The Internet & the Physical World

The lines of separation between the digital and physical worlds will continue to blur, altering economies around the world but also raising a host of security and privacy concerns.

Overview

The Internet of Things (IoT) is removing the separation between the Internet and our physical world. Gartner predicts that 8.4 billion "things" will be connected in 2017, more than doubling to over 20 billion by 2020.[1] IoT itself is not new, but the combination of increasing bandwidth, sensor technology and Artificial Intelligence (AI) may trigger an explosion of ubiquitous connectivity. Virtually everything that can be connected will be connected. This will transform whole economies and societies.

While innovation brings opportunity, the shift to a hyperconnected world raises key questions and uncertainties for the future. As the Internet will be used to control objects, infrastructure and much of our environment, questions about privacy, interoperability, regulation and security will need to be urgently answered.

The convergence of the physical and digital worlds will fundamentally change what it means to be online — this will have far-reaching implications for society and all sectors of the economy, from medicine to manufacturing.

For IoT to thrive, the security of connected devices must be addressed.

If appropriate safeguards to ensure transparency and user control are not put in place IoT could drive data-collection and use in ways that further undermine privacy and deepen surveillance.

Interoperability will be essential to the overall success of IoT and to maximise its positive impact on the global economy.

[1] Gartner source: http://www.gartner.com/newsroom/id/3598917

Socioeconomic Implications of Converging Digital and Physical Worlds

When virtually any object can be connected to the Internet, our digital and physical worlds will increasingly converge. IoT forms the basis of this convergence, but IoT is not a single technology. It is a set of applications and capabilities, services, and infrastructure that provide the intelligence needed to make connected objects useful. Developments in artificial intelligence will enable new means of interacting with connected objects through voice or gesture, and virtual and augmented reality will be powered by data generated by IoT. With IoT and AI, as well as increased bandwidth and sensor technologies, we are approaching a state of convergence where the lines between the digital and the physical blur. But for all of this to happen, we will need ubiquitous, reliable and secure connectivity around the globe.

> “
> We are entering a new phase of technological evolution, a phase where the Internet will be fully integrated into every part of our lives — how we learn, how we work, how we shop, how we get around.
>
> Private Sector, Europe

IoT could bring about a world in which the Internet is fully integrated into every part of economy and society. It may reduce mundane tasks, freeing workers to focus on creative, non-routine aspects of their jobs. But, as convergence gains momentum, every industry faces disruption that may change or even destroy jobs.

> “
> The Internet of Things, virtual reality, and artificial intelligence are changing the nature of work in a way that would empower and liberate people, and diminish inequalities among people and among countries -- or the outcome could be a diametrically opposite one.
>
> Academic, Europe

IoT also brings a convergence of digital and analogue industries, for example, of technology and manufacturing firms. The Internet will evolve from being dominated by the Web and mobile applications to an Internet that permeates all aspects of the physical world. This will change current market dynamics and bring increasing competition between traditional industry and the ICT sector.

The industry-specific regulatory frameworks we currently have in place are not well suited to a world in which connectivity blurs the lines between sectors of the economy. The challenge for policymakers will be twofold: one, to avoid falling further behind technological change; and two, to avoid disproportionate and potentially harmful regulations in response to evolving security threats.

> “
>
> Countries need to enhance their industrial policies and consumer protection-frameworks to prepare for IoT … National IoT frameworks will also need to incorporate cultural considerations that will impact IoT development.
>
> Internet Society Member, Africa

While lives may be improved by smart homes and smart cities, IoT’s promise of billions of devices constantly transmitting data raises many issues. We may see increased mass surveillance, the further erosion of privacy, and a growing dependence on data collection, analytics, and curation. The implications for privacy are profound. Without essential safeguards, greater amounts of data will be collected and used without the user’s knowledge or control.

> “
>
> IoT will make what remains of us, in terms of privacy, publicly available and ‘published’.
>
> Technologist, Middle East

Related to: Artificial Intelligence; The Role of Government; The Internet Economy

The Pressing Need for IoT Security

Connected devices add enormous complexity to an already complex security environment. They also raise the stakes, with increased potential for cyber threats to damage physical assets and harm human life. We are adopting IoT faster than we can secure it. This rush is accelerated by the increasing number of new entrants and the push to quickly release Internet-connected devices produced without prioritising security.

> “
>
> Africa must develop agriculture, AI, and IoT together to respond to Africa-specific challenges instead of copying others. However, it will be necessary to assure a greater level of security as attacks become more and more numerous.
>
> Internet Society Member, Africa

The Mirai attack of 2016[2] starkly shows the effect plug-and-play and remotely-managed IoT devices can have on the broader Internet. Many of the connected devices on the market today have very limited built-in security measures and will not be updated through the devices’ anticipated lifetime. This explosion in the number of connected devices — in transportation, wearables, health, smart homes, and alarm systems — alters the cyber threat landscape in unprecedented ways. A lack of agreement on IoT Security frameworks and best practices may jeopardise the safety of individuals around the globe.

[2] https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

> IoT compounds every security problem ever seen and multiplies every problem of the Internet. Your toaster could be sending out spam.
>
> Technologist, North America

Will governments increase regulation of the Internet in response to this new threat landscape? If so, will their responses be effective and respectful of privacy and individual autonomy? The more risk there is to critical infrastructure, the greater the perceived need for governments to intervene. If threats to critical infrastructure stem from something as innocuous as unsecured Internet-connected light bulbs, governments may be tempted to regulate in very detailed and prescriptive ways.

All stakeholders, from users to manufacturers to governments, will need to be more security aware and work together towards a more comprehensive and resilient security environment. The insurance industry may exert market influence, for example, by requiring systems or devices to have security certifications in order for their owners to be insurable.

A sustainable and effective long-term solution will require ongoing collaboration, and a commitment by manufacturers and service providers to incorporate privacy and security in their design processes, from initial conception to long-term support and updates. We need to address IoT-related security issues before we can realise the full benefits of the Internet economy.

> Security and trust of the consumer will be the key. With the current technology it is impossible to embed security. Governments worry about this. It is important to have security to have the full potential of the Internet. Security and trust are critical; the public and private sectors should work together. There should be a standard. It's a government challenge.
>
> Government, Asia-Pacific

Related to: Cyber Threats; The Role of Government

IoT, Interoperability and the Future of Internet

Interoperability is fundamental to the success of IoT. Much of IoT's promise is based on the assumption that everything falls into a common structure, with systems and data that are interoperable. McKinsey & Company estimates that "40 percent of the total value that can be unlocked requires different IoT systems to work together".[3] This won't just happen by itself. If IoT standards and Application Programming Interfaces [4] (APIs) are proprietary, especially in the early days of product development, we may not be able to optimise network infrastructure and spur innovation. As Jari Arkko, former IETF Chair put it, "Without interoperability, lights won't work with the switches, sensors can't be read by your smartphone, and devices cannot use the networks around them".[5] As one technologist in Asia predicted, "there may be a certain period of time in which the Internet infrastructure built for IoT will not be optimised due to the lack of interoperability between IoT systems".

> "Everyone loves a networked toaster! But interoperability and security becomes major factors... at least for technologists. Consumers won't care...
>
> Technologist, North America

Interoperability, standards and protocols, and security are all intertwined and essential to the success of IoT. Without them, we face a different kind of fragmentation — where devices and systems simply will not work together. People will hesitate to adopt IoT if it cannot be integrated with other technologies, it is too complex to easily manage, or if they risk being "locked in" to a particular vendor.[6]

> "The pressure to be a leader will mean that companies will rush to bring more and more IoT devices using proprietary/non-standard technologies. To mainstream these IoT devices on the Internet will require localised gateways that can integrate and bridge between the proprietary technologies/devices and the Internet. The proliferation of gateways/bridges between proprietary technology driven IoT devices and the rest of the open, end-to-end Internet, will present new Interoperability challenges to the Internet.
>
> Technologist, Middle East

Iot will make unprecedented demands on communication infrastructure and data storage, requiring significant investments to ensure security and privacy. In some cases, specialised access networks may need to be built to support sensors, for example in smart cities. This will increase demand on networks, energy supply and for Internet addressing. For IoT to work, the migration to IPv6[7] needs to happen, and quickly.

> **Our community is optimistic about ISPs' future ability to supply bandwidth to meet increasing demands. In fact, respondents from Central America, Western Africa, Indian Ocean Islands and the Middle East are confident that today's deficit will shift to a surplus over the next five years.[8]**

Related to: Networks, Standards & Interoperability; The Internet Economy

[3] http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
[4] An application programming interface (API) is a set of protocols, routines, functions and/or commands that programmers use to develop software or facilitate interaction between distinct systems. Source: https://www.techopedia.com/definition/24407/application-programming-interface-api
[5] Jari Arkko, https://www.ietf.org/blog/2016/01/an-interoperable-internet-of-things/
[6] https://www.internetsociety.org/doc/iot-overview
[7] https://www.internetsociety.org/what-we-do/internet-technology-matters/ipv6
[8] Future of the Internet Survey 2 - Question 2: "How well are Internet service providers (ISPs) able to meet the demand for bandwidth in [RESPONDENT'S REGION]"?