Foreword

This report outlines the key consumer benefits and risks associated with Internet of Things (IoT) devices in the “smart home”. It was developed as a companion to a paper prepared by the Working Party on Consumer Product Safety on Consumer Product Safety in the Internet of Things.

The report was prepared by Richard Bates, an independent consultant, working with Brigitte Acoca and Anna Barker of the OECD Secretariat. It was declassified by the Committee on Consumer Policy through a written procedure that concluded on 1 March 2018 and prepared for publication by the OECD Secretariat.

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 OLIS under the reference code:

DSTI/CP(2017)8/FINAL

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

© OECD 2018

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of OECD as source and copyright owner is given. All requests for commercial use and translation rights should be submitted to rights@oecd.org.


Table of contents

Foreword ................................................................................................................................. 2
Executive Summary ............................................................................................................... 4

1. Background ....................................................................................................................... 6
   1.1. The foundations of the smart home ........................................................................ 6
   1.2. Consumer engagement with the smart home market ........................................... 7
       Consumer adoption of smart home devices and appliances .................................. 8
   1.3. Smart home device and appliance categories ....................................................... 9
       Home security ............................................................................................................ 9
       Domestic appliances .................................................................................................. 10
       Smart energy systems .............................................................................................. 11
       Virtual assistants and automation hubs .................................................................. 12

2. Potential benefits ............................................................................................................. 13
   2.1. Convenience, time savings and control at a distance .......................................... 13
   2.2. Customised living spaces and services ................................................................ 13
   2.3. Updatability .......................................................................................................... 14
   2.4. Reduced energy consumption and cost savings .................................................. 14
   2.5. Security and safety ............................................................................................... 15

3. Potential risks and policy implications ........................................................................... 16
   3.1. Changes to traditional ideas of ownership ............................................................ 16
   3.2. Interoperability ..................................................................................................... 17
   3.3. Risks to consumer privacy from smart home data collection ............................. 18
   3.4. Connected homes may raise security-related risks .............................................. 20
   3.5. Need for aftermarket support ............................................................................ 21
       Lack of support could mean devices do not function properly, if at all ................. 21
       Lack of support could pose security and safety risks ........................................... 22
   3.6. Responsibility and liability in complex smart home supply chains ...................... 22

References ............................................................................................................................ 25

Notes ...................................................................................................................................... 32

Figures

Figure 1.1. Barriers to purchasing IoT devices and services ................................................. 9

Boxes

Box 1.1. The smartphone – an interface and remote control for the smart home ............... 9
Box 1.2. Beyond household electronics: towards greater human-machine interaction .. 11
The “smart home” looks set to be the arena in which many people will utilise consumer-facing Internet of Things (IoT) technologies for the first time. A new generation of familiar household devices and appliances (e.g. washing machines) are becoming “smart” through the addition of sensors, software and Internet connections. They are entering the home alongside innovative IoT era devices (e.g. smart speakers) – often integrating with them to form smart residential systems (e.g. relating to energy, entertainment and home security).

Smart home devices and applications span a range of categories, as everything from security cameras to sanitary ware gain the “smart” prefix. Smart TVs already account for the majority of TV shipments, and point to how some devices are set to follow the lead of the mobile phone, with the smart option becoming the default.

Smart home residents stand to experience significant benefits, including:

- Convenience, as smart devices work together to automate household chores.
- Customisation, as devices learn and respond to user preferences.
- Energy efficiency and cost savings, as smart energy devices can optimise a home’s energy efficiency and deliver cost and carbon savings in the process.
- Enhanced safety and security.
- Control, in terms of being able to issue voice commands to devices, and/or monitor and adjust them remotely via a smartphone.

The prospect of ongoing improvement is another benefit that smart home devices offer. Device manufacturers learn in real time about the consumer experience of their products and services via the data those devices generate. They then develop fixes, improvements and new functionality in response, and issue these through over the air (OTA) software updates.

However, there are potential risks for smart home residents such as data privacy and cybersecurity threats, limitations on interoperability, the need for lifetime product support, complex supply chains and liability regimes, and product safety. In addition, consumer risks arising from inadequate information disclosure and misleading or unfair commercial practices remain a concern in relation to smart home technologies. Some of these risks have already materialised. For example, insufficient attention to security risks has resulted in examples of smart home devices and appliances being hacked and used as vehicles for cybercriminal activity, including against their owners.

The functionality of some smart home devices requires that they be continuously listening or observing. As a result, they capture and may transmit extensive amounts of personal data relating to their user’s offline existence - ranging from the contents of their refrigerator, to what they are doing and whether they are asleep or awake. However, the practices and processes that underpin this all-seeing capability are largely invisible to the consumer.

Other risks may emerge from a lack of device interoperability, which can create consumer lock-in and potentially undermine choice and competition. In addition, in a market where device functionality and security depend on regular software updates and
support, a smart home device may become useless, or subject to greater security vulnerabilities, if that support is not provided.

The hybrid nature of smart home devices – meshing a hardware chassis and software brain – can also pose novel challenges for consumers. For example, end user licence agreements (EULAs) governing the use of device software can limit consumers’ freedoms to use, modify, repair and resell the device. Acting in defiance of these restrictions may expose consumers to remotely administered sanctions by the manufacturer (e.g. manufacturers disabling the device). This may challenge long-held norms regarding ownership of tangible goods.

Complex supply chains underpin many smart home products. “Links” in that chain may include, among others, the manufacturer, the developers of software to run the device and apps to use with it, and internet service providers (ISPs) to provide the connectivity. Complexity in the supply chain is mirrored in the complexity a consumer can face in identifying the responsible party and seeking redress when things go wrong.

Designed to serve as an introduction to the issues, this discussion paper contains neither conclusions nor recommendations. It does, however, offer the following questions as a starting point for consideration:

- How can consumers best be provided with meaningful information on: device interoperability, IoT security and safety risks, restrictions on access and usage, and dispute resolution and redress?
- What does ubiquitous but invisible data collection by smart home devices mean for traditional approaches to protection of personal data, and how can transparency be ensured? Can technological solutions (e.g. “infomediaries”) offer a more effective response than conventional regulatory approaches, or are other approaches required?
- Taking into account the complexity of smart home supply chains, are current regulatory frameworks for liability and redress still fit-for-purpose? Who should be held responsible if something goes wrong in the smart home?
- Smart homes usually rely on multiple devices working together. To what extent should policies encourage greater interoperability among devices, and what are the trade-offs in terms of ensuring security, and potentially, managing liability?
- What should consumers be able to reasonably expect in terms of ongoing aftermarket support and software updates and how should this be communicated to consumers?
- What do current software access and use restrictions mean for smart home products? Will consumers bring expectations from more traditional products regarding rights to modification, resale and transfer? Should such expectations be incorporated into consumer policy?

Developing effective responses to the consumer protection issues that arise from the smart home will be an ongoing challenge, one element of which is that many of the issues affecting consumers cut across sectors and regulatory mandates.
The smart home is characterised by the presence of smart devices and appliances that can monitor, control, automate and optimise functions relating to climate and energy management, lighting, security, safety, entertainment and appliance usage (Snow, 2016[1]). Smart devices range from doorbells to kitchen appliances, to automation hubs that can control the other devices. While the primary functions of these devices do not relate to computing in the conventional sense, they are Internet-connected and therefore capable of: (a) communicating with each other (where interoperability permits) and with their parent manufacturer or provider; and/or (b) remote control by their users.

Some smart home devices have been “born” smart – products of the innovation made possible by IoT technologies (e.g. voice-activated automation hubs with virtual assistants like Amazon Echo or Google Home). Others are IoT era incarnations of standard appliances and devices – made smart through the addition of sensors, network connections and a software brain, which in some cases relies on artificial intelligence (AI) (e.g. smart TVs, refrigerators and washing machines). In some instances, common household devices will follow the lead of the mobile phone, and see the smart version become the default. This is already occurring for TVs.

A smart device might work in isolation, function in concert with associated devices to form a system (e.g. for heating and cooling), and/or function horizontally across system boundaries within a smart home ecosystem (e.g. security devices and room lighting working in an integrated way).

In terms of outcomes, smart home occupants are promised (depending on the devices and appliances in use) enhanced convenience, control, comfort, customisation, security and entertainment (Harper, 2003[2]), along with greater energy efficiency and cost savings (see Chapter 2). These will be achieved by smart devices learning, responding to and, in some instances, anticipating the needs and preferences of the user and automating their tasks accordingly (Aldrich, 2003[3]).

1.1. The foundations of the smart home

The smart home is one of a number of potentially overlapping “smart environments” alongside smart energy, smart cities and smart manufacturing (European Commission, 2016[4]). For example, a smart meter installed in a smart home provides a household interface with the smart grid which can potentially manage interactions with it (e.g. selling surplus microgeneration onto the grid).

With regards to the proportion of IoT connections that are consumer-facing, Cisco (2016[5]) forecasts that the smart home segment will have the largest volume of machine-to-machine (M2M) connections over the period 2015-2020, and will increase rapidly from 2.4 billion connections in 2015 to 5.8 billion by 2020 - a figure that will represent nearly half of all (12.2 billion) M2M connections.

Of the trends and developments that are driving IoT growth more widely (in terms of the range of products available), three are particularly notable in a smart home context: (i) the falling costs of IoT components; (ii) extensive connectivity; and (iii) the advent of big data and advanced analytics.
The commoditisation of components results from the massive global demand for smartphones and tablets, which has driven down the costs and size of chips and sensors that are also used by IoT devices (OECD, 2015[6]). As a result, these components are gaining a ubiquitous presence in a number of everyday machines and devices. Everything from light bulbs to clothing can now be made smart and start to sense, automate, and communicate via network connections (Thierer, 2015[7]).

Extensive connectivity results from the inter-device and external communication capabilities embedded in each smart home device. Ethernet outlets might be wired into every room, or there may be a reliance on Wi-Fi and other wireless communications such as Bluetooth, ZigBee and Z-Wave (PC Magazine Encyclopedia, 2017[8]).

With regards to data, the smart home is a big data domain – both in terms of the volume of data captured by smart devices and the rate at which it is transferred to, and processed by, device manufacturers and service providers. The implications for how personal data is collected and used, and for consumer privacy, are significant and are discussed in Chapter 3.

Big data has necessitated the development of advanced techniques for data analysis, including machine learning and AI. Machine learning and AI systems can identify difficult-to-spot relationships in data that may otherwise have been missed and make sense of vast quantities of data in near-real-time. The algorithms used can change in response to their own output and automatically improve with experience (Government Office for Science (UK), 2016[9]).

Many smart home devices already depend on machine learning and leveraging of big data to drive AI applications, including those that enable smart devices to act autonomously in performing tasks, and/or understand and interact with voice commands from the user.

1.2. Consumer engagement with the smart home market

Broadly speaking, there are two routes by which consumers can acquire smart home devices and appliances. These are summarised below.

The first is to purchase smart home packages from Smart Home Service Providers (SHSPs) or Multiple System Operators (MSOs) (Argus Insights, 2016[10]). These are companies that specialise in the provision, installation and ongoing support of smart home devices. Packages can include bundles of complementary devices (e.g. smart locks, doorbells, and video cameras), which are marketed as a “plan” or “system”. Depending on the provider, the consumer might pay some or all of the hardware costs upfront, or finance these over the duration of the contract as part of a subscription. Subscriptions can also cover the costs of related services, including premium functionality and monitoring (for security equipment). Companies competing in this space include legacy utility firms (e.g. Hive, a subsidiary of Centrica), legacy telecommunications providers (e.g. AT&T’s Digital Life), and legacy home security providers (e.g. ADT’s Pulse), alongside dedicated smart home firms (e.g. Vivint).

The second route is the do-it-yourself option, where consumers choose, buy and install their preferred devices and appliances themselves - either directly from the manufacturer, or through retailers. In some cases, consumers will pay a subscription to the manufacturer to obtain related services or additional functionality.
These two approaches are not mutually exclusive and there are likely instances where consumers blend the two – for example, by supplementing package subscriptions with additional devices.

**Consumer adoption of smart home devices and appliances**

There is little data on consumer adoption of smart home devices and appliances in the public domain. What data there is suggest that smart TVs are the most popular smart domestic product (excluding tablets and smart phones) and the primary entry point to the smart home (GfK, 2017[11]). Sales figures from GfK (2017[11]) show significant global growth for smart TVs in recent years: European sales in 2016 reached 17.38 million, up from 5.61 million in 2011; while sales in Latin America grew to 6.48 million from 1.04 million over the same period. Moreover, more than half of TV sets shipped globally in the first quarter of 2016 were smart TVs (IHS, 2016[12]) and data from Nielsen indicates that enabled smart TVs were present in 29% of all US TV homes in August 2017, up from 22% in January 2016 (Nielsen, 2017[13]).

In comparison, sales of smart devices in other categories – home automation and security, large and small domestic appliances, and communication and control – are some way behind (GfK, 2017[11]). According to one forecast, 200 million Internet connected wireless smart home security and safety products will have been installed worldwide by 2020 (IEC, 2015[14]). Further, smart thermostat sales in Western Europe are forecast to increase from less than 700 000 units in 2016 to more than 1 million units in 2020; and from 5 million to around 7.5 million units in North America during the same period (Parks Associates, 2016[15]). In addition, Voicelabs (2017[16]) predicted that sales of Echo and Home - the leading smart speaker devices that can double as smart home automation and control hubs (see Section 1.3) - were to grow to 24.5 million in 2017, up from 6.5 million in 2016.

According to Accenture (2016[17]), growth in consumer demand for IoT devices is much slower than initially anticipated, with the slow pace of adoption being a major disappointment for the industry. Its research on consumer take-up of IoT technologies identified four barriers to increased adoption: (i) cost; (ii) privacy and data security concerns; (iii) satisfaction with the status quo and a lack of perceived benefit of new devices, and; (iv) the complex and confusing nature of such devices (Figure 1.1).

The lack of a clear use case for the current generation of consumer facing IoT products is a recurrent theme in industry observers’ analysis of why these technologies are yet to achieve greater breakthrough. Accenture (2016[17]) assert that moving from technology-led innovation to innovation that pairs technology with a deep understanding of core consumer needs will be critical to accelerate IoT device adoption. Similarly, GfK (2016[18]) assert that significant barriers must be overcome before what has been a tech-led evolution, can become a consumer-led revolution. Accenture’s research bears out these sentiments, finding that ease of use and customer experience are still lagging, with two thirds (64%) of IoT device owners experiencing challenges when using a new IoT device - a figure that Accenture deems far too high to drive widespread adoption (Accenture, 2016[17]). Likewise, McKinsey has described the market as fragmented and indicated that the potential for a truly smart home is still unrealized (Coumau, Furuhashi and Sarrazin, 2017[19]). However, it expects this to change rapidly and predicts that, smart homes will be commonplace by 2027.
Figure 1.1. Barriers to purchasing IoT devices and services

(% consumers identifying the issue as a barrier to IoT adoption)

1.3. Smart home device and appliance categories

The following sections provide an overview of some of the main smart home device categories, including: i) home security; ii) domestic appliances; iii) smart energy systems; and iv) virtual assistants and automation hubs. In many cases, the smartphone plays an important role as the interface, and, increasingly, a remote control, for many smart home products, as discussed in Box 1.1.

Box 1.1. The smartphone – an interface and remote control for the smart home

Many of the examples of smart home devices listed in this section are accompanied by an interactive smartphone app, through which the user can configure and control the device and interrogate any insights its data produces. The role of the smartphone is perhaps most pronounced when the user is away, as it affords them app-based remote access and control of smart devices in their home. Smartphone GPS sensors play a key role in the functionality of some smart devices – notifying the device of the occupant’s presence in, or proximity to, the home and acting accordingly (e.g. the smart thermostat that whirs into action when it detects the occupant is heading home). The smartphone is therefore an essential component of the smart home experience: an interface and remote control for everything.

Home security

By virtue of being Internet connected, smart security and safety devices and systems grant users a remote presence – enabling them to observe and interact with their home from afar and to take steps to minimise risk whenever a device alerts them to it.

Smart surveillance cameras are equipped with motion detection sensors. They alert the occupier when unexpected movement is detected, begin recording the scene and stream video to the occupant’s smartphone, enabling them to monitor the home from wherever
they are. Depending on the system, users may be able to have two-way conversations with present parties and, where required, use the system to sound an alarm and/or alert emergency services (or security personnel). Some cameras can determine whether occupants are home and (de)activate accordingly. For example, Canary (2017[20]) claims its camera is:

... always learning and adapting. It adjusts to your preferences, knows if you’re around — auto-arming if you’re not, and understands the difference between ordinary and unusual activity in your home.

Smart doorbells, such as those offered by Ring, work similarly. When pressed, or when motion sensors detect movement, they instantly alert the occupier – who can then monitor their doorstep by video link on their smartphone, have a two-way conversation with the visitor and capture an image of the visitor.

Owners of smart locks, such as the Kwikset Kevo, can track who enters and exits the home and receive alerts as required (e.g. when children arrive home). They can also check the lock status and lock or unlock remotely, as well as grant temporary “e-keys” to trusted parties.

Provided their smart security devices are interoperable, users also have the option to configure them to work together in a complementary manner. For example, a smart lock could deactivate an interior smart surveillance camera when it identifies a trusted party is entering the building.

Smart home safety devices, including smoke alarms, carbon monoxide detectors and water sensors are also available. These offer smartphone alerts, enabling users to be aware of and respond to incidents even when they are away. These devices can also be linked to and offer automated control of related equipment, such as shut off valves, in ways that can help mitigate damage (e.g. a water sensor can detect a leak and act to prevent a flood when the occupier is away).

**Domestic appliances**

It is expected that large appliances will become more and more connected with sensors and actuators, making our refrigerators, ovens and washing machines even smarter. Samsung and LG have recently introduced “smart” refrigerators to the market that respond to voice commands and feature embedded screens that can be used for managing recipes, web browsing and online grocery shopping. They also feature internal cameras to enable remote checking of contents, and issue alerts when items go past their use by date (2016[21]).

It is also expected that smart appliances will recognise user errors - sending users a smartphone alert when an action is required (e.g. the freezer door has been left open); and self-diagnose mechanical faults and provide alerts on the need for repair, which could include automated contact with the manufacturer’s repair department to arrange a fix. They may also be able to reorder supplies (Consumers International, 2016[22]).

As noted in Box 1.2, in the future, smart home products may extend beyond traditional household appliances to enable greater human-machine interactions (OECD, 2017[23]).
Box 1.2. Beyond household electronics: towards greater human-machine interaction

Beyond household electronics, the smart home is extending to household objects that, traditionally, have never had a connection to mains electricity, let alone Wi-Fi. For example, Eight’s Jupiter+ smart mattress tracks “over 15 factors about your sleep and health, including deep sleep, heart rate and respiratory rate” and relays this data to its smartphone app. It can detect when the user is in a light sleep, triggering “the alarm when it’s easier for your body to wake up” (Eight, 2017[24]). It can even instruct your smart coffee pot to start brewing when you wake. Similarly, it has been predicted that smart toilets will be coming to the smart home market soon (Crouch, 2014[25]). Smart toilets could be equipped with sensors to help users manage their health by monitoring blood sugars, cholesterol, hormones and other such indicators and relaying this information to users’ smartphones.

Smart energy systems

Public policy commitments are driving the wide-scale installation of smart energy meters across much of the European Union (EU) and North America (European Commission, 2017[26]). With the installation of a smart meter, hundreds of millions of homes will gain access to a key component of a domestic smart energy system and an interface with the smart grid.

Beyond smart meters, IoT solutions will be used to improve heating, ventilation and air conditioning consumption and lower energy usage, monthly expenses and greenhouse gas emissions (European Commission, 2016[4]). For example, following some initial input, Nest’s Learning Thermostat familiarises itself with occupants’ routines, along with their temperature preferences at different points in that routine. It knows whether occupants are home or not and adjusts the heating or cooling accordingly (e.g. by setting an “eco temperature” to save energy when the house is empty). It also knows when occupants are nearing home and can bring the home to preferred temperatures in anticipation of an occupant’s arrival. It can learn and adjust for the performance of the household’s heating and cooling systems and alert users when system behaviour or abnormal temperatures indicate a problem that may require attention. It can also detect and respond to external variables, such as significant changes in outside temperature or peak load events on the grid. It provides occupants with reports, enabling them to see when they use more energy and how to use less. And of course, all of this can be monitored and controlled remotely, using a smartphone. In order to deliver this breadth of functionality, the Learning Thermostat combines machine learning, sensor data, users’ GPS locations and third-party data sets (Nest, 2017[27]).

Smart plugs, light switches and lighting systems also contribute to a more energy efficient household as part of a connected smart energy system. They enable users to identify and power up and power down lights, devices and appliances remotely, or, by using a link to their smartphone’s GPS, identify when they are leaving or approaching the home and respond accordingly (i.e. shutting down lights and devices as they leave). Smart lighting can be programmed to respond automatically to presence, outside light levels and time or schedules.
Virtual assistants and automation hubs

Home automation hubs are set to play a key role in centralising the control, automation and monitoring of smart home devices. Given their automation hub and central command module capabilities, voice controlled smart speakers are likely to assume a leading role in this respect. In tandem with smartphone interfaces (see Box 1.1), smart speakers streamline the integration of compatible smart device actions and make it possible to control devices through voice commands. Amazon’s Echo and Google’s Home are currently the market-leading smart speakers. They are smart listeners too, as both come equipped with Virtual Personal Assistants (VPAs): Alexa “inhabits” Amazon’s Echo and Google’s Assistant is present in the Home.²

A wide range of smart devices and systems, including those offered by SHSPs and MSOs are already compatible with and controllable by the Echo and Home smart speakers. Both allow smart home brands to develop “skills” in the case of Alexa or “actions” in the case of Assistant, which enable compatibility with other smart devices. In addition, both allow the user to “stack” instructions to multiple devices and issue these as a simple, unified voice command. For example, saying “goodnight” could switch off all lights, power off devices, turn down the heating and ensure doors are locked. Data from Business Insider (Dunn, 2017[28]) indicates that 27% of smart speaker owners utilise their home automation capabilities, and data from Voicelabs (2017[16]) indicates that 29% of Echo and Home owners “like” their smart home functionality.

Apple’s Home app offers a similar set of capabilities, including the ability to voice control a range of smart home devices via its Siri VPA, using an iPhone, an iPad or the soon to be released HomePod smart speaker. However, the compatibility of Apple’s Home app is currently limited to a smaller range of devices. This is due in part to the greater control that Apple exerts through its HomeKit development framework, which requires manufacturers to comply with a range of Apple protocols. While this extends the time to market for HomeKit compatible and compliant devices, Apple’s protocols are likely to make these devices less prone to security attacks (Apple, 2017[29]; Crist, 2016[30])

Whereas voice controlled virtual personal assistants are multi-purpose devices for which control of smart home devices is one of a range of functions, companies such as Wink and Samsung subsidiary, Smartthings, offer dedicated smart home automation hubs. Dedicated hubs can offer the advantage of compatibility with a wider range of wireless communication protocols and therefore support a greater range of smart devices. Some can even translate different protocols to ensure compatibility between devices. Both Echo’s Alexa and Home’s Assistant can be used to voice control automation hubs offered by Wink and Smartthings.

There is also a free online platform and app, IFTTT (If This, Then That) which enables users to create conditional statements using “recipes” - where a defined event in one device or service automatically triggers an action in another. An example of a smart home IFTTT recipe would be if the smart smoke alarm is triggered, then the smart lights flash throughout the house. A number of smart home brands provide readymade IFTTT “recipes” that owners of their products can utilise.
2. Potential benefits

This chapter outlines some of the potential benefits that smart home occupancy and the use of smart home devices and appliances can offer consumers. The main benefits, which vary by device, include more convenience, the ability to customise the home or device functions and features, and product updatability. In addition, smart energy products have the potential to reduce energy consumption, and home security systems have the potential to enhance home security and safety.

2.1. Convenience, time savings and control at a distance

Convenience is a key benefit of – and selling point for – the smart home. A PWC (2017[31]) survey of American consumers found that a desire to increase convenience had motivated 10% of smart home device owners to buy their first smart product (a high proportion relative to other drivers). Convenience in the smart home can be achieved through the automation of tedious or time-consuming tasks and chores. As Apple (2017[32]) implores “put your home on autopilot ... Set it up once and you’re done.”

Convenience through automation can take a number of forms. For example, a connected robot vacuum cleaner or an intelligent oven, that identifies its contents and cooks it to perfection, may liberate the user from certain household chores. The ability for consumers to specify that certain tasks (or sequences of inter-related tasks) are undertaken at a specific time, or in response to a defined event, can also deliver convenient outcomes – e.g. when children arrive home from school, the smart lock lets them in, disarms the security system and reports their arrival to their parents. Autonomous automation, for example, where the smart thermostat “learns” from and then anticipates its user’s behaviours and needs, makes energy efficient behaviours much more convenient than they would otherwise be (e.g. see the Nest Learning Thermostat example in Section 1.3).

The convenience that smart devices offer is bolstered by the flexible ways in which they can be controlled. The ability to use VPAs to control devices by voice allows smart home occupants to instruct the device to complete one task, while they themselves are preoccupied with another task. Similarly, as highlighted in Box 1.1, smartphones can act as the remote control for everything, putting control of the home in the palm of the hand. Using an Internet connection, that control can also be remote - with smart home occupants gaining control of (and information from) connected devices regardless of their location.

2.2. Customised living spaces and services

In addition to enhanced convenience, smart home occupants can enjoy a much greater degree of customisation of their home environment than was traditionally been possible. This is in part due to smart devices being, by nature, much more customisable than their “dumb” predecessors. For example, the Hue lighting system offers 16 million colours “to instantly change the look and atmosphere of your room” and preferred settings can be saved and recalled on demand (Philips, 2017[33]).

Significantly, customisation arises from smart devices that can identify which occupants are home, distinguish between them, know which space they are in and adjust that space
to meet their preferences (including heating, lighting, water temperature, media, when the coffee should be ready etc.). Those preferences will have been pre-set as user profiles, or reflect device-generated profiles where devices continually “learn” occupants’ behaviours, routines and preferences in order to better anticipate and respond to individuals’ needs. Greater customisation will also arise from the ability of devices to track behaviours and present the resultant data as personalised insights and actionable options.

2.3. Updatability

Device providers that are able to constantly gather and analyse data on the use and performance of their smart devices and associated apps, can they learn very quickly about the consumer experience of goods or services, identify faults and make adjustments, and issue OTA updates. For example, because Amazon’s Echo is always connected, new features and updates can be “delivered automatically ... Just in the last few months we’ve added Alexa calling and messaging ... and thousands of new skills from third-party developers” (Amazon, 2017[34]). In the words of David Rose “when has a car, or shoe, or furniture company been able to upgrade your object from afar? Now when we want an improvement, we won’t have to throw out the hardware” (Carmichael, 2014[35]).

In addition to introducing new functions and features, updates can also fix bugs and patch security vulnerabilities. For example, in 2014 Nest discovered defects in its Protect smoke detectors in the United States: a feature that allowed users to switch it off with a wave of the hand could be activated inadvertently. Nest halted sales and moved to remotely deactivate the feature on all relevant smoke alarms that were Wi-Fi-connected via a software update. For those products that could not be patched remotely (including units that were not Wi-Fi-connected), Nest launched a recall (DiClerico, 2014[36]).

2.4. Reduced energy consumption and cost savings

Mandated smart meter programmes represent a significant investment in IoT technologies. For example, the UK’s smart meter program is expected to connect up to 53 million electricity and gas smart meters in homes and small businesses by 2020 (Government Office for Science (UK), 2014[37]). As well as streamlining and driving improvements in industry processes (e.g. accurate and timely billing), it is expected that smart meters will drive tangible improvements in energy efficiency and reduce energy bills, carbon emissions and overall energy demand. In the UK, it is estimated that if smart meters are combined with thermostats, weather sensors and boilers, energy savings could range from 6-29% (Lewis et al., 2014[38]).

Smart meters’ home area networks and linked in-home displays promise near real-time energy consumption information to consumers - giving them greater insights on their energy usage and its costs, and supporting steps to better manage these. For example, where smart meter feedback is combined with pricing data, consumers will be able to exploit energy efficiency incentives – adapting energy consumption in response to dynamic tariffs and managing microgeneration output, including selling power to the grid (GSMA, 2012[39]). As with other smart home systems, much of this will be able to be automated and customised to reflect consumer preferences and/or behaviours, and monitored and managed through smartphone apps and interfaces.

Research by PWC (2017[31]) found that while the prospect of energy savings had motivated the purchasing decisions of only 6% of US smart home device owners, this was
seen to be the main benefit of a smart home device by non-owners. Eighty-six percent of non-owners said reducing their energy bill or increasing energy efficiency would affect their decision to own a connected home device in the future. A product review of smart thermostats estimated that energy cost savings could be between 15-25% (compared to manufacturers’ claims of 20-30%) (Kelly, 2015[40]).

2.5. Security and safety

A smart home can also be a safer, more secure home. PWC (2017[31]) found that 10% of US owners of smart home devices had bought a device because they felt it would make their home safer. Accenture (2016[17]) found that 11% of its survey respondents intended to purchase a connected home surveillance camera in the coming year.

As with traditional security systems, smart incarnations can act as a deterrent to intruders. However, they also offer the ability for users to know and see what is happening in their homes from afar – empowering them to respond in the moment and take steps that, potentially, minimise harm. This represents a marked advantage over traditional systems. These early warning and remote interaction capabilities also apply to connected smoke alarms, carbon monoxide detectors and water leak detectors. Taken together, these capabilities can serve to increase home protection and peace of mind (notwithstanding the relevant risks outlined in Sections 3.1 and 3.4).
3. Potential risks and policy implications

This chapter outlines the potential risks that smart home devices and appliances can present to consumers, and some of the key policy implications. While these risks and policy issues may not be unique to the smart home, and may vary between different smart home devices, they may be magnified by the key characteristics of smart home products, including:

- **Hybrid nature of products**: Products that combine hardware that consumers own and software used under license may change traditional notions of ownership (Section 3.1).
- **Lack of interoperability**: The incompatibility of connected devices and systems, whether they result from market conditions, design differences or contractual restrictions, may create consumer lock-in (Section 3.2).
- **Ubiquitous data collection**: The collection of vast, untargeted data from smart devices can create privacy risks (Section 3.3).
- **Security vulnerabilities**: The connected nature of the products and the need for updating can create additional security vulnerabilities that can be exploited by malicious actors and have physical as well as virtual consequences (Section 3.4).
- **Aftermarket support requirements**: The lack of aftermarket support can challenge the usability, safety and security of a smart home device or ecosystem (Section 3.5).
- **Complex supply chains**: While not unique to smart homes, the multiple entities involved in developing, manufacturing and maintaining smart home devices and products can have implications for consumers’ ability to obtain redress or determine liability if something goes wrong. (Section 3.6)

In addition, some longstanding consumer issues such inadequate disclosure and misleading or unfair conduct remain concerns in the smart home. Some of these issues are similar to those that have previously been identified by the OECD (2014) for digital content products, such as misleading practices involving advertising for smart home products, renewable contracts and issues relating to defective products and repair and redress for intangible products. Further, some of these issues can raise product safety concerns, some of which are highlighted in OECD (forthcoming).

3.1. Changes to traditional ideas of ownership

When a consumer purchases a smart home device, they in effect buy two things: (i) an inanimate piece of device hardware; and (ii) a license granting the right to use the software that underpins the device’s functionality. While the consumer owns the hardware, the software remains the property of the device manufacturer and is used under license. The licensing arrangement is typically reflected in an End User License Agreements (EULAs), which contain access and usage conditions for the software, set out by the manufacturer. As software is integral to the operation of smart devices, permitted uses of the software govern, by extension, the access and usage conditions of the device itself.

While it is widely accepted that consumers rarely engage with EULAs (see, for example, OECD (forthcoming), the terms they nonetheless agree to can undermine the rights they
might otherwise enjoy in relation to: repair (by themselves or by their preferred third party); modification, enhancement and other “tinkering”; use with third party peripherals; and resale or transfer (Manwaring, 2017[42]). As such, hardware use dictated by software licenses risks undermining consumer assumptions of what they are able to do with a device they ostensibly own.

When consumers act in contravention of the access and usage conditions set out in a device’s EULA, they may – knowingly or unknowingly – commit illegal acts. Attempts to undertake repairs or modifications will likely require the user to interface with device software, at which point they are exposed to technical and legal barriers related to copyright (Manwaring, 2017[42]). Technical barriers take the form of digital locks - designed to prevent piracy and other copyright infringements - and mechanisms that prevent certain programmes or apps running on, or being downloaded to devices (e.g. for “jailbreaking” a smartphone) (Consumers International, 2016[22]). Regardless of whether a copyright infringement takes place, circumventing a digital lock is often an illegal act in jurisdictions signatory to and compliant with the WIPO Copyright Treaty (Manwaring, 2017[42]).

The consequences of circumventing digital locks in smart devices may be severe. Because manufacturers can easily and remotely observe device use, infractions could be automatically dealt with from afar, and could include feature disablement, the blocking of access, or the erasure of data (Consumers International, 2016[22]). This could occur despite consumers having little understanding of having done anything wrong given that not all manufacturers disclose information to consumers in a clear, conspicuous and unavoidable manner. Similar disclosure issues have previously been highlighted by the OECD (2013[43]) in respect of digital content.

This issue is already on the radar of policy makers in a number of jurisdictions. The Economist (2017[44]) recently reported on the growth of a movement fighting for a “right to repair”. It reports that in America, the movement has already managed to get relevant bills on the agenda of legislatures in a dozen states. Also in the United States, two members of Congress have introduced legislation – entitled the You Own Devices Act (YODA) - that seeks to remove restrictions preventing the purchaser of a smart device from transferring ownership of it (Sheehan, 2017[45]). Further, in Europe, the European Parliament has recently passed a motion calling for regulation to require manufacturers to make their products more easily repairable (The Economist, 2017[44]).

3.2. Interoperability

Interoperability is key to ensuring systems and devices can connect and are able to “talk the same language” of protocols and encodings (Rose, Eldridge and Chapin, 2015[46]). Interoperability can be achieved by adherence to common open standards, or by implementing systems or platforms that enable different IoT systems to communicate with one another (Manyika et al., 2015[47]).

Some commentators have argued that the current lack of IoT interoperability may cause detriment to consumers to the extent that it creates a fragmented ecosystem with integration inflexibility, ownership complexity, vendor lock-in, and obsolescence due to changing standards (Internet Society, 2016[48]).

As things stand, IoT interoperability is being held back by what the Internet Society calls “schedule risk” (Rose, Eldridge and Chapin, 2015[46]). This occurs when the rate at which new products are introduced to market outpaces the availability of interoperability
standards. It is driven by manufacturers’ hopes of gaining first-mover advantages and market share. While full interoperability across products and services is not always feasible, necessary, or desirable (Rose, Eldridge and Chapin, 2015[46]), the ISO describes the lack of consistent standards as the biggest problem facing the IoT, observing that:

While some layers of the IoT technology stack have no standards, others have numerous competing standards with no obvious winner. Without a “common communication method”, devices will only be able to talk to their own brands and severely limit the helpfulness of connected machines. (Gasiorowski-Denis, 2016, pp. 10-11[49])

At present, the lack of widely adopted standards and the desire for a competitive advantage prompts manufacturers to adopt either closed or limited compatibility proprietary standards. This can result in “walled gardens” where a manufacturer’s devices and peripherals are compatible with each other, but will not work with otherwise complementary products from rival manufacturers and third parties.

By ensuring smart home devices and appliances from different manufacturers can work seamlessly together, interoperability could potentially support consumer choice and hence competition in the smart home market. In particular, interoperability can allow consumers to choose devices with the best features at the best price, and offers the means to make those devices work together (Rose, Eldridge and Chapin, 2015[46]). However, it could also be argued that there are some benefits to restricted interoperability. In particular, restricted interoperability may provide stronger incentives for new products and innovations. Further, it may allow for more control over the security of a manufacturer’s devices and/or systems. For example, given the potential security risks associated with unsecured smart home devices (see Section 3.4), making interoperability conditional on complying with minimum security thresholds may be a legitimate business approach that also reflects consumer interests.

Further, in the absence of standards, some smart home brands are already providing some clarity on the interoperability of their devices. The big three voice-controlled VPA automation hubs from Amazon, Apple and Google all provide “works with” lists, detailing compatible devices from other manufacturers, who in turn are clear on the VPAs their devices are compatible with. For example, Apple’s HomeKit compatibility label is displayed on partner manufacturer’s products and is used online and in-store, making it straightforward for users of Apple’s Home App to determine which devices are compatible. Similarly, Nest has developed the “works with Nest” logo for compatible devices. These moves are consistent with the OECD’s E-Commerce Recommendation (OECD, 2016[50]) which specifically calls on businesses to disclose information about interoperability.

Some commentators have also stressed the importance of data interoperability. For example, Consumers International (2016[22]) has argued that incompatible and proprietary data formats may present challenges for consumers seeking to integrate systems, switch services, or exercise leverage by unlocking “the utility value of that data (e.g. combining it with different data)”.

3.3. Risks to consumer privacy from smart home data collection

Many of the benefits associated with smart homes devices - especially where the functionality of those devices is reliant on machine learning and AI - would not be possible without data collection at scale. As the US Federal Trade Commission (FTC)
(2015\textsuperscript{51}) notes, the massive volume of granular data allows those with access to the data to perform analyses that would not have been imaginable in the past. However, the sheer volume of data that devices can generate is stunning. An FTC IoT workshop participant indicated that fewer than 10,000 households using their company’s IoT home automation product can generate 150 million discrete data points a day (Federal Trade Commission (US), 2015\textsuperscript{51}). This equates to approximately one data point every six seconds for each household, and that is just for one company.

Where it happens, the practice of vast, non-targeted data capture in the smart home creates a tension with data minimisation principles. Deloitte (2015\textsuperscript{52}) believes that it will be tempting for companies to operate under a “collect it if you can” basis, and that advances in IoT technology aid this impulse by providing the ability to easily and cheaply collect more data than is required to deliver the service or functionality in question.

The implications are significant, given that data relating to consumers’ offline existence - captured in the sanctuary of their homes - can be more intimate, sensitive and revealing than anything they would readily divulge online (or off). Depending on the device, this could include: what consumers say, energy usage (including which devices are being used), where consumers are (potentially down to what room of their house), who they are with, the contents of their refrigerators, what they are cooking, their children’s activities, which films they watch, sleeping patterns, vital signs, and even sexual activity (Apthorpe et al., 2017\textsuperscript{53}).

Advances in data storage and analytics make it possible to aggregate and correlate different datasets in ways that generate inferences about an individual - even where the individual has never directly shared such information. This includes the potential to infer sensitive insights from data that may appear innocuous at first, such as past purchase behaviour or electricity consumption. While such inferences could underpin services that benefit consumers, they could equally be misused in ways that are detrimental to consumer welfare, for example through the creation of detailed individual profiles that can be used to target or discriminate against customers based on their perceived value.

The problem is compounded by the fact that many consumers have little understanding about what data is being collected. While the scale and sensitive nature of data captured might be considered intrusive, the means by which these data are observed and collected are, by contrast, unobtrusive. IoT devices are often designed to operate in the background as part of the home environment so that individuals may never know (or may forget) they are there. Indeed, it has been claimed that, to be successful, IoT devices should be effectively invisible: if they’re working well, you never really see them (Withers, 2017\textsuperscript{54}).

Some smart devices and appliances lack screens or user interfaces (e.g. smart smoke alarms, plugs, light bulbs). Unless the device has an associated smartphone app, it may be difficult to effectively communicate with consumers about data collection and privacy policies. Hence, traditional models for gaining consent may no longer be fit-for-purpose and may need to be reconsidered (Office of the Privacy Commissioner of Canada, 2016\textsuperscript{55}).

Companies can also be less than forthcoming on how data are used. A recent study undertaken by 25 data protection regulators found that six in ten IoT devices do not properly disclose to consumers how their personal information is being used (Information Commissioner’s Office (UK), 2016\textsuperscript{56}). This may diminish consumer understanding about what information is being collected, used and disclosed by such devices.
3.4. Connected homes may raise security-related risks

Making the home more secure is a popular reason for purchasing smart devices. However, poorly secured devices can potentially introduce new security-related risks. In particular, vulnerabilities can allow malicious actors to hack, infect and remotely utilise connected devices with a view to either (a) turning them against their users in ways that can compromise the privacy, security and safety of smart home occupants; or (b) launching external attacks on services on the wider web, after infecting a multitude of smart devices simultaneously. Risks relating to data and privacy also arise where smart device manufacturers and service providers take insufficient steps to secure personal data in transit or storage.

IoT security vulnerabilities have been well-documented. For example, a 2015 study of popular IoT devices revealed a high average number of vulnerabilities per device (Hewlett Packard, cited in (OECD, 2016[57])). Seventy per cent of devices used unencrypted network services; 60% provided user interfaces vulnerable to basic attacks; and 80% used weak passwords. Similarly, the 2016 DEF CON hacker and computer security conference disclosed 47 vulnerabilities affecting 23 IoT-enabled items (including door locks, wheelchairs, thermostats and more) from 21 manufacturers (Rainie and Anderson, 2017[58]). The interconnectedness of smart home systems also means that one “weak link” can potentially compromise the security of the system as a whole.

As IoT products increasingly influence or control the physical world around them, digital security incidents involving the IoT can have physical consequences (e.g. the smart thermostat could be used to freeze and burst the water pipes in winter, if hacker ransom demands go unpaid). In Bruce Schneier’s words “attacks against data and information have become attacks against flesh, steel, and concrete” (2016[59]).

Security vulnerabilities in devices can also lead to consumer privacy being compromised. The peace of mind a user expects from a smart security camera turns to great distress if a malicious party accesses the device and turns its remote viewing capability on the user - watching them in their homes, potentially with criminal intent.

In 2013, the FTC alleged that the lax security practices of TRENDNet, a maker of video security cameras, had exposed the private lives of hundreds of consumers to public viewing on the Internet (Federal Trade Commission (US), 2013[60]). In its complaint, the FTC alleged that TRENDNet violated the Federal Trade Commission Act by failing to use reasonable security to design and test its software. The FTC (2017[61]) has also taken enforcement action against D-Link for leaving its wireless routers and Internet cameras vulnerable to hackers by failing to take steps to address a number of well-known and easily preventable security flaws.

In a similar case, the FTC (2016[62]) reached a settlement with ASUS relating to security flaws in its routers and associated cloud services that were exploited by hackers in 2014 to gain unauthorised access to over 12 900 consumers’ connected storage devices. The FTC alleged that ASUS did not address security flaws in a timely manner or notify consumers about risks associated with the vulnerable routers or the availability of security updates.

More broadly, insecure devices can be taken over and used to launch malware attacks with wide-reaching consequences. For example, a major 2016 distributed denial-of-service attack (DDoS) attack was implemented by infecting tens of millions of IoT-connected devices like printers, digital video recorders, cable set-top boxes, webcams and...
baby monitors with a malware called Mirai (Woolf, 2016[63]). In 2014, Proofpoint documented the first case of common appliances being used in a digital security attack (Starr, 2014[64]). Hackers remotely commandeered 100,000 home IoT devices - including routers, multimedia centres, televisions and at least one refrigerator – using them to send 750,000 spam emails.

Finally, the scale of manufacturers’ and service providers’ data infrastructure reflects the need to store (potentially indefinitely) and process the growing volume of personal data collected by smart home devices. If insufficient steps are taken to secure this infrastructure, the opportunities for data breach, whether negligent or malicious – also grow. A data breach could compromise privacy and result in significant distress and detriment to the consumers affected.

3.5. Need for aftermarket support

Equipping household devices and appliances with computer circuit boards is nothing new. But, where a refrigerator was once an electromechanical appliance whose functionality was aided by the presence of computer components, its smart descendant is a computer with a refrigerator attached. Software and an Internet connection are critical to its optimal operation and underpin a range of functions and complementary services. This change points to how devices and appliances in the smart home are becoming hybridised versions of their former selves, as the hardware body gains a software brain.

The software dependency of smart home devices and appliances can give rise to two (sometimes inter-related) aftermarket risks: (i) the use of a device can be impeded, or even prevented, by the manufacturer’s (in)actions in relation to support for the software on which it runs; and (ii) unsupported software can pose a significant security risk to the device and to the consumer’s wider smart home ecosystem.

Lack of support could mean devices do not function properly, if at all

Nest’s 2014 acquisition of Revolv, the manufacturer of a smart home automation hub, provides an illustration of the first risk. Post-acquisition, Nest immediately discontinued the product, before “unilaterally rendering the devices inoperable” two years later (Federal Trade Commission (US), 2016[65]). Despite being sold with a “lifetime subscription”, this move left Revolv hub owners with unusable USD 300 (United States dollar) “bricks” (Statt, 2016[66]). Although the ensuing backlash eventually prompted Nest to offer a refund (Nest, 2016[67]), the case raised serious questions about the longevity of smart home devices - not least where small start-ups are acquired by a larger company.

Following its preliminary investigation of Revolv, the FTC decided not to take formal enforcement action against the company. It nevertheless took the opportunity to outline its expectations of what consumers should be able to expect in terms of support for smart devices. The FTC noted both the consumer expectation that “things they buy will work and keep working, and that includes any technical or other support necessary for essential functioning”; as well as the risks that consumers can be exposed to when technical support is withdrawn (Federal Trade Commission (US), 2016[68]).

A related issue can arise when malfunctioning software updates cause temporary, or even long-term inoperability of smart devices, resulting in significant inconvenience and, potentially, safety risks for users. For example, the USD 469 Lockstate smart lock was rendered inoperable by a “fatal” software update for which a remote fix was impossible (Morse, 2017[69]). Similarly, manufacturer updates can also modify device functionality
without notice, leaving the user vulnerable to whatever changes the manufacturer makes - possibility eliminating features that persuaded the consumer to purchase the device initially.

In some instances, smart home devices and appliances can suffer post-sale neglect. This can arise because of manufacturer bankruptcy, as was the case with the popular Jawbone fitness tracker (Klienman, 2017[70]), or where the manufacturer ends software and technical support for what it deems to be a legacy product. As the FTC (2015[51]) noted, post-sale neglect can also happen where companies focused on low value devices lack the economic incentive to provide ongoing support or software security updates, leaving consumers with unsupported or vulnerable devices shortly after purchase. In each of these cases, the consumer is left with an orphan device that lacks any means of long-term support.

The bricking and orphaning practices outlined above suggest that premature obsolescence could become a significant area of consumer detriment in the IoT, given that consumer expectations, based on prior experience of owning common devices (e.g. 8 to 15 years for washing machines), are many years longer than is typically associated with high-tech equipment (OECD, 2016[57]). For this reason, the OECD (2016[57]) has noted that information (provided at the point of sale) that clearly indicates what support a consumer can expect over the lifetime of a device regarding software updates for the device and related apps, would be useful to consumers. Similarly, the FTC has noted (2017, p. 2[71])

Providing consumers with clear information about whether, how, for how long, and at what cost their IoT devices will receive security support can benefit consumers, foster competition, and promote innovation in security.

Further, in relation to software updates, the FTC (2017[71]) recommends that businesses disclose: (1) whether a device can receive security updates; (2) how it receives security updates; and (3) the anticipated end of security support.

Lack of support could pose security and safety risks

Consumers can be exposed to heightened security and safety risks where a manufacturer is negligent in identifying risks (or defects) and applying updates and patches. Consumers are left similarly exposed in instances where they continue to utilise the Internet-dependent functionality of a device that has been orphaned by the manufacturer, following the discontinuation of software support. Either eventuality leaves the device, the user’s smart home ecosystem and, potentially the individual themselves, exposed to the range of security and safety risks highlighted above. For a more thorough discussion of the consumer product safety risks associated with the IoT, see OECD (forthcoming).

3.6. Responsibility and liability in complex smart home supply chains

In order to operate effectively and in the manner expected, smart home devices are often dependent on a complex supply chain. This can include product designers, developers of the software on which the device runs, developers of the smartphone app by which the consumer controls the device, manufacturers of the sensors, processors and other computer hardware that powers the device, and the device manufacturer and/or provider. The successful operation of a smart device or appliance can also depend on:

- The correct installation of the device in the home, which may be undertaken by a provider.
The device’s remote interaction with the provider, especially where the consumer has a subscription service.

- Other devices, including automation hubs, which the device needs to connect with in order to perform a task.
- A means of Internet connection (e.g. WiFi) and therefore routers, modems and the home’s ISP.
- Remote data storage and processing – e.g. the cloud systems of the device manufacturer and its partners.
- Providers of associated services – e.g. a smart refrigerator that can reorder its contents from a retailer as items expire or run low; and related payment services.

This supply chain may become even more complex where one device integrates with others to form a smart home “system”.

The nature of a smart device supply chain presents the risk that when things go wrong, identifying and seeking redress from the responsible party could be as complicated for the consumer as the supply chain itself. For example, a Nest thermostat user seeking to understand their rights and the obligations and responsibilities of the various parties in the device’s supply chain needs to read at least thirteen legal documents (Noto La Diega and Walden, 2016[72]).

A related risk arises wherever hardware-focused device manufacturers attempt to offload or shift liability, for example by claiming the software developer is the real party responsible for any defect, or that the service provider is responsible (Noto La Diega and Walden, 2016[72]). This can hamper the allocation of liability for faults and hinder redress, especially where the costs of pursuing a legal claim exceed the cost of the detriment experienced (Manwaring, 2017[42]).

Where smart home devices involve autonomous decision-making, even more complex questions of liability might arise. There are reported instances of Amazon orders being simultaneously placed by Echo devices in multiple households after the Alexa VPA overheard TV news reports that children had placed orders using Alexa (Liptak, 2017[73]). There are also reports of Alexa placing orders in response to parrots mimicking their owners (Greatrex and White, 2017[74]). These examples illustrate an important question in relation to autonomous decision-making and liability and redress, namely: who is liable for an unwanted contract entered into by a smart home device or appliance (Manwaring, 2017[42])?

These issues are currently receiving attention in the EU as part of the European Commission’s review of the EC’s Directive on Liability for Defective Products (2016[75]). The review includes an assessment of whether the Directive remains fit-for-purpose in light of new technological developments, including the IoT.

A related question is what should be the role of the consumer in ensuring that their devices, systems, personal data and personal effects are secure? It might be argued that consumers should assume greater responsibility for good digital “housekeeping”. For example, consumers might be expected to secure wireless networks, replace default passwords with strong ones as a matter of course, and act on alerts for software updates and installing them in a timely manner. In practice, however, a significant proportion of consumers do not take these steps.

Determining the various roles and responsibilities will be a key issue for policy makers. This may be further complicated by the number of regulators that are likely to be involved in protecting smart home consumers. For example, a smart energy meter is an...
energy device, a telecommunications device and a data capture device. As such, energy metering is no longer the sole concern of utility regulators. Instead it represents a point where the mandates of four regulators – utility, telecoms, consumer and data protection authorities – converge. If a utility company uses customer data to gain an unfair competitive advantage, competition authorities may also take an interest. This pattern of converging regulatory interests repeats across a range of smart home technologies and highlights the need for co-ordination and co-operation in terms of regulatory oversight and enforcement if effective consumer protection is to be ensured in the smart home.

In its 2015 “Digital Economy Outlook”, the OECD noted that the complex structure of IoT markets can obscure which authorities are responsible for helping consumers, making policy and undertaking enforcement (OECD, 2015). It cautioned that the ongoing development of separate responses to emerging technology developments “risks an overall loss of regulatory coherence” (OECD, 2015, p. 271). It also noted that a single regulatory framework, or at least a joint approach, for addressing the changing dimensions of IoT activities would offer “a more coherent arrangement for both businesses and consumers engaging in such activities” (OECD, 2015, p. 271).
References


Consumer Reports (2014), Best Home Automation System, https://www.consumerreports.org/cro/magazine/2014/06/run-your-home-from-your-
phone/index.htm (accessed on 11 October 2017).


OECD DIGITAL ECONOMY PAPERS


---

**Notes**

1 An actuator is a mechanical device for moving or controlling a mechanism or system. It takes energy, usually transported by air, electric current, or liquid, and converts that into some kind of motion (European Commission, 2016[4]).

2 VPAs are software applications that use natural language processing, machine learning and AI to comprehend, process and respond to user requests and instructions. They can organise and play music, manage schedules, answer questions, search the web, make calls and execute tasks, such as ordering a pizza.