department of Commerce. “Fog Computing Conceptual Model”. Special Publication 500-325. *NIST*, March 2018. http://bccl.ir/wp-content/uploads/2018/07/NIST.SP_.500-325.pdf (accessed 5 January 2019).

20. Langner, Ralph. “Stuxnet: Dissecting a Cyberwarfare Weapon”. *IEEE Security & Privacy* (IEEE) 9, no. 3, May-June 2011: 49-51.

21. Kolias, Constantinos et al. “DDoS in the IoT: Mirai and Other Botnets”. *Computer* 50, no. 7, 2017: 80-84.

22. Sarma, Sanjay. “I helped invent the Internet of Things. Here’s why I’m worried about how secure it is”. *Politico*, 29 June 2015.

23. Gubbi, Jayavardhana et al. “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions”. *Technical Report CLOUDS-TR-2012-2, Cloud Computing and Distributed Systems Laboratory, The University of Melbourne*, 29 June 2012.

24. Atzori, Luigi, Antonio Iera and Giacomo Morabito. “The Internet of Things: A survey”. *Computer Networks* 54, no. 15, October 2010: 2787-2805.

25. Jasper; Cisco. *The IOT Value/Trust Paradox.* n.d. https://www.jasper.com/resources/reports/iot-value-and-trust-survey?ecid=af_700000005 (accessed 5 January 2019).

26. The Economist. “Cutting the cord”. *The Economist,* 7 October 1999. https://www.economist.com/special-report/1999/10/07/cutting-the-cord (accessed 5 January 2019).

27. Dell and IDG Research Services. “Internet of Things: A Data-Driven Future for Manufacturing”, 2015.

28. New York Times. “Burger King ‘O.K. Google’ Ad Doesn’t Seem O.K. With Google”. *The New York Times,* 12 April 2017. https://www.nytimes.com/2017/04/12/business/burger-king-tv-ad-google-home.html (accessed 5 January 2019).

29. Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System,* 2008. https://bitcoin.org/bitcoin.pdf (accessed 11 January 2018).

30. IOTA Foundation. *The Economy of Things.* n.d. https://iota.org/ (accessed 11 January 2018).

31. Al-Fuqaha, Ala et al. “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”. *IEEE Communications Surveys & Tutorials* (IEEE) 17, no. 4, June 2015: 2347-2376.

32. Lee, In and Kyoochun Lee. “The Internet of Things (IoT): Applications, investments, and challenges for enterprises”. *Business Horizons* (Elsevier) 58, no. 4, July-August 2015: 431-440.

33. Siegel, Joshua, Sumeet Kumar and Sanjay Sarma. “The Future Internet of Things: Secure, Efficient, and Model-Based”. *IEEE Internet of Things Journal* (IEEE), October 2017.

34. Siegel, Joshua. *Design, Development, and Validation of a Remotely Reconfigurable Vehicle Telemetry System for Consumer and Government Applications.* S.B. Thesis, MIT, 2011.

35. Tuegel, Eric J. et al. “Reengineering aircraft structural life prediction using a digital twin”. *International Journal of Aerospace Engineering*, 2011.

36. Siegel, Joshua, Dylan Erb and Sanjay Sarma. “Algorithms and Architectures: A Case Study in When, Where and How to Connect Vehicles”. *Intelligent Transportation Systems Magazine* (IEEE) 10, no. 1, January 2018: 74-87.

37. Siegel, Joshua, Sumeet Kumar and Sanjay Sarma. “The Future Internet of Things: Secure, Efficient, and Model-Based”. *IEEE Internet of Things Journal* (IEEE), October 2017.

38. Industrial Internet Consortium (IIC). “IIC Connected Care Testbed.” *Industrial Internet Consortium,* 2016. https://www.iiconsortium.org/connected-care.htm (accessed 2 July 2018).

39. Manyika, James et al. *The Internet of Things: Mapping the Value Beyond the Hype.* McKinsey Global Institute, 2015.

40. Connected-Car. “BMW, Audi, Mercedes Take On Waze”. *The Connected Car news,* 7 August 2017. https://www.theconnectedcar.com/author.asp?section_id=627&doc_id=735031& (accessed 15 January 2018).

41. Dell and IDG Research Services. “Internet of Things: A Data-Driven Future for Manufacturing”, 2015.

42. Forrester Research Inc. *Internet of Everything Solutions Are Gaining Momentum.* A Forrester Consulting Thought Leadership Paper Commissioned By Cisco, 2015.

43. Sarma, Sanjay. “I helped invent the Internet of Things. Here’s why I’m worried about how secure it is”. *Politico*, 29 June 2015.

44. Sarma, Sanjay and Josh Siegel. “Bad (internet of) things”. *Computerworld*, 30 November 2016.

45. The Register. “Sons of IoT: Bikers hack Jeeps in auto theft spree”. *theregister.co.uk,* 31 May 2017. https://www.theregister.co.uk/2017/05/31/bikers_hack_jeeps_in_auto_theft_spree/ (accessed 5 January 2019).

46. *SimpliSafe.* n.d. https://simplisafe.com/ (accessed 5 January 2019).

47. Bilefsky, Dan. “Hackers Use New Tactic at Austrian Hotel: Locking the Doors”. *The New York Times*, 30 Janury 2017. https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html (accessed 10 January 2018).

48. Mashable. “Hackers exploit smart thermometer to steal casino information”. *Mashable news,* 15 April 2018. https://mashable.com/2018/04/15/casino-smart-thermometer-hacked/#6MjapIJuBaqV (accessed 15 April 2018).

49. World Economic Forum. *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services,* January 2015.

50. Kolias, Constantinos et al. “DDoS in the IoT: Mirai and Other Botnets”. *Computer* 50, no. 7, 2017: 80-84.

51. Adamov, Alexander and Anders Carlsson. “The state of ransomware. Trends and mitigation techniques”. *2017 IEEE East-West Design & Test Symposium (EWDTS)*, 2017.

52. Sarma, Sanjay. “I helped invent the Internet of Things. Here’s why I’m worried about how secure it is”. *Politico*, 29 June 2015.

53. New York Times. “Burger King ‘O.K. Google’ Ad Doesn’t Seem O.K. With Google”. *The New York Times,* 12 April 2017. https://www.nytimes.com/2017/04/12/business/burger-king-tv-ad-google-home.html (accessed 5 january 2019).

54. Washington Post. “An Amazon Echo recorded a family’s conversation, then sent it to a random person in contacts”. *The Washington Post,* 24 May 2018. https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/ (accessed 5 January 2019).

55. CTRL-Labs. *CTRL-Labs.* May 2018. https://www.ctrl-labs.com/ (accessed 5 January 2019).

56. Weber, Rolf H. “Internet of Things - New security and privacy challenges”. *Computer Law & Security Review*, 2010: 23-30.

57. Weis, Stephen A. et al. “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”. *Security in Pervasive Computing* (Springer Berlin Heidelberg), 2004: 201-212.

58. Sweeney, Latanya. “k-anonymity: A model for protecting privacy”. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10.05, 2002: 557-570.

59. Dwork, Cynthia. “Differential privacy”. *Automata, languages & programming* (Springer Berlin Heidelberg), 2006: 1-12.

60. Mayer, Simon and Josh Siegel. “Conversations with connected vehicles”. *2015 5th International Conference on the Internet of Things,* 2015.

61. The Economist. “Cutting the cord”. *The Economist,* 7 October 1999. https://www.economist.com/special-report/1999/10/07/cutting-the-cord (accessed 5 January 2019).

62. Dell and IDG Research Services. “Internet of Things: A Data-Driven Future for Manufacturing”, 2015.

63. Mukhopadhyay, S.C. and N. K Suryadevara. “Internet of Things: Challenges and Opportunities”. In *Internet of Things. Smart Sensors, Measurement and Instrumentation, vol 9*. Springer, Cham, 2014.

64. The Economist. *The Internet of Things Business Index: A quiet revolution gathers pace.* The Economist Intelligence Unit, 2013.

65. Kumar, Sumeet et al. “Urban Street Lighting Infrastructure Monitoring Using a Mobile Sensor Platform”. *IEEE Sensors Journal* (IEEE) 16, no. 12, June 2016: 4981-4994.

66. O'Connor, Mary C. "Sensors Turn Parking Meters Into Parking Helpers". *RFID Journal*, 2 October 2014. http://rfid.grandcentr.al/articles/sensors-turn-parking-meters-into-parking-helpers (accessed 8 January 2019).

67. World Economic Forum, *IoT for Sustainable Development Project*, n.d. http://widgets.weforum.org/iot4d/ (accessed 11 January 2018).

68. World Economic Forum, *Internet of Things: Guidelines for Sustainability*, January 2018, http://www3.weforum.org/docs/IoTGuidelinesforSustainability.pdf (accessed 5 January 2019).

69. Mukhopadhyay, S.C. and N. K Suryadevara. "Internet of Things: Challenges and Opportunities". In *Internet of Things. Smart Sensors, Measurement and Instrumentation, vol 9*. Springer, Cham, 2014.

70. Dell and IDG Research Services. "Internet of Things: A Data-Driven Future for Manufacturing", 2015.

71. CNET. "Fire Phone one year later: Why Amazon's smartphone flamed out". *cnet.com*, 24 July 2015. https://www.cnet.com/news/fire-phone-one-year-later-why-amazons-smartphone-flamed-out/ (accessed 5 January 2019).

72. CNBC. "Ford's Chariot aims to fill NYC transit gaps with ride-sharing shuttle service". *CNBC.com*, July 2017. https://www.cnbc.com/2017/07/27/fords-chariot-aims-to-fill-nyc-transit-gaps-with-ride-sharing-shuttle-service.html (accessed 2 July 2018).

73. CMO Council and BPI Network. "The Impact of Connectedness on Competitiveness". *Business Performance Innovation (BPI) Network, Programs Background*, 2017.

74. Erb, Dylan. *Optimizing hybrid vehicles: battery pack design, energy management, and collaborative learning.* MIT PhD thesis, 2016.

75. W3C. *World Wide Web Consortium.* n.d. http://w3.org (accessed 5 January 2019).

76. Creative Commons. *Creative Commons.* n.d. http://creativecommons.org (accessed 5 January 2019).

77. SCMP. "China Mobile scrambles to catch up after supporting wrong 'internet of things' standard". *South China Morning Post*, 7 July 2017. http://www.scmp.com/tech/china-tech/article/2101138/china-mobile-grapples-internet-things-after-its-wrong-footed (accessed 5 January 2019).

78. The Verge. "Keurig's attempt to 'DRM' its coffee cups totally backfired". *The Verge*, 5 February 2015. https://www.theverge.com/2015/2/5/7986327/keurigs-attempt-to-drm-its-coffee-cups-totally-backfired (accessed 5 January 2019).

79. World Economic Forum. *Industrial Internet of Things Safety and Security Protocol*, April 2018. https://www.weforum.org/whitepapers/industrial-internet-of-things-safety-and-security-protocol (accessed 5 January 2019).

80. Wilhelm, Erik et al. "Cloudthink: a scalable secure platform for mirroring transportation systems in the cloud". *Transport* 30, no. 3, 2015: 320-329.

81. Sarma, Sanjay. "I helped invent the Internet of Things. Here's why I'm worried about how secure it is". *Politico*, 29 June 2015.

82. Carayannis, Elias and Jeffrey Alexander. "Strategy, Structure, and Performance Issues of Precompetitive R&D Consortia: Insights and Lessons Learned From SEMATECH". *IEEE Transactions on Engineering Management* (IEEE), no. 51, June 2004: 226-232. https://www.researchgate.net/publication/3076813_Strategy_Structure_and_Performance_Issues_of_Precompetitive_RD_Consortia_Insights_and_Lessons_Learned_From_SEMATECH (accessed 8 January 2019).

83. Subirana, Brian et al. "Peloton Planning Tool: Applying the Peloton to the EPC Industry". *GS1 EPC Global White Paper Collection*, 2005.

84. GS1. "Welcome to GS1". n.d. https://www.gs1.org/ (accessed 5 January 2019).

85. Industrial Internet Consortium (IIC). n.d. https://www.iiconsortium.org/ (accessed 5 January 2019).

WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org