OECD publishing

CONSUMER PRODUCT SAFETY IN THE INTERNET OF THINGS

OECD DIGITAL ECONOMY PAPERS

March 2018 **No. 267**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report assesses the consumer product safety benefits and challenges raised by the Internet of Things. It was developed by the Working Party on Consumer Product Safety (WPCPS) as a follow-up to its work on online product safety and as a companion to the work by the Committee on Consumer Policy (CCP) on Consumer Policy in the Smart Home.

The report was prepared by Rod Freeman, international product safety lawyer and partner at Cooley (UK), working with Brigitte Acoca of the OECD Secretariat.

The report benefitted from a financial contribution from the government of Korea. It was declassified by the CCP by a written process that concluded on 2 March 2018.

This publication is a contribution to the OECD Going Digital project, which aims to provide policymakers with the tools they need to help their economies and societies prosper in an increasingly digital and data-driven world.
For more information, visit www.oecd.org/going-digital.
#GoingDigital

Note to Delegations:
This document is also available on O.N.E. under reference code:
DSTI/CP/CPS(2017)7/FINAL

Table of contents

Figures

Executive Summary

There is no globally agreed definition of what is encompassed within the Internet of Things (IoT). The OECD refers to it as *"an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world"* (OECD, 2016[1]). The IoT includes (OECD, 2015[2]):

> *… devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals. This includes laptops, routers, servers, tablets and smartphones, often considered to be part of the "traditional Internet". However, these devices are integral to operating, reading and analysing the state of IoT devices and frequently constitute the "heart and brains" of the system. As such, it would not be correct to exclude them.*

Associated technologies include artificial intelligence, cloud computing, and blockchain. There are four broad categories of consumer goods and services ("products") that rely on IoT technologies. These include wearables, smart home devices and applications, toys and childcare equipment, and connected automobiles. Such products often combine the use of sensors with data collection and analysis to enable autonomous and intelligent systems that can not only interact with each other, but also with people.

The lack of or variation in IoT definitions has made measurement of the market difficult. Available data however seem to suggest that consumer markets for IoT products should continue to grow, spurred by a number of perceived benefits for consumers and businesses alike. For consumers, IoT offers greater product choice, safety, insights into consumption habits and cost savings, convenience and personalisation. For businesses, the benefits include increased possibilities to track and trace products across global supply chains, and assisting manufacturers and other IoT actors in identifying and mitigating risks.

While these technologies could potentially enhance the quality of products and prevent or reduce consumer product safety hazards, they may also present new safety risks, which existing product safety regulatory and liability regimes may be ill-equipped to manage. It is therefore important that consumer product safety is at the front of the minds of policy makers in order to ensure that the full benefit that these technologies have to offer can be harnessed.

There is an argument that the IoT brings new challenges for product safety and that regulatory regimes will need to be adapted. However, there is a counterargument that although the products are new, the issues are not necessarily novel and existing regulations are sufficient. When considering those two approaches, a balance will need to be made between ensuring a high level of consumer product safety, and ensuring that innovation is not unnecessarily stifled, resulting in deprivation to consumers of new technologies that could enhance product safety.

This report does not seek to draw final conclusions or make specific policy recommendations. It is intended to highlight some of the key issues that confront product safety policy makers in this important area, which are as follows:

- To what extent do product safety regulatory frameworks adequately address the product safety risks and challenges associated with the IoT?

- If changes are needed to the product safety regimes, to what degree are changes also required to the product liability regimes?
- Taking into account the complexity of IoT supply chains:
  a. Who should be responsible for safety certification and compliance (both initially and on an ongoing basis)?
  b. How should consumers be able to identify the responsible party(ies)? And
  c. What should be the extent of those responsibilities?

Consumer Product Safety in the Internet of Things

1. Introduction

Despite fading productivity growth in recent years, new digital consumer markets have emerged globally, driven by the development and diffusion of a range of innovative and evolving technology-driven products and production processes. These include the IoT, which is enabled by the confluence of network connectivity, machine to machine ("M2M")[1] interconnection, machine-embedded software, data collection and analysis ("big data"), as well as technology, such as artificial intelligence, blockchain, and cloud computing.

While there is no internationally agreed definition of the IoT, the concept is understood as an ecosystem where devices and other objects are either directly connected to the internet or mediated through local or wide area networks. Such devices and objects include sensors and actuators, which, combined with big data analytics and cloud computing, enable autonomous machines and intelligent systems. The data can be used to analyse patterns, to anticipate changes and to alter an object or environment to realise the desired outcome, often autonomously. As such, the IoT enables interactions not only among devices and objects but also with and between individuals in computer aware environments that can avail themselves of new and innovative services (OECD, 2016[1]; OECD, 2017[3]). A range of actors are involved in the IoT market, including product and sensor manufacturers, software producers, designers, infrastructure providers, and data analytics companies. Available data shows that the IoT market for consumer products is increasing rapidly, spurred by the growing availability of a variety of innovative products, ranging from "wearables" (such as exercise wristbands), to "smart home" applications that link appliances and in-home devices together.

In addition to offering greater product choice and convenience to consumers, the IoT is expected to revolutionise the way product design, manufacturing, and product delivery processes are monitored, analysed and improved, including remotely.

Agencies responsible for product safety policy around the world are increasingly trying to understand the implications of the IoT for product safety. On the one hand, there is interest in the potential for such technologies to give rise to new safety risks, and questions about whether existing liability and product safety regulatory regimes are adequate. On the other hand, there is increasing interest in the opportunities afforded by such technologies to enhance the quality of products, to help prevent consumer product safety hazards or damage, and to create better ways to manage safety in the supply chain and in the marketplace. This, in itself, gives rise to policy challenges, as questions are raised about how liability and product safety regulatory policy can, or should, be adapted to better facilitate the delivery of these benefits to communities around the world.

Ensuring that consumers can benefit from safe IoT-enabled products will be key to building and maintaining trust in this emerging marketplace. Growth will in particular require governments and other stakeholders to enhance cooperation internationally and

assess compliance of the new IoT digital business models with existing consumer product safety policy frameworks (Law 360, 2016). As emphasised by EC Commissioner Jourova and Chairman Kaye, of the US Consumer Product Safety Commission (CPSC) at the IoT plenary of the International Consumer Product, Health and Safety Organisation (ICPHSO) held in Brussels in November 2016, whether and how such frameworks may need to be adapted to meet the realities of the transformative global supply chains, without stifling innovation, will require special attention. This may include reviewing how key consumer product safety concepts (such as "product", "safety", "defect", "damage", and "liability") may be understood in such an environment where: i) products can potentially become defective and unsafe as a result of digital security incidents, and can increasingly take, anticipate, and predict decisions without human intervention; and ii) new means of communicating and gathering data can create new opportunities but also risks to consumers.

This report describes current and emerging IoT developments that may have implications for consumer product safety policy design and enforcement. It contains three sections focusing respectively on: (i) IoT concepts and general trends; (ii) key benefits and emerging consumer product safety risks; and (iii) related policy challenges. The paper is intended to highlight the issues that confront product safety policy makers in this important area. It does not seek to draw final conclusions or make specific policy recommendations; nor does it cover in detail the various IoT policy issues which may have direct product safety implications, but fall outside of the consumer product safety area, such as privacy and security.

2. IoT concepts and trends

The following provides an overview of key IoT concepts and definitions; it also identifies the main IoT product categories for use by consumers, and related market trends.

2.1. Defining the IoT and related concepts

There is no globally agreed definition of what is encompassed within the IoT. It has been broadly described by the OECD as *"an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world"* (OECD, 2016[1]). It includes (OECD, 2015[2]):

> *… devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals. This includes laptops, routers, servers, tablets and smartphones, often considered to be part of the "traditional Internet". However, these devices are integral to operating, reading and analysing the state of IoT devices and frequently constitute the "heart and brains" of the system. As such, it would not be correct to exclude them.*

The IoT is being understood as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes and virtual personalities and use intelligent interfaces and are seamlessly integrated into the information network (Alliance for Internet of Things Innovation (AIOTI), 2015[4]). The IoT has been further summarised as encompassing the following three elements: (1) the "sensors" that collect data about us and our environment (such as smart thermostats, street and highways sensors); (2) the "smarts," which figure out what the data means and how to respond to it. This includes all the computer processors on the IoT devices and, increasingly, in the cloud, as well as the memory that stores all of this information; and (3) the "actuators" that affect the device and the environment; the point of a smart thermostat is for example not limited to the record of the temperature but also to control other devices, such as an air conditioner (Schneier, 2017[5]).

The IoT is often referred to by some as the "third wave" of the internet, following the desktop internet revolution (the first wave) and the connection of people to the internet through their mobile devices (the second wave) (Jankowski, 2014[6])

For the purposes of this report, the IoT is understood as covering consumer products that are connected, or at least have capability to be connected, to the internet, and through such connectivity the behaviour of the products, including, potentially, their safety, can be altered. As the policy implications of the IoT are considered, it is prudent to assume that the categories of products encompassed within the IoT, the technologies utilised, and the ways in which the "connectivity" of such products will be used, is subject to ongoing change and development, likely in ways that cannot currently be predicted.

2.2. Trends in IoT products and markets

This section describes the main IoT-enabled devices and applications used by consumers based on the current state of technology and commercialisation. It also examines the

technologies that support, complement and help to enhance the IoT, and explores recent market trends.

2.2.1. IoT devices and applications

The consumer market currently hosts a great variety of IoT-connected devices and applications. Given that the IoT is still nascent, many more as-yet-unimaginable technologies may be around the corner, which could lead to changes in productivity, environmental impacts, and new products, services, and business models (OECD, 2016[1]). Below are descriptions of several broad categories of current devices on the market, which include: (i) wearables, health monitors, and implantable devices; (ii) smart home applications; (iii) toys and childcare equipment; and (iv) connected automobiles.

Wearables, health monitors, and implantable devices

One of the most important and rapidly developing categories of consumer-facing IoT devices at this point of time is wearables. They are just as they sound: devices, connected to the IoT that are worn by consumers for a variety of reasons. Wearables include the recognisable "smart watches" that are often used in conjunction with a smart phone as well as the more-basic fitness and exercise trackers. They also include devices that reveal knowledge about not only the functioning of the thing itself, but also people and other things it interacts with. This is especially the case with health monitors, which collect and analyse data about an individual's physiology and health. The wearables market also includes a broader set of emerging products, such as spectacle-type glasses that deliver information to consumers, deploy cameras and other recording technologies or, utilising developing technology, operate in the "augmented reality" space. It also includes products that have installed, for example, global-positioning system (GPS) trackers in products, such as shoes, or clothes.

Related to wearables are devices that are ingested by or implanted directly into consumers. Known as the "Internet of Living Things," these devices are being developed primarily for monitoring chronic health conditions like diabetes and heart disease (Information Age, 2015[7]). They can also be used to detect accidents, fits, seizures, or heart attacks and alert emergency services. Furthermore, such devices can gather information about medication-taking, activity, and sleep patterns of patients, as well as measure blood pressure, glucose levels, and heart rates (OECD, 2016[1]). These devices greatly assist physicians in developing and tailoring treatment plans for their patients and also help ensure that urgent-care facilities are reserved only for true emergencies (OECD, 2016[1]; Murray, 2015[8]).

As will be evident from the descriptions above, wearables that have functions related to the health and wellbeing of the consumer may come to be considered medical devices, and subject to specific regulations that exist in most jurisdictions for that class of product. It is beyond the scope of this paper to consider the implications of products that fall within such regulatory regimes, save to note that the "crossover" of wearables into the medical devices field may become more common as wearable consumer products become increasingly higher-functioning and capable of delivering a greater range of data for the consumer.

CCS Insight predicted that the wearables market would reach USD14 billion by the end of 2016, and Business Insider expects the market to total 162.9 million units by the end of 2020 (Meola, 2016[9]). The global market for wearables is estimated to total 230 million

unit shipments in 2018, with a revenue stream of USD32 billion, up from USD10 billion in 2013 (Walker and Roashan, 2015[10]).

Smart home applications

Another important and diverse category of IoT devices and applications is in the home setting[2]. Devices include: smart thermostats that can track energy usage and patterns; smart home appliances that can regulate operations remotely (like ovens that consumers may turn on before arriving home); smart locks and other security systems; sensors to detect flooding, smoke, or carbon dioxide; smart televisions; and "home hubs" that are themselves connected and can provide information to consumers, but can also permit consumers to control through voice commands other home IoT devices like smart lighting, security systems, smart thermostats, and smart high definition televisions.

The "smart home" is a rapidly-developing sector in the IoT, and is significant from a product safety policy perspective as it brings "traditional" household products into this area of new technology. As everyday products, such as whitegoods and small electrical appliances, are developed with technologies that allow them to be "connected" and their functions affected by external inputs, the management of the safety of those products becomes more complicated, and may raise new issues from a policy perspective.

Toys and childcare equipment

This category covers both devices used by children for play, and devices used by their parents to monitor their safety and health.

Currently, advanced children's toys on the market include varieties of dolls and toy creatures that can change their behaviour in order to entertain (such as by remembering answers given by a child, knowing what time it is or giving a weather forecast, and otherwise adapting to the child's responses); construction games permitting children to build programmable gadgets; and specially-designed tablets that have various features permitting children to interact with their environment in different ways (including by uploading photos and documents to personalise) (Telefonica, 2016[11]). However, even more complex and advanced products are being developed. For example, 3D printers designed to enable a child to make their own simple toys in the home are already on the market, with further development of this technology likely.

Related and often overlapping classes of devices are those that monitor a child's safety and health. Some of these devices are simply cameras or microphones connected to the internet for remote monitoring purposes. Others may provide more information, such as a toy containing a sensor that simultaneously relays to the parents information about the child's location, body temperature, and heart rate. Another example is a child car seat that contains sensors to alert parents to their child's physical condition, in the event the child is alone in a car and potentially overheating. The "connected" nature of such products brings obvious benefits to consumers, including a safer environment for children.

Given the vulnerable nature of the target group of consumers, safety considerations are particularly acute in this category. Of the potential concerns that relate to IoT products generally, there are some which come into sharper focus when considered in the context of products used by, and aimed at, children. Data protection and privacy concerns regarding a child's personal data (i.e. who uses it, and who has access to it, and for what purpose) may be more sensitive, particularly where a child may be less aware of the risks

of sharing certain personal data online. These considerations may have genuine safety implications, as well as raising privacy concerns.

More generally, functionality of a toy that enables its performance to be modified through the course of its usable life may raise particular safety implications. For example, new or altered functionality may give rise to the need for fresh instructions to be given to the child, which may therefore require a greater level of adult supervision in relation to the use of the toy generally.

Connected automobiles

Automobiles are increasingly being connected to the internet, for such reasons as providing warnings to drivers of dangerous weather or road conditions, offering real-time diagnostics on the car's condition, and even permitting the vehicle to be operated remotely or autonomously (OECD, 2016[1]). Technologies are also being developed and commercialised that enable a consumer's vehicle to connect with other devices, including with home-based technologies. For example, technology is being commercialised that allows users to control smart home products from their vehicles e.g. triggering custom routine actions (such as dimming lights or lowering the thermostat), showing the status of smoke or security alarms, and causing the garage door to open as the driver nears their home.

The OECD expects that this increased connectivity will dramatically change the global automotive market. Market research suggests that the market share of automated and autonomous cars will rise sharply in the coming decades; Cisco, for example, predicts that it will grow from a market share of 0.1% in 2020 to over 35% by 2040 (OECD, 2016[1]).

2.2.2. Complementary technologies

The IoT also incorporates a range of new technologies that enhance the functionality of products and create new opportunities to provide benefits to consumers and even create new markets for products that did not previously exist. This includes technologies such as artificial intelligence, blockchain, augmented reality and virtual reality. These technologies both complement and enhance the IoT, as discussed below.

Artificial intelligence

There is no globally accepted definition of artificial intelligence (AI). At the OECD's 2016 Technology Foresight Forum, participants defined AI as the capability of a computer programme to perform functions usually associated with intelligence in human beings, such as learning, understanding, reasoning and interacting, in other words to "*do the right thing at the right time"* (OECD, 2017[12]).

AI undoubtedly has implications for many aspects of human life, the full extent of which is beyond the scope of this report. As is relevant here, AI is often identified with the second basic element of the IoT: the "smarts" that decide how to interpret and act on the data transmitted by a device or application. Current AI applications include machines understanding human speech, competing in strategic games, driving car autonomously, or interpreting complex data (OECD, 2017[12]). Less obvious AI applications include credit card payment checking, spam filters, electronic personal assistants, GPS navigation systems, search engines, spell and grammar checkers, and robotic devices like vacuum-cleaner robots.

The rate of progress made in this field has increased rapidly. Automated perception, including vision, is already at near human-level performance, and advances in perception will be followed by algorithmic improvements in higher level reasoning capabilities, including planning or predicting danger (Stanford University, 2016). For example, an autonomous vehicle may be able to detect a ball bouncing on a street, recognise that this ball could be followed by a child, plan for this situation in case it happens and adjust its decisions accordingly (The Engineer, 2017).

The development of AI has enormous potential for the management of consumer product safety. "Smart" products, with capabilities to "learn", can be designed to adapt to consumer behaviour. At least in theory, this could mean that such products could come to detect patterns in consumer behaviour that may not have been fully anticipated by the designer of the product, and which may create a safety risk. In such cases the "smart" product could adapt its own performance in order to reduce or minimise the risk, thereby creating higher levels of safety.

AI can also be developed and deployed to enable companies to more effectively deal with post-market surveillance, by: i) helping to identify potential risks based on inputs from a wide range of data sources, including usage-related data sourced from the products themselves, as well as other sources, and ii) processing that data to help identify solutions.

Blockchain technology

Blockchain is a technology permitting untrusted parties to coordinate themselves on a peer-to-peer basis without the need to rely on any trusted third party because the parties instead trust that the underlying technological infrastructure will operate as planned (OECD, 2017[12]). The best-known example of blockchain technology is Bitcoin.

Blockchain technology can be understood as a decentralised and distributed ledger system that facilitates economic transactions and peer-to-peer interactions without the need for any trusted authority or intermediary sponsor. Blockchain technology allows parties to store and manage data through a network run on software logic rather than a centralised operator. Networks constructed in this manner are inherently append-only, which makes them tamper-resistant because such appended data cannot be subsequently deleted or modified by any one party. Data added to the blockchain is authenticated, time-stamped, and stored chronologically by the network. In the context of the IoT, blockchain technology has the potential to allow devices to communicate directly with one another and exchange value without passing through an intermediary (OECD, 2017[12]). For example, a washing machine connected to the IoT could detect that it is out of detergent and use blockchain technology to order and pay for new detergent. In addition, the potential benefits of blockchain technology to product safety are not hard to imagine – the ability to track and trace products through the supply chain could have resounding effects in the area of corrective actions and recalls, assisting companies to locate and trace affected products.

New and emerging projects using blockchain for the purposes of enhancing product safety are also being developed. These include Microsoft's Project Manifest, which includes sponsors like Mojix, Amazon, FedEx, Target, and Home Depot, and aims to track and trace a range of products (from auto parts to medical devices) through their supply chain. One aspect of this project involves a concept that would trigger "smart contract"[3] functions when certain actions occur (e.g. shipment of goods, receipt by retailers) (del Castillo, 2017[13]). Additionally, GS1 (a non-profit global business

communication standards company) has recently announced collaborative efforts with IBM and Microsoft to integrate its standards for identification and structured data into supply-chain based blockchain applications, with the intention of increasing data integrity and reducing data duplication and reconciliation (Nation, 2017[14]; GS1, 2017[15]).

The benefits of blockchain technology could therefore go further: assisting consumers and businesses alike by improving transparency in the supply chain and allowing participants to view and share information swiftly and confidently, and possibly bringing new angles to various issues facing actors in supply chains across the world, including for example the "country of origin" labelling or reliability of certifications.

Augmented and virtual reality

Technologies that enhance, alter, or completely change a consumer's perception of his or her surrounds—such as augmented and virtual reality—have the potential to revolutionise how consumers experience the world.

Augmented Reality refers to a class of technologies that collects information about the real world, processes that information in real time, combines it with useful contextual information, and permits users to experience computer-generated elements—such as images, video, text, or sound—superimposed over real-world environments using mobile or wearable sensory devices. Augmented reality differs from virtual reality as it is a combination of real-world and computer-generated elements (Tech Policy Lab, 2015[16]; Goldman and Falcone, 2016[17]; Inside Counsel, 2017[18]; Live Science, 2016[19]).

Augmented reality applications already in daily use include real-time traffic navigation programs, entertainment and gaming systems, educational programs (such as astronomical and wildlife overlays), and ratings applications that provide reviews for local businesses (R Street, 2016[20]). Future augmented reality applications could assist the disabled by describing television and movie scenes for the blind or overlaying subtitles for the deaf.

Virtual reality is a class of technologies permitting users to experience and interact with a wholly immersive digital world using sensory devices. Virtual reality differs from augmented reality in that Virtual reality entirely blocks the outside world (Goldman and Falcone, 2016[17]; Live Science, 2016[19]).

Virtual reality is presently seen primarily in gaming systems and may soon be utilised in a wide range of other applications, for example in supporting therapies to help paraplegics, stroke victims, and those with post-traumatic stress disorder and cerebral palsy cope with their conditions (R Street, 2016[20]; Reed Smith LLP, 2017[21]). Both augmented and virtual reality also have the potential to teach people to drive, or train people to perform historically-risky jobs like welding or surgery.

Consumers currently experience these technologies largely through their mobile phones and tablets, and specialised devices such as gaming consoles, but companies are researching new devices such as augmented reality earbuds, contact lenses, and other wearable devices. Ultimately, some market observers believe that there is a *"sense that phones and tablets will get replaced"* as companies drive toward the goal of convenient and natural immersion (Live Science, 2016[19]).

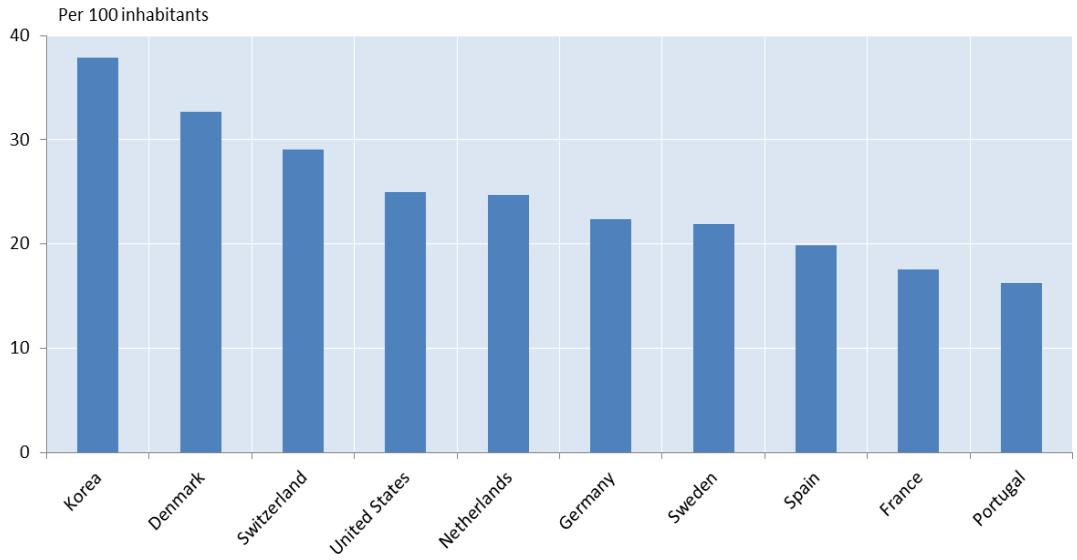
2.2.3. Market size and growth

In order to be in the best possible position to assess what is the appropriate policy response to the development of the IoT and any consumer product safety issues arising, it is important to understand the size of the consumer market for connected devices, and to assess how it is likely to develop. How to measure the market is directly linked to how it is being defined; yet, as discussed above, *"[m]easuring the growth of the Internet of Things is not a simple task because the IoT does not have clear boundaries"* (OECD, 2016[1]). As a result, different metrics have been adopted to measure and forecast the consumer market for connected devices, as reflected by the data below, which are difficult to compare to one another, and also likely include connected devices and applications that are outside the scope of the consumer market (such as devices and applications for infrastructure and industrial uses). Despite such lack of comparability, available data suggests that the market is growing in leaps and bounds. Available estimates suggest that in addition to growth in the number of devices that will be connected to the internet in the coming years, the value of the IoT marketplace should increase rapidly (OECD, 2016[1]). Such growth should be enabled by a number of factors, such as: process efficiency, customer service, speed of decision-making; cost savings; consistency of delivery across markets; transparency/predictability of costs; and performance in new markets.

Connected devices and applications

One useful way to measure market growth is the increase in connected devices and applications in general use. Because *"[e]fforts to develop metrics are still in their infancy"*, the OECD has collected data from regulatory authorities on M2M subscriptions and regards this metric as *"[o]ne of the most accurate measurements though not complete"* (OECD, 2016[1]). Between 2012 and the end of 2016, these data showed that the number of actual M2M SIM cards in use in tracked countries grew from 72 million to 149 million (OECD, 2017[22]).[4] Another source (Shodan, the world's first search engine for Internet-connected devices), provides a snapshot of the top 10 countries with the largest numbers of IoT devices connected to the internet per 100 inhabitants (Figure 1). Shodan has found that there are 363 million connected devices currently around the world, with 84 million in the People's Republic of China, 78 million in the United States, 18 million each in Korea, Brazil, and Germany, and 8-10 million each in Japan, Spain, the United Kingdom, and Mexico.

Figure 1. Devices online per 100 inhabitants, top OECD countries



Note: Last updated: 29-May-2015.
Source: (OECD, 2015[2]), using data from Shodan.

Other organisations suggest even more dramatic growth. The European Commission (EC) predicts that the number of IoT connections within EU Member States will rise from about 1.8 billion in 2013 to almost 6 billion in 2020 (Cartwright, 2017[23]). Projections from Cisco show that by 2021, the number of mobile devices and connections will grow to 11.6 billion, with 8.3 billion handheld or personal mobile ready devices and 3.3 billion M2M connections (Cisco, 2016[24]). Ericsson forecasted that there would be 16 billion connected things globally in 2016 and that the number would reach 29 billion by 2022, including cars, machines, meters, sensors, point-of-sales terminals, electronics and wearables with this increase being driven by *"an increasing range of use cases and business models, and supported by falling device costs"* (Ericsson , 2017[25]).

Market sales and projections

Another helpful measure is the amount of money spent by consumers in the IoT market. The International Data Corporation estimates that the market value of the IoT will reach USD1.29 trillion in 2020 (IDC, 2017[26]). McKinsey estimates that in 2015 the size of the IoT market was USD900 million but that it will grow to USD3.7 billion by 2020 (McKinsey, 2016[27]). This growth could generate a potential impact of USD11.1 trillion a year in economic value by 2025 if policy makers and businesses overcome crucial technical, organisational and regulatory hurdles (McKinsey, 2015[28]). General Electric estimates that by 2025 this "industrial internet" will touch 43% of the global economy spanning across the engines of global economic growth: energy, healthcare, transportation and manufacturing (Marco Annunziata and Economist, 2015[29]).

The market for complementary technologies is also a useful metric for estimating the overall impact of the IoT. The Analysis Group estimates that, if augmented and virtual reality are fully adopted by 2020, it could impact the global economy by as much as USD126 billion (R Street, 2016[20]). Other analysts predict that the combined market will be USD162 billion by 2020, with augmented reality accounting for most of the growth

(Inside Counsel, 2017[18]). Bank of America projects that the virtual reality industry alone could be valued at USD150 billion, with more than 300 million users, by 2022 (R Street, 2016[20]).

3. Consumer Product Safety Benefits and Risks in the IoT

This section describes the benefits that the IoT may bring to consumers and businesses alike. It also identifies key emerging risks that have accompanied the spread of IoT, which are likely to be magnified by the increased complexity of today's global supply chains.

3.1. Benefits of IoT

The IoT has the potential to deliver significant benefits to consumers. This includes the potential to better manage consumer product safety, and thereby to deliver greater levels of consumer protection.

One of the more obvious benefits is that IoT-enabled devices and applications make consumers' lives easier and less prone to risk, and aim to promote efficiency and sustainability. For example, an IoT-connected thermostat permits a consumer to remotely adjust the environmental controls of his or her home, thereby reducing the unnecessary consumption of energy during times when the consumer is not there. Not only does this benefit the consumer through lower energy bills, but it also benefits society through a reduction in wasted energy resources. Furthermore, the ability of manufacturers to remotely modify IoT devices and applications means that these products have the potential to be upgraded even after they are acquired by consumers. For that reason, the same connected thermostat may gain improved performance or even entirely new features over the course of its life in the consumer's home (OECD, 2016[1]).

There are also benefits to IoT-connected devices and applications that have the potential to make them safer to use. A feature of being connected to the IoT is that such a product can warn responsible parties about unsafe conditions and permit these problems to be addressed before a negative outcome occurs. Car seat sensors working via Bluetooth may, for example, be used to prevent parents from leaving their children on their own in a car, through an alert via their smartphone. If the problem is severe or cannot be rectified remotely, manufacturers can also initiate recalls in a timely and effective manner. Thus, in the same example above, an IoT-connected thermostat may be remotely monitored by the manufacturer or a third party for problems. Then, if a problem arises, the consumer can be notified immediately of the issue and, if necessary and possible, the device's software could be updated or patched. And if the thermostat cannot be fixed remotely, the product could be recalled.

Manufacturers may also make use of technologies that form part of IoT to track and trace their products through the supply chain. At a general level, manufacturers can identify and mitigate risks to their supply chains, and thereby avoid situations that previously would have caused their incoming raw materials and supplies or outgoing finished products to be lost or delayed. Manufacturers can also trace individual products or batches in the supply chain and, in conjunction with blockchain technology and related "smart contracts," ensure that the product complies with regulatory requirements and automatically receive payments when the product is delivered (Iansiti and Lakhani, 2017[30]). A "smart contract"[5] is one that triggers an action (such as the transfer of money) when negotiated conditions are met. For example, if a "smart contract" called for the release of a payment upon the delivery of a batch of IoT-connected products, the manufacturer could use the IoT to identify a batch that complies with the purchaser's

local regulations, direct it to be sent to the proper location, and automatically receive the payment when the purchaser logs in a blockchain that it was received. With the IoT, manufacturers can both ensure compliance with local laws and eliminate or reduce otherwise-expensive costs of doing business, such as traditional business structures like intermediary accountants and lawyers.

3.2. Potential product safety risks

Along with the above benefits from IoT devices and applications come potential risks related to consumer product safety. To date, there has been limited consumer reporting of IoT device and application safety incidents, possibly due to the fact that the market is new and quite complex. Consumers may not have fully embraced IoT devices and applications or, if they have, the complexity of the market may leave them uncertain about which party to contact to resolve problems. In 2017, however, the US Consumer Product Safety Commission identified a number of categories of potential product safety hazards, including: a loss of the product's safety features through malfunction or a change in performance due to software updates, a loss of connection to the internet and a corresponding loss of function, the corruption of data used to support a safety feature, and potential physical harms from wearable IoT devices and applications (Consumer Product Safety Commission (CPSC) (US), 2017[31]). Other sources have developed and enlarged these categories as discussed below.

3.2.1. Malfunction by defect or update

An IoT device or application could malfunction, either from a defect that existed when the product was sold, or even by a newly-released update or patch from the manufacturer. The ability to update software after an IoT device or application has left the manufacturing facility creates both opportunities and risks. For example, a device that is found to be defective because of defective software could be rendered non-defective by way of an update pushed out over the internet if the device is connected. At the same time, an otherwise non-defective device could be rendered defective by a software upgrade that is itself defective. If an application malfunctions, it could cause a device to act or react in an unanticipated, and potentially unsafe, manner. Additionally, an application being hacked by a wrongdoer could also impact the safety of the device, if such a hack were to, for example, speed up or slow down the appliance causing mechanical failure or overheating (CertifiGroup, 2016[32]).

The complexity goes deeper: software modifications can directly affect the functioning of the device or application, or they can indirectly create a malfunction if the device or application necessarily works with other technology and the update disrupts its ability to do so. Such a defect might manifest by inadvertently disabling a safety mechanism or another technology connected to a safety device, or by causing the IoT-connected device or application to operate in a manner contrary to the safe operation of complementary devices, applications, or technology.

3.2.2. Loss of connectivity and product obsolescence

A second risk comes in the form of loss of connectivity, which might prevent the IoT device or application from operating correctly. If the product is dependent on connection to the IoT in order to function safely, this could have potential safety implications if the product is not designed to have a "fail safe" in the event that it loses connectivity. The issue will be more acute where the device itself has a protective function, intended to

eliminate or mitigate a risk (e.g. a home security system), such that the mere failure of that protective system to operate properly will itself give rise to a safety risk.

Concerns have also been raised about the use of the IoT from a "planned obsolescence" perspective (i.e. companies using the IoT to render older products obsolete or slow so that consumers are forced to buy newer versions). This is not unique to IoT devices, as it has been raised in respect of products such as microwaves and cars in the past, but the IoT would theoretically increase a manufacturer's control over their ability to "end" the life of a product at a particular time. However, the ability to do so could also assist manufacturers in preventing users from continuing to use products that are unsafe and/or pose risks to the consumer. The development of connected devices, supported by other technologies, therefore provides greater opportunities for manufacturers to deal with safety at the end of the product's life, thereby better ensuring safety throughout the full product life cycle.

3.2.3. Data quality and integrity concerns

Another hazard is the quality and integrity of the data used to support a safety function. To the extent the safety feature relies on certain data, it is imperative that the data be accurate and uncorrupted or the safety feature may not function.

Data quality especially is an emerging problem with the IoT, specifically when the data used by automated decisions comes from third-parties without a reliable reputation, or the data lacks attribution or provenance information (McAfee, 2013[33]). For example, barcodes are useful as machine-readable numbers identifying a manufacturer or a product, but the ways in which many third-party applications access meta-data is often unclear and thus the information relayed by a barcode could be incorrect. Just as if data is corrupted, if meta-data is incorrect or misleading, it may cause IoT devices and applications to behave unexpectedly or unsafely. As previously mentioned the benefits of blockchain technology may well bear fruit in this area and help manage some of the issues: data and information stored in a blockchain is far less, if at all, susceptible to hackers and corruption due to its de-centralised nature.

Similarly, there may be dangers when an IoT-connected device operates in conjunction with an augmented-reality application. In one possible scenario, the combination might mis-identify an object in the real world and thereby cause a human to act contrary to his or her own safety. This may be the case, for example, in the event where the technology causes a repairperson to mistakenly replace a broken car part with the incorrect spare and the mistake harms a driver or bystander (Tech Policy Lab, 2015[16]; R Street, 2016[20]).

Digital security is, therefore, a significant issue for product safety policy as the IoT continues to develop. This goes well beyond issues of consumer privacy, as the maintenance of data integrity can be critical to ensuring the safe and proper functioning of products.

Both the United States' Federal Trade Commission (US FTC) and the European Parliament have expressed their concerns in relation to potential digital security implications from a product safety perspective. For example, the US FTC (2015[34]) published a report which noted that (among other risks) "*unauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases*". The US FTC proposed several recommendations, including that companies should build digital security measures into their devices at the outset, ensure that their personnel practices promote good digital security, find and provide oversight to capable service

providers, implement multiple layers of security measures, limit access to devices from unauthorised users, and monitor products throughout their lifecycle in order to patch known vulnerabilities (Federal Trade Commission US, 2015[34]).

3.2.4. Physical dangers

IoT devices and applications in, on, or near the body, such as wearables, have the potential to physically injure consumers. The US CPSC (2017[31]) identified a number of potential hazards in this category, including: hearing loss from an implanted audio device that malfunctions or plays signals from another source, chemical or thermal burns and skin irritation from leaking or faulty batteries or other reactive materials in the device or application, or even muscle strains from powered exoskeletons moving beyond the natural range of a person's motion. Augmented and virtual reality devices may also cause eyestrain, eye trauma, eye-development issues, or motion sickness (R Street, 2016[20]). In more extreme cases, these devices may even cause epileptic seizures (Reed Smith LLP, 2017[21]).

Additionally, IoT-connected devices could distract consumers, or users could rely on information provided by such a device in error, and injure themselves or third parties as a result (Tech Policy Lab, 2015[16]). For example, a car equipped with a heads-up display operating an augmented reality application could replace a stop sign with a virtual advertisement and thereby cause an accident. Or a user could injure him or herself simply by tripping over a real-world object while immersed in an augmented or virtual reality and falling (R Street, 2016[20]). Consumers could also damage property using IoT-connected devices, such as by manipulating sensory devices equipped with augmented or virtual reality without sufficient real-world physical space to accomplish the desired motion (Reed Smith LLP, 2017[21]).

The European Parliament has expressed concern in relation to the potential physical safety implications of the increase in robotics, as part of its recommendations to the Commission on Civil Law Rules on Robotics (2015/2102(INL)). For example, humans may be exposed to physical dangers *"when a robot's code proves fallible"* or the *"potential consequences of system failure or hacking of connected robots and robotic systems at a time when increasingly autonomous applications come into use"* (e.g. dangers involving robotic vehicles, care robots or robots used for maintaining public order).

4. Policy challenges: Rethinking product safety and product liability laws

The mere fact that a new product technology might present risks to consumers does not, itself, create a need for a policy response. In an increasing number of countries around the world, consumers are generally well-protected by robust product safety laws, regulations and standards that cover a broad range of risks. In most countries, those safety rules and regulations are supported by legal systems by which consumers who are injured by unsafe products may obtain compensation from the manufacturer or seller responsible for putting that product on the market. It may be that those existing product safety and product liability regimes are well adapted to dealing with the challenges presented by new technologies, including those related to IoT. In its 2015 report, the Alliance for Internet of Things Innovation (AIOTI) concluded that although there are certain special considerations in the areas of product compliance, product liability and insurance related issues for certain IoT products, there was not a clear need for new legislation or new regulation ([4]). Given that many of the product liability risks highlighted are not unique to IoT products and platforms, it was considered that careful thought and dialogue should take place before making any amendments to the existing regime, and that the goal of achieving consumer safety should be balanced with the need to stimulate innovation in the IoT market (Alliance for Internet of Things Innovation (AIOTI), 2015[4]). This is not a new concept, as it has long-been the challenge of product regulatory regimes to ensure that they are sufficiently adaptable to support appropriate technological development. The main new challenge in the era of the IoT is the sheer pace of technological development, which puts strain on any regulatory regime to adapt with sufficient speed and foresight to maintain protection of consumers whilst allowing the benefits of technology to be realised.

This section summarises three main policy challenges raised by the adoption of IoT, and the potential implications these challenges have on global product safety and liability laws and regulations (both of which are considered in turn below). The three policy challenges are:

- The impact of IoT on the distinction between “hardware” and “software”, “products” and “services”.
- The question of who is responsible for the safety of products, what is the extent of responsibility, and how is liability allocated in the event of failure; and
- Communicating safety to consumers.

Examples of how governments and other stakeholders across the globe are dealing with these challenges, as revealed by initiatives, recent litigation and enforcement actions from various jurisdictions are included throughout. As a start, a good illustration of the complexity of the task facing governments and regulators alike comes from the US CPSC, which stated that each IoT-connected device or application must be considered as unique, and that there will likely be no “one-size-fits-all” approach to regulating the IoT (American Bar Association, 2017[35]). Collaboration with consumers and industry will be key to this approach. It will also be important that there be a high level of co-ordination between policy makers around the world. Intrinsically, the IoT transcends geographical and political borders. Also, markets for such technologies are increasingly global. In order to harness the full potential of IoT technology, international co-ordination is needed

to avoid inefficiencies, and to ensure a consistent experience for consumers, including in the protection of their safety. Indeed, some commentators have called for the creation of a new international organisation to regulate IoT; operating across borders and consisting of, in contrast to the regulation of the internet, a *"multipolar decentralized policy institutional setting, considering the needs of all stakeholders involved, managed by several entities"* (Weber, 2009[36]).

4.1. The interplay between "hardware", "software", "products", and "services"

The typical components of IoT devices include hardware, software, and communication protocols/standards. At a general level, "hardware" in this context may be considered to be a device or set of devices or physical objects which are responsive in nature, and have the capability to retrieve data and follow instructions. "Software" is the set of programs which enable the data collection, storage, processing, manipulating and instructing to and from hardware components. The IoT has generated further opportunities in the hardware and software space, whereby users can access "smart" data and control the system remotely, and whereby devices can autonomously "learn" from inputs not necessarily controlled by the product designer or user.

Typically, product safety regulatory and liability regimes draw a distinction between the supply of "goods" and the supply of "services", with each scenario being regulated differently. In the technology sector, that distinction has led to debate and legal controversy around the distinction between "hardware" and "software", and in particular in relation to whether software ought to be considered a "good" and therefore subject to product safety and product liability regimes (Alliance for Internet of Things Innovation (AIOTI), 2015[4]). The IoT does not obviously raise entirely new issues in this regard. However, IoT brings a greater level of complexity in the interaction between hardware and the software that drives it, with the behaviour of products in many sectors being increasingly dependent on changeable software and data that resides both in the product, and external to it.

These factors do not necessarily change the fundamental analysis of the distinction, but it potentially makes the need for a clear distinction more acute, and therefore a greater challenge for policy makers and enforcers. Because an IoT device or application can be a mix of goods and services, the extent to which product safety and product liability laws apply may be difficult for courts or product safety agencies to determine. For example, existing product liability regimes may not capture the action of *"providing data through an IoT system"* as it is considered a service (Medium, 2017[37]). In some jurisdictions (such as Austria, Germany, and Switzerland), the courts have treated digital content products in general in the same manner as goods; however, others, such as in the United Kingdom, draw a distinction between software supplied on a tangible medium, such as a CD, and software supplied via an intangible medium, such as software downloaded from the internet. The former is seen as a sale of goods, whereas the latter is not (OECD, 2013[38]). This has important implications for consumer rights and remedies as a sale of goods is generally afforded greater legal protection than the provision of services. If a consumer is damaged by a defective good, they generally have a right to have the product replaced, receive a refund or claim damages for loss. However, the same rules may not apply if the "thing" that damaged the consumer is considered as "service", in which case the consumer may need to rely on less protective principles in order to claim damages.

In the product liability context, these questions are especially important because various jurisdictions, such as the European Union and the United States, have enacted "no fault"

or strict liability regimes to govern product liability claims (Alliance for Internet of Things Innovation (AIOTI), 2015[4]).

Further, the intersection of hardware and software in IoT connected devices and applications presents unique opportunities as well as challenges from the perspective of the protection of consumer safety. Traditionally, a hardware developer would aim to release a final and perfect version of a product to try to avoid a number of negative potential consequences that can arise in the event of a defect. Software developers have had an ability to take a new product to the market with the knowledge that if any defects are discovered, a remedy is likely to be easy to deliver by way of a software patch, with little or no interruption for the consumer (and in some cases without their knowledge), in circumstances where consumers, and their software, are easily traceable. In the event a product is defective, manufactures could use blockchain, for example to better trace and identify the defect and allow for more effective corrective action.

The development of IoT products marks the arrival to the market of a wide range of products that sit in the middle of these two traditional positions. The fact that the performance and functionality of such products are increasingly controlled by software means that unexpected defects are increasingly likely to be software-based (or at least remedied by software), such that defects can be rectified remotely with little disruption to consumers. These new complexities give rise to interesting and potentially important policy questions when it comes to consider how responsibility to ensure product safety should be addressed, and how liability should be allocated in the event that a product causes injury.

4.2. Responsibility and liability

As emphasised in the revised 2016 OECD Recommendation on Consumer Protection in E-commerce ("the OECD E-commerce Recommendation"), identifying *"the appropriate allocation of responsibility for the protection of consumers among relevant e-commerce actors is key to promoting consumer welfare and enhancing consumer trust"* (OECD, 2016[39]). Traditional notions of product safety and liability may not, however, map cleanly onto the new world of IoT-connected devices and applications. As discussed above, these products may become defective and unsafe in a myriad of ways, such as through a data breach, or because a third-party device or application has malfunctioned. Furthermore, the devices may rely on uninterrupted connectivity, without which the safety of the device could become (or remain, if the device is defective and awaiting a software update to fix that defect) compromised. Powered by AI, these devices and applications can further take, anticipate, and predict decisions without human interaction. Therefore, it is possible that consumer product safety regulations and standards, and liability rules, may not effectively address the resulting product safety issues.

4.2.1. Who is responsible for the safety of products?

For example, if third party software embedded in a product is not defective when first marketed but, as a result of an update by the third party, the product develops an unexpected product safety risk, it may not always be clear which party is responsible. Matters may be even more complicated when the performance of a product is influenced or controlled by data produced through AI. Because AI relies on large amounts of data from a wide range of sources, it may be difficult or nearly impossible for any of the parties to understand why a product acted in the manner that it did.

At a product safety compliance level, given the high level of integration between devices and applications and the complexity of the IoT ecosystem, it may be difficult to determine initially who should certify the safety and compliance of the product, the extent of the certification that is required, and for how long that party is responsible for the safety of the product. Indeed, the EC has flagged these issues as being particularly problematic in their report on "Advancing the Internet of Things in Europe" (European Commission, 2016[40]). These questions are not new, and are not unique to the IoT, but again the complexity of IoT technology, and the greater extent to which products are controlled by software and data, brings these questions into sharper focus from a policy perspective.

A complicating factor, therefore, is that IoT devices and applications are generally, by the nature of their design, dependent on third party technology to perform their basic functions and maximise benefit to the consumer (Alliance for Internet of Things Innovation (AIOTI), 2015[4]), and the performance and the safety of a product may be altered by inputs from third parties after the product has been placed on the market (potentially in circumstances well beyond the knowledge or control of the manufacturer). This has come to the attention of regulators in the United States. For example, the US CPSC (2017[31]) has stated that it will focus on *"not only the products [operating] safely, but [that] the products also do not adversely affect the operation of other devices"*. Moreover, these interdependencies may increase and become ever more complex over the life of the device or application.

Beyond that, questions also arise as to the extent to which a supplier of hardware or software should be responsible to ensure the product is protected from a digital security attack on an ongoing basis. This can become particularly challenging in a world in which cyber-criminals are constantly devising new ways to unlawfully access data in order to commit their crimes, forcing those who create the products to continue to develop patches and protections to ensure the ongoing protection of the products in the field.

4.2.2. How may liability be allocated?

Overlapping the product safety considerations is the question of how to allocate liability to pay compensation in the event that a defect or fault in a product causes damage. This overlap is important, because inefficiencies will be created if product safety policy develops in such a way that there are differences between the product safety regime and the product liability regime (i) in respect of identification of the parties responsible for safety and compliance, and the extent of those responsibilities; and (ii) in respect of the question of what is an acceptable level of safety.

The interdependency of goods and service producers, actors and consumers in the IoT ecosystem means that liability could be difficult to allocate as there are challenges in *"identifying the root cause of product failures"* (European Commission, 2016[40]). For example, in the context of a car accident involving an autonomous vehicle, a number of IoT actors may be wholly, or partially responsible for the accident; these may include the application determining the movement of the car, the manufacturer of the sensors, the operator of the sensor network, the road operator, and the third party that provided the software (Medium, 2017[37]).

To prove his or her claim, a consumer must ordinarily show the defect, the damage, and that the defect caused the damage. Different jurisdictions have established different tests for these elements. For example, to prove a defect, both the European Union and the United States apply variants of a "reasonable expectation" test, where a court compares the offending product to how a consumer would have expected such a product to behave.

But even with such a general test, specific application can vary widely even within a jurisdiction, such as between Member States in the EU or states in the US. Product liability regimes may also provide a manufacturer defences (such as proving that its product was the "state-of-the-art" at the time it was marketed), as well as limit liability to only certain categories of damages, such as death, personal injury, or damage to other property. All of the points above create challenges for accurately and efficiently allocating liability in the event of a defective product.

These questions are under active consideration in some jurisdictions and regions. For example, the EC is currently conducting a review of the EC's Product Liability Directive, with an express focus on whether its provisions, which have remained largely unchanged since 1985, continue to remain fit for purpose taking into account the challenges of new technologies (European Commission, 2016[41]). Based on submissions received by the EC through a public consultation on the topic, approximately half of those who responded to the consultation believed that the Directive needed to be adapted for innovative products (European Commission, 2017[42]).

The European Parliament is also involved in addressing the problem of apportionment of liability in IoT. In February 2017, its Members voted to ask the EC to urgently propose rules on robotics and AI in order to clarify liability issues.

Some have suggested that some of these questions of liability for manufacturers and other stakeholders in the product chain could, perhaps be dealt with by an insurance-based solution whereby stakeholders would "pool" risk and collectively insure IoT connected devices and applications. In its annual SONAR report, Swiss Re (2017[43]) considered the possibility of a new legal personality for "electronic persons". This may seem farfetched, but could provide a "simple focal point" to pursue in the event of a product liability dispute, particularly if coupled with a strict liability regime and compulsory insurance, rather than the complex issue of determining liability in the event of an autonomous vehicle accident – would it be the driver, vehicle manufacturer, software, and/or data provider (Kidman and Turner, 2017[44]). However, this discussion highlights that questions of allocation of responsibility for compliance, and for liability in the event of injuries, is a complex one that raises particular policy considerations in an IoT context.

Given these challenges, a fundamental question arises as to whether existing product safety and liability regimes around the world are fit for purpose in the era of the IoT. On the one hand, it might be said that the IoT does not necessarily raise issues that are entirely new. It is not uncommon for products to be sold that can be adapted or modified by third parties, or even by consumers themselves. On the other hand, it might be said that, for the reasons described above, existing regulatory and liability regimes may need to be adapted to adequately deal with these new concepts and challenges. These are important questions for policy makers. Failure by policy makers to identify and introduce any necessary adaptions could lead to the rapid commercialisation of categories of products without adequate supervision over safety and performance, such that consumers would face increased risk. When considering those two approaches, a balance will need to be made between ensuring: i) a high level of consumer product safety in the IoT, and ii) that innovation is not unnecessarily stifled, resulting in deprivation to consumers of new technologies that could enhance product safety.

4.3. Communicating safety to consumers

Throughout the IoT, product manufacturers and suppliers have unprecedented capabilities to connect with the consumer base of users more quickly and effectively, especially in the case of a product recall. Typically, the consumers' interaction with IoT devices is supported by an app or a software-based service remote from the device, which gives the company responsible for controlling the software a unique ability to connect with the active user of the product, whether or not that user is the original purchaser of the product.

Through these means, it is to be expected that there are unique opportunities for product suppliers to communicate important safety information to consumers, both at the time the product is first activated, and through the entire lifecycle of the product. This might include communication of safe installation and setup instructions, ongoing reminders about safe use as the product is in use, updates on safety instructions as new data comes into the hands of manufacturers, information about product recalls or safety modifications, and timely information about maintenance requirements and end-of life issues.

The challenge for policy makers lies, first, in ensuring that regulations and enforcement practices are sufficiently flexible to encourage the use of such technology in this way to enhance safety. By way of example, the most recent revision of the European Commission's "Blue Guide" on interpretation of EU product safety regulations included for the first time a reference that suggests that safety warnings must always be delivered to consumers in paper form accompanying the product (European Commission, 2016[45]). In the era of the IoT, this guidance already seems out of date, at least for products where there are much more effective ways to deliver critical safety warnings and instructions to consumers.

More generally, as discussed above, these capabilities give rise to questions about the extent of responsibilities of economic operators who are responsible for the development and marketing of IoT products, in relation to the ways in which safety information is communicated, the timing of such information, and obligations in the event that unexpected safety issues arise.

References

Alliance for Internet of Things Innovation (AIOTI) (2015), *Working group 4 Report on Policy Issues*, https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf. [4]

American Bar Association (2017), *Consumer Product Safety Administration seeks collaboration in managing internet of things*, https://www.americanbar.org/news/abanews/aba-news-archives/2017/05/consumer_productsaf.html (accessed on 13 October 2017). [35]

Annunziata, Marco; (2015), *The Moment For Industry*, http://gereports.cdnist.com/wp-content/uploads/2015/09/29153350/Annunziata_Moment-for-industry_Final1.pdf (accessed on 12 October 2017). [50]

Barboutov, K. et al. (2017), *Ericsson Mobility Report*, https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf (accessed on 12 October 2017). [49]

Business Insider (2016), *Wearable technology and IoT wearable devices*, Business Insider, http://www.businessinsider.fr/uk/wearable-technology-iot-devices-2016-8/ (accessed on 12 October 2017). [56]

Cartwright, J. (2017), *Product liability and the internet of things | Charles Russell Speechlys*, https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/commercial/2017/product-liability-and-the-internet-of-things/ (accessed on 12 October 2017). [23]

CertifiGroup (2016), *www.CertifiGroup.com Experts in UL, CSA, CE & International Regulatory Compliance*, http://certifigroup.com/whitepapers/product-safety-and-iot.pdf (accessed on 12 October 2017). [32]

Charles Russell Speechlys (2017), *Product liability and the internet of things |*, https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/commercial/2017/product-liability-and-the-internet-of-things/ (accessed on 12 October 2017). [68]

Cisco (2016), *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update*, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf (accessed on 12 October 2017). [24]

Cisco (2017), "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update The Cisco ® Visual Networking Index (VNI) Global Mobile Data Traffic Forecast Update", https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf (accessed on 12 October 2017). [69]

CNET (2016), *Virtual reality doesn't mean what you think it means - CNET*, https://www.cnet.com/uk/news/virtual-reality-terminology-vr-vs-ar-vs-360-video/ (accessed on 12 October 2017). [66]

Coindesk (2017), *Microsoft's Blockchain Supply Chain Project Grows to 13 Partners - CoinDesk*, https://www.coindesk.com/microsofts-blockchain-supply-chain-project-grows-to-13-partners/ (accessed on 12 October 2017). [63]

Consumer Product Safety Commission (CPSC) (US) (2017), *Potential Hazards Associated with Emerging and Future Technologies*, https://www.cpsc.gov/s3fs-public/Report%20on%20Emerging%20Consumer%20Products%20and%20Technologies_FINAL.pdf (accessed on 13 October 2017). [31]

Consumer Product Safety Commission United States of America (2017), *Staff Report - Potential Hazards Associated with Emerging and Future Technologies*, https://www.cpsc.gov/s3fs-public/Report%20on%20Emerging%20Consumer%20Products%20and%20Technologies_FINAL.pdf (accessed on 12 October 2017). [47]

del Castillo, M. (2017), *Microsoft's Blockchain Supply Chain Project Grows to 13 Partners*, CoinDesk, https://www.coindesk.com/microsofts-blockchain-supply-chain-project-grows-to-13-partners/ (accessed on 12 October 2017). [13]

DiClerico, D. (2014), *Nest Protect Recall | Smoke and CO Alarm Reviews - Consumer Reports News*, https://www.consumerreports.org/cro/news/2014/05/nest-labs-recalls-nest-protect-smoke-co-alarm/index.htm (accessed on 12 October 2017). [48]

Ericsson (2017), *Ericsson Mobility Report*, https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf (accessed on 12 October 2017). [25]

European Commission (2016), *Advancing the Internet of Things in Europe*, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN. (accessed on 12 October 2017). [40]

European Commission (2016), "Evaluation and Fitness Check (FC) Roadmap Evaluation of the Directive 85/374/EEC Concerning Liability for Defective Products", http://ec.europa.eu/smart-regulation/evaluation/index_en.htm (accessed on 12 October 2017). [41]

European Commission (2016), *The 'Blue Guide'on the implementation of EU product rules 2016*, European Commission, http://ec.europa.eu/DocsRoom/documents/18027 (accessed on 12 October 2017). [45]

European Commission (2017), *Brief factual summary on the results of the public consultation on the rules on producer liability for damage caused by a defective product*. [42]

Federal Trade Commission US (2015), *Internet of Things Privacy and Security in a Connected World FTC Staa Report*, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (accessed on 12 October 2017). [34]

Goldman Sachs (2014), *Goldman Sachs | Our Thinking - The IoT as the Third Wave of the Internet*, http://www.goldmansachs.com/our-thinking/pages/iot-video.html. [57]

Goldman, J. and J. Falcone (2016), *Virtual reality doesn't mean what you think it means - CNET*, https://www.cnet.com/uk/news/virtual-reality-terminology-vr-vs-ar-vs-360-video/ (accessed on 12 October 2017). [17]

GS1 - The Global Language of Business((n.d.)), *Blockchain: GS1, IBM and Microsoft collaborate to leverage standards | GS1*, https://www.gs1.org/articles/2256/blockchain-gs1-ibm-and-microsoft-collaborate-leverage-standards. [54]

GS1 (2017), *Blockchain: GS1, IBM and Microsoft collaborate to leverage standards*, https://www.gs1.org/articles/2256/blockchain-gs1-ibm-and-microsoft-collaborate-leverage-standards. [15]

Iansiti, M. and K. Lakhani (2017), *The Truth About Blockchain*, https://hbr.org/2017/01/the-truth- [51]

about-blockchain.

Iansiti, M. and K. Lakhani (2017), *The Truth About Blockchain*, Harvard Business Review, https://hbr.org/2017/01/the-truth-about-blockchain (accessed on 13 October 2017). [30]

IDC (2017), *Internet of Things Spending Forecast to Grow 17.9% in 2016 Led by Manufacturing, Transportation, and Utilities Investments, According to New IDC Spending Guide*, https://www.idc.com/getdoc.jsp?containerId=prUS42209117 (accessed on 13 October 2017). [26]

IHS Markit (2015), "Global Shipment and Revenue Market Forecast for Wearable Technology The Small Revolution is Making Big Waves", http://dx.doi.org/10.0. [58]

Information Age (2015), *Who is liable when the Internet of Things goes wrong?*, http://www.information-age.com/who-liable-when-internet-things-goes-wrong-123460320/ (accessed on 13 October 2017). [7]

Information age (2017), *Who is liable when the Internet of Things goes wrong?*, http://www.information-age.com/who-liable-when-internet-things-goes-wrong-123460320/ (accessed on 13 October 2017). [55]

Inside Counsel (2017), *Augmented Reality and IoT: Enjoying the Ride, While Avoiding Legal Snafus*, http://www.insidecounsel.com/2017/03/29/augmented-reality-and-iot-enjoying-the-ride-while?slreturn=1507888346 (accessed on 13 October 2017). [18]

Jankowski, S. (2014), *Our Thinking - The IoT as the Third Wave of the Internet*, Goldman Sachs, http://www.goldmansachs.com/our-thinking/pages/iot-video.html. [6]

Kidman, D. and S. Turner (2017), *Electronic persons: time for a new legal personality?*, New Law Journal, https://www.newlawjournal.co.uk/content/electronic-persons-time-new-legal-personality-0 (accessed on 15 October 2017). [44]

Law 360 (2016), *CPSC Chair Kaye Eyes Safety Risks In New Technologies - Law360*, https://www.law360.com/articles/824104/cpsc-chair-kaye-eyes-safety-risks-in-new-technologies (accessed on 13 October 2017). [71]

Live Science (2016), *What is Augmented Reality?*, https://www.livescience.com/34843-augmented-reality.html (accessed on 13 October 2017). [19]

Marco Annunziata, B. and C. Economist (2015), *The Moment For Industry*, General Electric, http://gereports.cdnist.com/wp-content/uploads/2015/09/29153350/Annunziata_Moment-for-industry_Final1.pdf (accessed on 13 October 2017). [29]

McAfee (2013), *Data Quality in the Internet of Things*, https://securingtomorrow.mcafee.com/business/data-quality-in-the-internet-of-things/ (accessed on 13 October 2017). [33]

McKinsey & Company (2016), *Unlocking the potential of the Internet of Things | McKinsey & Company*, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world (accessed on 13 October 2017). [70]

McKinsey (2015), *Unlocking the potential of the Internet of Things*, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world (accessed on 13 October 2017). [28]

McKinsey (2016), *Internet of Things: The IoT opportunity - Are you ready to capture a once-in-a-lifetime value pool?*, http://hk-iot-conference.gs1hk.org/2016/pdf/_04_Mc%20Kinsey%20-%20(Chris%20Ip%20)%20ppt%20part%20%201%20_IoT%20-%20Capturing%20the%20Opportunity%20vF%20-%2021%20June%202016.1pptx.pdf [27]

(accessed on 13 October 2017).

Medium (2017), *IoT Raises New Challenges for Assigning Liability*, https://medium.com/iotforall/iot-raises-new-challenges-for-assigning-liability-7387b65decd0 (accessed on 13 October 2017). [37]

Meola, A. (2016), *Wearable technology and IoT wearable devices*, Business Insider, http://www.businessinsider.fr/uk/wearable-technology-iot-devices-2016-8/ (accessed on 12 October 2017). [9]

Murray, S. (2015), *How the internet of things can speed up health delivery*, https://www.ft.com/content/8ad4d226-bdcc-11e4-8cf3-00144feab7de?mhq5j=e7 (accessed on 13 October 2017). [8]

Nation, J. (2017), *IBM, Microsoft, And GS1 Will Create Supply-Line Blockchain Standards*, ETHNews.com, https://www.ethnews.com/ibm-microsoft-and-gs1-will-create-supply-line-blockchain-standards (accessed on 12 October 2017). [14]

Nation, J. (2017), *IBM, Microsoft, And GS1 Will Create Supply-Line Blockchain Standards - ETHNews.com*, https://www.ethnews.com/ibm-microsoft-and-gs1-will-create-supply-line-blockchain-standards (accessed on 12 October 2017). [64]

OECD (2013), "Protecting and Empowering Consumers in the Purchase of Digital Content Products", *OECD Digital Economy Papers*, No. 219, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k49czlc7wd3-en. [38]

OECD (2015), *Digital Economy Outlook 2015*, OECD Publishing, http://dx.doi.org/10.1787/9789264232440-en. [46]

OECD (2015), *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264232440-en. [2]

OECD (2016), "The Internet of Things: Seizing the Benefits and Addressing the Challenges", *OECD Digital Economy Papers*, No. 252, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlwvzz8td0n-en. [1]

OECD (2016), *Recommendation on Consumer Protection in E-Commerce*, OECD Publishing, Paris, http://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf (accessed on 15 October 2017). [39]

OECD (2017), *The Next Production Revolution: Implications for Governments and Business*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264271036-en. [3]

OECD (2017), "OECD Digital Economy Outlook 2017", http://www.oecd-ilibrary.org/docserver/download/9317011e.pdf?expires=1507887341&id=id&accname=ocid84004878&checksum=2FD899553D50E7BE04BFBD9687A93D0B (accessed on 13 October 2017). [12]

OECD (2017), *Summary of the CDEP Technology Foresight Forum Economic and Social Implocations of Artificial Intelligence*, https://www.oecd.org/sti/ieconomy/DSTI-CDEP(2016)17-ENG.pdf (accessed on 13 October 2017). [60]

OECD (2017), "Access and connectivity", in *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264276284-6-en. [22]

R Street (2016), "Reality Check: The Regulatory Landscape for Virtual and Augmented Reality", *R Street Policy Study*, Vol. 9/69, https://www.rstreet.org/wp-content/uploads/2016/09/69.pdf (accessed on 13 October 2017). [20]

R Street (2016), *Reality Check: The Regulatory Landscape for Virtual and Augmented Reality*, https://www.rstreet.org/wp-content/uploads/2016/09/69.pdf (accessed on 13 October 2017). [67]

Reed Smith LLP (2017), *Augmented and Virtual Reality - Emerging Legal Implications of "The Final Platform" | Perspectives | Reed Smith LLP*, https://www.reedsmith.com/en/perspectives/2017/08/augmented-and-virtual-reality (accessed on 13 October 2017). [21]

Schneier, B. (2017), *Click Here to Kill Everyone with The Internet of Things*, http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html (accessed on 13 October 2017). [5]

Stanford University (2016), "ARTIFICIAL INTELLIGENCE AND LIFE IN 2030", https://ai100.stanford.edu/sites/default/files/ai100report10032016fnl_singles.pdf (accessed on 13 October 2017). [61]

Swiss Re (2017), *New Emerging Risks Insights 2017*, http://www.swissre.com/library/expertise-publication/swiss_re_sonar_new_emerging_risks_insights_2017.html (accessed on 15 October 2017). [43]

Tech Policy Lab University of Washington (2015), "Augmented Reality: A Technology and Policy Primer", http://techpolicylab.org/wp-content/uploads/2016/02/Augmented_Reality_Primer-TechPolicyLab.pdf (accessed on 13 October 2017). [65]

Tech Policy Lab (2015), *Augmented Reality: A Technology and Policy Primer*, University of Washington, http://techpolicylab.org/wp-content/uploads/2016/02/Augmented_Reality_Primer-TechPolicyLab.pdf (accessed on 13 October 2017). [16]

Telefonica (2016), *5 Amazing Things made reality by IoT technology*, https://iot.telefonica.com/blog/5-amazing-things-made-reality-by-iot-technology-toys-edition (accessed on 13 October 2017). [11]

Telefonica (2016), *5 Amazing Things made reality by IoT technology. Toys Edition | Welcome to The IoT World of Telefónica*, https://iot.telefonica.com/blog/5-amazing-things-made-reality-by-iot-technology-toys-edition (accessed on 13 October 2017). [59]

The Engineer (2017), *How AI is Paving the Way for Fully Autonomous Cars - The Engineer*, https://www.theengineer.co.uk/ai-autonomous-cars/ (accessed on 13 October 2017). [62]

Torchia, M. (2017), *Internet of Things Spending Forecast to Grow 17.9% in 2016 Led by Manufacturing, Transportation, and Utilities Investments, According to New IDC Spending Guide*, https://www.idc.com/getdoc.jsp?containerId=prUS42209117. [52]

Walker, S. and R. Roashan (2015), "Global Shipment and Revenue Market Forecast for Wearable Technology The Small Revolution is Making Big Waves", http://dx.doi.org/10.0. [53]

Walker, S. and R. Roashan (2015), *Wearable Technology: The Small Revolution is Making Big Waves*, IHS, https://technology.ihs.com/515418 (accessed on 13 October 2017). [10]

Weber, R. (2009), "Internet of things – Need for a new legal environment?", *Computer Law & Security Review*, Vol. 25/6, pp. 522-527, http://dx.doi.org/10.1016/j.clsr.2009.09.002. [36]

Notes

[1] M2M is understood as point-to-point communications between devices performing actions without the manual assistance of humans using embedded hardware modules and either cellular or wired networks. M2M communications are only one element of the IoT and only become "smart" when combined with the logic of cloud services, remote operation and interaction (OECD, 2016[1]).

[2] More information on smart home devices and key characteristics is available in the draft discussion paper that has been prepared to support discussion under session 3 (Consumers in the Smart Home) of the joint CCP/WP roundtable on Connected Consumers.

[3]A blockchain can store "smart contracts", which are software programs that are executed in an autonomous and distributed manner by the miners of a blockchain-based network. An example is OpenBazaar, which is a decentralised marketplace that relies on blockchain technology to enable buyers and sellers to interact directly with one another, without passing through any centralised middleman. Once a buyer requests a product from a seller, an escrow account is created on the Bitcoin blockchain to ensure that the funds will only be released after the buyer has received the product (OECD, 2017[12]).

[4] It should be noted that the number of M2M SIM cards/modules only indicates the number of M2M devices which use mobile connectivity. However, M2M communication may be based on all kinds of connectivity and mobile connectivity only represents a small part of connectivity used in M2M communication (OECD, 2016[1]).

[5] A blockchain can store "smart contracts" which are software programs that are executed in an autonomous and distributed manner by the miners of a blockchain-based network. An example is OpenBazaar, which is a decentralised marketplace that relies on blockchain technology to enable buyers and sellers to interact directly with one another, without passing through any centralised middleman. Once a buyer requests a product from a seller, an escrow account is created on the Bitcoin blockchain to ensure that the funds will only be released after the buyer has received the product (OECD, 2017c).