EUROPEAN
COMMISSION

Brussels, 20.1.2022
SWD(2022) 10 final

COMMISSION STAFF WORKING DOCUMENT
Accompanying the document

REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

Final report - Sector inquiry into consumer Internet of Things

{COM(2022) 19 final}

Table of Contents

GLOSSARY

This glossary contains a list of terms used in the report and defines them for the specific purpose of the report only. The report's terminology is without prejudice to the terminology used in any other document and any legal or factual qualifications set out therein.

CONSUMER INTERNET OF THINGS (IOT) SECTOR: encompasses various services, devices and technologies that support the interaction of consumers with connected devices ("things"), which collect and exchange data over the internet.

CONSUMER IOT ECOSYSTEM: a network of connected and interdependent technologies that work together around a consumer IoT technology platform providing services and functionalities to the user.

CONSUMER IOT SERVICES: services that consumers can access via a SMART DEVICE, through a VOICE ASSISTANT and/or through other smart home USER INTERFACES. These services may be grouped into categories that include, but are not necessarily limited to, health and fitness services, creative content services (e.g. music streaming services, video-on-demand platforms), online information services, search engines, online intermediation services (e.g. marketplace, food delivery service, car-sharing service) and shopping services.

CONSUMER IOT TECHNOLOGY PLATFORM: underlying technological solution for integrating consumer IoT services and SMART DEVICES in a connected system. For the purpose of this report, technology platforms refer in particular to VOICE ASSISTANTS and SMART DEVICE OPERATING SYSTEMS. Consumer IoT players develop specific applications to make their services and devices compatible with CONSUMER IOT TECHNOLOGY PLATFORMS.

PROPRIETARY TECHNOLOGY (OR "CLOSED STANDARDS"): refers to technology developed by one vendor, which retains control over access to its technology.

SMART DEVICES: wireless electronic consumer Internet of Things devices, such as wearable devices, smart speakers and other smart home devices, capable of connecting to other devices or networks, exchanging data with them and operating to some extent interactively and autonomously. This definition does not include smart mobile devices (i.e. smartphones and tablets).

SMART DEVICE OPERATING SYSTEM: a piece of software that manages smart device hardware and software resources of a SMART DEVICES, and provides common services for applications running on it.

SMART HOME APPLICATION: application that enables the user to connect, control and/or monitor one or more smart home devices remotely.

STANDARDS: technology resulting from collaborative standardisation processes involving various vendors and stakeholders.

USER INTERFACE: device or device application (e.g. SMART HOME APPLICATIONs, mobile devices, dedicated touch-screens, remote controls, VOICE ASSISTANTs or wearable devices) that forms the user-facing entry point through which SMART DEVICES are accessed and controlled by the user.

VOICE APPLICATIONS: software designed for a specific VOICE ASSISTANT that supports commands by users to connect with SMART DEVICES, to execute actions or tasks, or to engage with CONSUMER IOT SERVICES that consumers access via that VOICE ASSISTANT. VOICE APPLICATIONS written for Amazon Alexa are called “skills” and for Google Assistant “actions”.

VOICE ASSISTANTS: a voice-activated piece of software that can process voice commands and return relevant information or perform certain functions as requested by the users.

1 INTRODUCTION

1.1 WIDER CONTEXT

(1) On 16 July 2020, the Commission launched a sector inquiry into consumer Internet of Things (IoT) in the EU. The sector inquiry, which is carried out on the basis of the EU competition rules, pursuant to Article 17 of Regulation 1/2003[1], focuses on gathering information on companies active in various areas of the consumer IoT sector.

(2) The sector inquiry fits within the broader context of the Commission's digital priorities and ongoing policy and legislative initiatives that also concern the area of IoT. In recent years, the Commission has adopted a set of policy actions to accelerate the take-up of IoT in the EU, including launching the Alliance for Internet of Things Innovation (AIOTI) in March 2015, to support the creation of an innovative and industry-driven European IoT sector. This was followed in April 2016 by the publication of the European Commission staff working document "Advancing the Internet of Things in Europe", which sets out the EU's IoT vision, and by the "European data economy" initiative, launched in January 2017, which proposes policy and legal solutions aimed at contributing to the creation of a European single market for IoT. Looking ahead, the findings of the sector inquiry will feed into the ongoing legislative debate on the Digital Markets Act[2] (DMA).

1.2 REASONS FOR LAUNCHING THE SECTOR INQUIRY

(3) The consumer IoT sector has grown rapidly in recent years and is forecast to continue to do so in the next decade. Worldwide consumer IoT revenue is predicted to increase from approximately EUR 107.2 billion in 2019 to approximately EUR 408.7 billion by 2030[3]. It is expected that there will be more than 8 billion consumer internet and media devices worldwide by 2030, making this area by far the most common use case of the IoT as a whole[4]. Moreover, the number of voice assistants in use worldwide is expected to double between 2020 and 2024, from 4.2 billion to 8.4 billion[5].

---

[1] The sector inquiry was launched pursuant to Article 17 of Council Regulation (EC) 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 4.1.2003, p. 1.

[2] European Commission. *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (COM/2020/842 final).* European Commission, Brussels, 15 December 2020, retrievable from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

[3] Transforma Insights (22 December 2020), 'Internet of Things (IoT) revenue worldwide from 2019 to 2030 (in billion U.S. dollars), by vertical.' [Chart], *Statista*, retrieved on 24 March 2021, https://www.statista.com/statistics/1183471/iot-revenue-worldwide-by-vertical/

[4] Transforma Insights, (22 December 2020), 'Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by use case (in millions)' [Graph], *Statista*, retrieved on 20 March 2021, from https://www.statista.com/statistics/1194701/iot-connected-devices-use-case/

[5] Voicebot.ai, and Business Wire (28 April 2020), 'Number of digital voice assistants in use worldwide from 2019 to 2024 (in billions)*.' [Chart], *Statista*, retrieved on 24 March 2021, from https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-in-use/

(4) In the EU as well, the use of consumer IoT products is increasingly becoming part of everyday life for citizens. The use of connected audio and video entertainment devices in particular has become relatively widespread: in 2020, for example, 51% of individuals in the EU reported to Eurostat that they used the internet on a smart TV, games console, home audio system, or smart speaker[6]. Smart wearable devices are also becoming a feature of Europeans' lives. In 2020, 19% of individuals in the EU used a smart watch, fitness band, connected goggles or headset, safety tracker, smart clothing, accessories, or shoes. Moreover, 11% of Europeans surveyed in 2020 used a voice assistant[7].

(5) The use of other smart device types is still quite low: in 2020, only 10% of individuals in the EU used a smart thermostat, utility meter, lighting solution or other smart solution for energy management in their home[8] and even fewer used smart security solutions[9] (5% of individuals)[10] and/or smart home appliances such as cleaning or kitchen appliances (5% of individuals)[11]. Nonetheless, revenue for the smart home segment (encompassing smart entertainment systems, appliances, heating, lighting systems and security systems) in Europe is forecast to more than double between 2020 and 2025 (from approximately EUR 17 billion to approximately EUR 38.5 billion)[12].

(6) At the same time, there are also indications that consumers are wary of the risks posed by this technology. In 2020, 13% of individuals in the EU cited concerns about the privacy and protection of personal data generated by IoT devices or systems as their reason for not using IoT personally or in their household[13]. There are also concerns about the interoperability of consumer IoT products, with 5% of individuals citing a lack of compatibility with other devices or systems as their reason for not using IoT[14].

(7) National Competition Authorities are also taking an interest in the consumer IoT sector. In 2020, the German Competition Authority carried out a sector inquiry, under consumer protection law, into smart TVs, including a focus on their data collection and

---

[6] Eurostat, Data browser: Internet of Things - use, *Eurostat*, retrievable from https://ec.europa.eu/eurostat/databrowser/view/isoc_iiot_use/default/table?lang=en

[7] Eurostat, Data browser: Internet of Things - use, *Eurostat*, retrievable from https://ec.europa.eu/eurostat/databrowser/view/isoc_iiot_use/default/table?lang=en

[8] Eurostat, Data browser: Internet of Things - use, *Eurostat*, retrievable from https://ec.europa.eu/eurostat/databrowser/view/isoc_iiot_use/default/table?lang=en

[9] I.e. a smart home alarm system, smoke detector, security camera, door lock or other internet-connected security or safety solution.

[10] Eurostat, Data browser: Internet of Things - use, *Eurostat*, retrievable from https://ec.europa.eu/eurostat/databrowser/view/isoc_iiot_use/default/table?lang=en

[11] Eurostat, Data browser: Internet of Things - use, *Eurostat*, retrievable from https://ec.europa.eu/eurostat/databrowser/view/isoc_iiot_use/default/table?lang=en

[12] Statista (11 September 2020), 'Smart Home - revenue forecast in Europe from 2017 to 2025 (in million U.S. dollars)' [Chart], *Statista*, retrieved on 23 March 2021, from https://www.statista.com/forecasts/528116/revenue-in-the-smart-home-market-in-europe

[13] Eurostat, Data browser: Internet of Things – barriers to use, *Eurostat*, retrievable from https://ec.europa.eu/eurostat/databrowser/view/isoc_iiot_bx/default/table?lang=en

[14] Eurostat, Data browser: Internet of Things – barriers to use, *Eurostat*, retrievable from https://ec.europa.eu/eurostat/databrowser/view/isoc_iiot_bx/default/table?lang=en

processing capability[15]. In 2019, the French Competition Authority contributed to a joint study on voice assistants and connected speakers[16].

(8) While the consumer IoT sector is still developing, there are indeed indications of company behaviour that may be conducive to distortions of competition in this sector. Such practices could lead to raising barriers to entry and innovation, dependency on third-party proprietary technology for competitors and consumer lock-in.

1.3 THE PURPOSE OF THE SECTOR INQUIRY

(9) Sector inquiries are investigations that the Commission decides to carry out in sectors of the economy or in relation to particular types of agreements across various sectors where there are indications that competition may be restricted or distorted within the internal market.[17] A sector inquiry is a fact-finding exercise, a systematic investigatory tool, which can inform or complement future decision-making and potential investigations. Its aim is not to target individual companies. However, the results of a sector inquiry may point to potentially anti-competitive practices and the Commission may decide to open case-specific investigations under Articles 101 and 102 Treaty on the Functioning of the European Union after the conclusion of the sector inquiry.

(10) The purpose of this sector inquiry is to gain a better understanding of the consumer IoT environment, the competitive landscape, and developing trends in this developing sector. It focuses specifically on the consumer aspect of the consumer IoT sector. Where it focuses on products or services sold to business-to-business (B2B) customers, it does so only to the extent that such products or services are subsequently integrated into consumer-oriented offers.

(11) Industrial IoT is not within the scope of the sector inquiry. Industrial and consumer IoT are distinct sectors with specific characteristics. One of the special characteristics of consumer IoT is that the type of data collected by smart devices typically includes personal data. Consequently, the development of this sector can be expected to have a significant impact both directly on consumers and on society as a whole. For this reason, the sector inquiry focuses on consumer IoT.

(12) Similarly, connected cars are not subject to the sector inquiry because of their distinctive regulatory and factual characteristics.

---

[15] Bundeskartellamt, *Sector inquiry smart TVs - Conclusion and recommendations for action (Az. V-22/17)*, 17 July 2020, retrievable from https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/AktuelleMeldungen/2020/17_07_2020_Sector_inquiry_smart_TVs_conlusion.html

[16] Hadopi & CSA, *Assistants vocaux et enceintes connectées - l'impact de la voix sur l'offre et les usages culturels et médias*, mai 2019, retrievable at https://hadopi.fr/actualites/lhadopi-et-le-csa-sassocient-pour-la-realisation-dune-etude-commune-sur-les-assistants

[17] Article 17 of Council Regulation (EC) 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 4.1.2003, p. 1.

1.4 DATA GATHERING AND ANALYSIS

1.4.1 Questionnaires to stakeholders

(13) The sector inquiry has been conducted on the basis of requests for information pursuant to Article 17 of Regulation 1/2003 ("questionnaires"). In July 2020, different questionnaires were sent to companies active in four consumer IoT segments in the EU; (i) the manufacture of smart home devices; (ii) the provision of voice assistants; (iii) the provision of consumer IoT services; and (iv) the manufacture of wearable devices. A fifth questionnaire was sent to standard-setting and industry organisations. The type and number of questions varied across the five questionnaires.

(14) The questionnaires were sent to a selection of companies active in the consumer IoT sector. Relevant addressees were identified by desk research.

(15) While the selection of addressees was not intended to correspond to a statistically representative sample of the EU consumer IoT sector, the selection covers a variety of consumer IoT products and services and represents different types of companies in terms of size, activities and range of products offered (see Chapter 3 on characteristics of respondents).

(16) Companies active in more than one consumer IoT segment received several of the four different questionnaires.

(17) The responses to these questionnaires constituted the main source of information for the sector inquiry, complemented by the input received through the public consultation on the preliminary report (See 1.4.2.). Nothing in this report should be read or construed as an endorsement of the practices reported, nor as an assessment of their compatibility with applicable Union or national law, including the EU General Data Protection Regulation, (GDPR)[18].

(18) The data collected and presented in this report summarise the qualitative information obtained from the responses. They should not be read as statistically relevant figures in the strict sense.

(19) Similarly, the market dynamics, products and services referred to in this report describe the situation as it was at the time when the respondents provided their replies to the questionnaires and submitted their comments to the public consultation on the preliminary report, that is, respectively in the second half of 2020 and the summer of 2021.

(20) Throughout this report, proportions are calculated based on the number of respondents who replied to the relevant question, unless specified differently.

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88.

(21) The sector inquiry focuses on topics of particular potential interest in examining possible competition issues in the consumer IoT sector. The different questionnaires sent included questions on the following:

a. The characteristics of respondents' consumer IoT products and services in order to gain an overview of the sector.

b. The main features of competition in the consumer IoT sector, including potential barriers to entry and the role of various business strategies.

c. The role of standards in the consumer IoT sector, including the importance of standards and standard-setting organisations (access conditions and competition among standards).

d. The interaction between devices, services and voice assistants in the consumer IoT sector. This includes questions on interoperability, pre-installation and default settings, exclusivity and other preferential treatment; and

e. The role of data in terms of the consumer IoT sector. This includes questions on the collection of data, how it flows between parties, how it is used and potentially monetised by companies, and the interoperability and portability of data.

(22) The questionnaire sent to standard-setting and industry organisations focused on point c. above.

1.4.2 The public consultation and the final report on the sector inquiry

(23) On 9 June 2021, the Commission published a preliminary report[19], which presented the Commission's preliminary findings.

(24) The publication of the preliminary report was followed by a public consultation open to all interested stakeholders. The public consultation ended on 1 September 2021. Altogether, the Commission received 26 submissions to the public consultation. These submissions welcomed the publication of the preliminary report and generally agreed with the main conclusions drawn in relation to the current and main challenges of the consumer IoT sector in the EU.

(25) The input received through the public consultation on the preliminary report has complemented the preliminary findings to complete the Commission's evaluation in the consumer IoT sector.

[19] European Commission, *Commission Staff Working Document: Preliminary Report – Sector Inquiry into consumer Internet of Things (SWD(2021) 144 final)*, European Commission, Brussels, 9 June 2021, retrievable from https://ec.europa.eu/competition-policy/system/files/2021-06/internet_of_things_preliminary_report.pdf

(26) The adoption of a final report from the Commission to the Council and the European Parliament completes the sector inquiry. This staff working document accompanies the final report and summarises the main findings of the sector inquiry.

2 CHARACTERISTICS OF CONSUMER IOT PRODUCTS AND SERVICES

2.1 OVERVIEW

(27) The following paragraphs describe the main characteristics of the different consumer IoT segments on the basis of replies submitted by the respondents of the sector inquiry and in the submissions to the public consultation on the preliminary report. This chapter also includes a description of how consumer IoT services, devices and voice assistants interact with one another.

2.2 VOICE ASSISTANTS

2.2.1 Characteristics of voice assistants

(28) Voice assistants are voice-activated pieces of software that can perform a variety of tasks, acting both as a platform for voice applications and a user interface. The results of the sector inquiry indicate that voice assistants represent the fastest developing interface for users to access the web, to use and control smart devices and access consumer IoT services.

(29) From the respondents' replies, it emerges that there are currently four voice assistants widely used in the EU, namely Amazon's Alexa, Samsung's Bixby, Google's Google Assistant and Apple's Siri. Apple was the first to launch its voice assistant in the EU in 2011, followed by Alexa and Google Assistant in 2016, and Bixby in 2018. However, many respondents indicate that the uptake of voice assistants really took place when Amazon launched its first smart speaker Amazon Echo in 2014, followed by Google launching its smart speaker Google Home in 2016 and Apple its HomePod in 2018. Today Google Assistant, Alexa and Siri are seen as the leading voice assistants in the consumer IoT sector.

(30) These voice assistants are general-purpose voice assistants, as they enable users to access a broad range of features. For example, they can be used for:

- Playing music and videos, or listening to the radio, news, podcasts or audiobooks on the smart device itself or on other devices (for example on headphones, smart speakers, or smart TVs);
- Controlling smart home devices (for example lights, switches, outlets and thermostats), smart displays, and smart clocks;

- Providing information (for example news, sports scores, recipes, and weather);
- Helping in planning and executing daily routines (for example booking a taxi ride, setting or assigning reminders or creating calendar events).

(31) Other voice assistants are considered specialised voice assistants. They are usually provided by consumer IoT service providers or smart home device manufacturers and have limited functionalities, mainly relating to the service provider's or device manufacturer's own services and/or devices. These include, for example, Orange's voice assistant Djingo, the main function of which is to provide access to Orange's services (TV, music, smart home, telephony or radio) or Microsoft's Cortana, which is a feature of Microsoft's M365 productivity solutions.

(32) Google Assistant and Siri are currently the voice assistants available in most languages (around 20 to 30 languages each with a few additional dialects supported), followed by Alexa (15 languages) and Bixby (8 languages), whereas the specialised voice assistants are typically available in only one or two languages. This is because specialised voice assistants usually target a specific Member State or a particular group of users (for example, the subscribers of the specific service provider). For example, Orange's voice assistant is only available in French, whilst Magenta, Deutsche Telekom's voice assistant, is only available in German. Telefónica's voice assistant, Aura, is available in Spanish, English and German, but the user is not able to switch between the languages. The precise number of languages in which a voice assistant is available may also differ according to smart device type.

2.2.2 User interaction

(33) For most voice assistants, the interaction of the voice assistant with the user takes place through the following phases: (i) activation by the user; (ii) instruction by the user; (iii) processing by the voice assistant; and (iv) trigger and response by the voice assistant.

(34) More precisely, as a first step, the user activates or "wakes up" the voice assistant. This part of the interaction usually takes place locally on the smart device. Depending on the type of smart device as well as the voice assistant brand, the user can activate the voice assistance functionality in different ways. For example, in the case of smart speakers, this is done by saying an activation word (also called "hotword" or "wake word") such as "Hey Siri", "OK Google" or "Hi Bixby" directly to the device. On some other devices, such as smartphones and remote controls, before saying the activation word, the user is required to touch the screen or press a button.

(35) As a second step, the voice assistant collects the voice command. In practice this means that the user gives a precise instruction or command to the voice assistant (to execute a task such as switching on lights, playing music, setting a timer, compiling a shopping list or sending a message) or asks a question (to receive information such as the weather forecast or the time of day).

(36) As a third step, the voice assistant generally processes the command in two stages. The first stage is understanding the request. Unless the intent is recognised with certainty and the instruction is processed locally, the speech recognition is performed by cloud-based technology. The second stage is to identify the available responses. Once the voice assistant understands the user's voice query, it identifies different options to fulfil the user's request (for example providing information on the weather, dimming the lights). With slight differences depending on the underlying technology, the available responses are ranked by the voice assistant on the basis of various parameters: the relevance and availability of the response, predicted user satisfaction, suitability of the response for the type of device concerned and alignment with the user's current activity.

(37) As a final step, the voice assistant responds by: (i) letting the user know that it does not understand the request; (ii) triggering an action or retrieving the information identified as appropriate; or (iii) responding that it has identified the most appropriate option or a list of options.

2.3 SMART HOME DEVICES

2.3.1 Characteristics of smart home devices

(38) Smart home devices encompass a very large group of devices that can be grouped in the following main product categories: smart home appliances; smart home entertainment devices; comfort and lighting devices, and security devices.

(39) The smart home appliances category includes all kinds of smart household appliances, ranging from large appliances such as refrigerators, washing machines and ovens, to small appliances such as microwaves, coffee machines, vacuum cleaners and mowing robots.

(40) Smart home entertainment products include (multi-room) entertainment systems such as sound systems, smart TVs and receivers, streaming devices (for example the Amazon Fire TV stick and Google Chromecast) and smart speakers.

(41) Comfort and lighting devices include, for instance, smart light sources such as smart bulbs, sensors and actuators such as door and window sensors, shutters, smart clocks, thermostats, air conditioning and radiator controllers.

(42) Security devices encompass all devices aimed at detecting or preventing burglaries, or notifying household hazards. These include, for instance, garage door controls, smart locks, smart security cameras and smoke detectors.

2.3.2 User interaction: Smart home user interfaces

(43) In order to enable the connection to the smart home device, the user is usually required to complete registration on the manufacturer's smart home application. Through the application, which functions as a user interface, the user can configure, set up, and manage the connected device. The manufacturers indicate that their smart home

applications are generally available for various operating systems in order to allow consumers to connect to the smart home device from various types of devices. They can typically be accessed via mobile device app stores (in particular the Google Play store and Apple App Store), as well as via a web browser. The smart home application can be used to pair new devices, view the status of the device and control or automate the device remotely.

(44) There are many different user interfaces for controlling smart home devices and all manufacturers of smart home devices offer several options. The most common user interfaces available to users are smart mobile devices and the respective smart home applications, voice assistants, touch screens, keypads, remote controls, smart buttons, smart switches, PCs and laptops.

(45) Across all types of smart home devices and based on the total number of the monthly active users (MAUs)[20], smart home applications emerge as the most popular user interface. However, the popularity of user interfaces also depends on the smart home device type. For example, voice assistants are the most popular user interface for smart speakers, while remote controls are the most popular user interface for smart TVs.

(46) Most smart home devices can be controlled via the manufacturer's own user interface(s). However, almost all manufacturers of smart home devices also allow third-party user interfaces to connect to and control their smart home devices. Interaction through third-party user interfaces has gained traction in the smart home environment as a way to facilitate interoperability in heterogeneous environments with multiple brands.

(47) For example, the majority of smart home manufacturers have developed integration with leading general-purpose voice assistants, namely Google Assistant, Alexa and Siri.

2.4 WEARABLE DEVICES

2.4.1 Characteristics of wearable devices

(48) Wearable devices are electronic devices that can be worn and which can send and receive data wirelessly via a network. Such devices generally include sensors and are powered by an operating system. Wearable devices include products such as ear-worn devices (earphones, headphones, earbuds) and wrist-worn devices (smart watches, fitness trackers, sport watches) as well as other wearable items (for example smart clothes and shoes, smart glasses, head-mounted displays, virtual reality headsets).

(49) Wearable devices offer numerous functions to users (for example heart-rate monitoring, activity tracking, navigation, making phone calls) and can often interoperate with and function as user interfaces for smart devices. Voice assistants are also often integrated into wearable devices (most frequently, earphones, earbuds and smart watches).

[20] Based on the number of MAUs in 2019, as well as for the period 1 January 2020 to 30 June 2020.

2.4.2 User interaction: wearable devices and companion apps

(50) The vast majority of respondents' wearable devices can be used, at least for basic functions, without the users having to carry around their smart mobile device in addition to the wearable device. For instance, on fitness trackers, speed tracking and heart rate tracking are often active even if the wearable device is used independently of a smart mobile device.

(51) However, given the limited connectivity and reduced storage and processing capacity of wearable devices, connecting them to smart mobile devices unlocks a number of additional features and it is usually highly recommended by wearable device manufacturers. The connection between the wearable device and the smart mobile device is supported by a specific companion app. A companion app is a software application enabling a user, among other functionalities, to extend the mobile device's display onto the wearable device, to relay user interactions from the wearable device to the smart mobile device and to update the wearable device as needed.

(52) More specifically, depending on the wearable device type and brand, some of the health and fitness metrics tracked through the wearable device can be viewed and used exclusively on the wearable device, whilst some can only be viewed and accessed via the companion app on the smart mobile device. For example, the companion app is often able to analyse metrics in the long term, providing more detailed information in terms of historic data and training progress. Sometimes it also includes data that has been added manually. The metrics which can usually be viewed on the device itself are more limited and typically include current activity time, calories burnt, heart rate, distance, number of steps, speed, blood oxygen level and similar metrics.

2.5 CONSUMER IoT SERVICES

2.5.1 Characteristics of consumer IoT services

(53) Consumer IoT services are defined for the purposes of this sector inquiry as services that consumers can access via a smart device, through a voice assistant and/or through other user interfaces. They encompass a wide range of services, including for example creative content services, information and search services, health and fitness services, intermediation services (for example marketplaces, car-sharing services), comfort and lighting, security and shopping services.

(54) Most of these services are accessible also outside the consumer IoT sector, for instance, via laptops and PCs or smart mobile devices. However, the consumer IoT sector provides new ways to access these services (for example using voice commands) and integrate them in new ways with various smart home and/or wearable devices. For instance, users are able to program different scenarios, such as morning routines, which can involve several smart devices and services working together: the wearable device's sleep monitoring function can be connected to the alarm clock function, which in turn

can be connected to the smart home lights or thermostat as well as the coffee machine or the smart speaker providing the news.

(55) The majority of the respondents' consumer IoT services are currently available on third-party smart devices and voice assistants. The services in question are generally accessible on both Apple's operating system (iOS) and Google's operating system (Android), as well as via Alexa and Google Assistant, while fewer are also accessible via Siri, Bixby, and other voice assistants.

2.5.2 User interaction: Access requirements for consumer IoT services

(56) About half of the providers of consumer IoT services indicate that users need to register before using their consumer IoT services. Subscription fees may also be charged, sometimes only in relation to a premium service or offer. Respondents have mentioned other registration requirements, including optional registration or minimum-age requirements.

(57) In order to access certain consumer IoT services on some smart home devices, the user is required to link the smart home account with the consumer IoT service account or a voice assistant account.

2.6 INTERACTION BETWEEN CONSUMER IOT PRODUCTS AND SERVICES

2.6.1 Voice assistants and smart home devices

(58) Voice assistants are becoming key entry points to the smart home, in the sense that they allow companies to establish interoperability and to build a smart home environment based on products from different manufacturers. Almost all of the respondents' smart home devices can be controlled by a voice assistant, with Alexa and Google Assistant by far the most popular voice assistants chosen by the responding smart home device manufacturers for this purpose. The replies to the Commission's questionnaires and the submissions to the public consultation on the preliminary report indicate that voice assistants are still used less frequently as a smart home user interface compared to smart home applications. However, several respondents stress that voice assistants have only recently been added as a user interface for their devices.

(59) In their submissions to the public consultation, Amazon and Google underline the fact that, currently, the importance of voice assistants is limited compared to other interfaces (in particular smart mobile devices). At the same time, Google also submits that, "*Google Assistant currently works with over 50,000 smart home devices from more than 10,000 popular brands, and we are adding new brands all the time.*" Similarly, according to an Amazon statement from January 2020, "*there are now hundreds of millions of Alexa-enabled devices in customers' hands and customers interact with*

Alexa billions of times each week. Customers rely on Alexa to control smart home devices hundreds of millions of times each week"[21].

(60) The majority of the voice assistant providers say that the largest part of their MAUs use the voice assistant on the providers' own smart devices rather than on third-party smart devices and, in some instances, exclusively on their own smart devices.

(61) Voice assistants can interoperate with smart devices by being directly built into the devices themselves, by controlling the smart devices through an application, or by connecting to them via so-called "works with" solutions. In a "works with" scenario, the voice assistant runs on a separate device, usually a smart mobile device or a smart speaker, which carries a microphone and via which the voice assistant can be activated[22].

(62) More than a third of the manufacturers of smart home devices have a voice assistant built into at least one of their devices and these devices are mostly smart speakers and smart TVs. All providers of voice assistants that manufacture smart home devices have their own voice assistant built into their devices. On most of these devices, the first-party voice assistant is the only voice assistant built into the device. Moreover, only two of the general-purpose voice assistants, namely Alexa and Google Assistant, are built into third-party smart home devices. Siri and Bixby are only built into Apple and Samsung's smart devices respectively.

(63) Through built-in integration, users can access all of the functions supported by the third-party voice assistant directly from the manufacturer's smart home device, including control of other smart home devices and access to third-party consumer IoT services.

(64) Around two thirds of the manufacturers provide the possibility to connect to and control their smart home devices using more than one voice assistant. In most cases, this is achieved via a "works with" solution. This is because only a few smart home devices have more than one voice assistant built into the device. Instead, many manufacturers of smart speakers, for example, market different smart speaker models – one for each of the general-purpose voice assistants that are available on third-party devices, namely Google Assistant and Alexa.

(65) There are two categories of smart home devices that have more than one voice assistant built-in. A first category are smart home devices that have two or more general-purpose voice assistants built-in, that is, Alexa and/or Google Assistant and/or Bixby. Although the user is able to switch between those voice assistants by changing the settings, concurrent use of voice assistants - that is, switching between the voice assistants

[21] Amazon (30 January 2020), *Amazon.com Announces Fourth Quarter Sales up 21% to $87.4 Billion*, 30 January 2020, retrieved on 11 October 2021, from https://ir.aboutamazon.com/news-release/news-release-details/2020/Amazoncom-Announces-Fourth-Quarter-Sales-up-21-to-874-Billion/default.aspx

[22] For more information on the "works with" solution, please see paragraph 197 in Chapter 5.

interchangeably by, for example, using different activation words - is reportedly not possible on any of the smart home devices in question.

(66) A second category are smart home devices that have Alexa built-in, in addition to the device manufacturer's own specialised voice assistant. For example, Deutsche Telekom's smart speaker has Alexa built-in in addition to Deutsche Telekom's own voice assistant Magenta. In some cases, these voice assistants can be used concurrently.

2.6.2 Voice assistants and wearable devices

(67) Around two thirds of the manufacturers of wearable devices have a voice assistant available on at least one of their devices. More than half of these respondents mention Google Assistant and less than a third mention Alexa. It appears that none of the respondents have more than one voice assistant available on their wearable devices. Google Assistant is included automatically on all wearable devices that use Google's operating system Wear OS. Siri is available on Apple Watch but not on third-party wearable devices.

2.6.3 Voice assistants and consumer IoT services

(68) Although access to consumer IoT services via smart mobile devices is the most frequent way to access consumer IoT services, access via a voice assistant is another means to access services that is frequently indicated by the respondents. This is especially the case for certain types of smart devices such as smart speakers. Overall, almost half of the respondents' consumer IoT services are currently accessible via voice assistants and of these, around two thirds are accessible via more than one voice assistant[23].

(69) According to the replies, Google Assistant and Alexa are the most popular choices to enable voice assistant access to the respondents' consumer IoT services.There are thousands of consumer IoT services available via each of these voice assistants.

(70) The majority of consumer IoT service providers build integrations with voice assistants by developing voice applications. These voice applications are known as "skills" for Alexa, "actions" for Google Assistant, "shortcuts" for Siri and "capsules" for Samsung's Bixby.

(71) The leading voice assistant providers are themselves also providers of various consumer IoT services, accessible via the providers' own voice assistants. In some cases, these services can also be accessed via third-party voice assistants. Among the services provided by the voice assistant providers, the most frequently offered are online information and search services, online creative content services, and online shopping services.

[23] However, since concurrent use of voice assistants is not possible on most smart devices (see paragraph 65), the users are usually not able to switch from interacting with a certain consumer IoT service via one voice assistant to interacting with that service via another voice assistant.

2.6.4 Consumer IoT services and smart home devices

(72) Most consumer IoT services available through the respondents' smart home devices can be accessed via a mobile device application and/or a voice assistant. On some devices, such as smart TVs, the services can be integrated directly into the device or downloaded via the device's app store.

(73) The number of consumer IoT services accessible via each smart home device depends largely on the type of device. For example, smart home appliances such as light bulbs, thermostats or switches typically only provide access to comfort and lighting services. Security devices provide access to a range of consumer IoT services related to security, such as alarms, camera surveillance etc. Smart speakers and smart TVs seem to give access to the widest selection of consumer IoT services, ranging from creative content services, intermediation services, information services, and search services, to shopping services.

(74) In the context of the public consultation on the preliminary report, one stakeholder submitted that usage of its consumer IoT services via smart home devices currently accounts for a limited portion of usage compared to other channels, such as web browsers and mobile apps.

(75) A specific type of service relevant to certain types of smart home devices, such as smart dishwashers, smart printers or smart coffee machines, are automatic product re-ordering services, which allow users to automatically re-order consumables (such as dishwasher tabs, ink cartridges or coffee beans) when their supply levels run low.[24] The choice of product brands offered to the user is typically decided by the service provider.

(76) Similarly, some smart home devices make consumer IoT services available that can suggest purchases to users, or create shopping lists based on profiling of the user. Such purchasing suggestions are usually made by the consumer IoT service provider and are mostly based on previous purchases or other past behaviour of the user.

2.6.5 Consumers IoT services and wearable devices

(77) Some of the consumer IoT service providers indicate that their services are also available on wearable devices and may be accessed either via a smart mobile device, a voice assistant or by being installed as an application directly on the wearable device.

(78) In fact, almost half of respondents indicate that one or more of their wearable devices enable users to download and install applications. The most common applications available via the respondents' wearable devices fall within the following categories: fitness applications, timers, alarms, reminders, calendars, music and podcast players, weather, maps and navigation, watch faces[25] and sleep-related applications.

[24] These types of services are also known as automatic replenishment services.
[25] A watch face is a watch's home screen.

(79) Three out of four manufacturers of wearable devices are themselves active in the provision of consumer IoT services, and of these, the vast majority declare that one or more of their consumer IoT services is accessible via their own and/or third-party wearable devices.

2.7 KEY FINDINGS

The findings of the sector inquiry indicate that an increasing number of devices and services are becoming "smart", so that users have the possibility to access a progressively wider range of interconnected devices and services in and outside their homes.

As the overall accessibility of the different smart devices and consumer IoT services depends on the user interface used, the consumer's daily routines become shaped around the choice of such interface. In this respect, general-purpose voice assistants play an increasingly important role because they allow for the connection of all of the components, including various brands of smart devices and consumer IoT services, in a single, integrated environment.

A limited number of general-purpose voice assistants is currently available. Alexa, Google Assistant and Siri are the most popular general-purpose voice assistants in the consumer IoT sector.

Despite the growing popularity of voice assistants, the smart mobile application or companion app remains the most popular user interface to access smart home and wearable devices as well as consumer IoT services. In that sense, smart mobile devices and their operating systems also play an important role in the consumer IoT sector. Google's Android and Apple's iOS are the leading operating systems for smart mobile devices.

3 CHARACTERISTICS OF RESPONDENTS

(80) This chapter describes the main characteristics of the companies and organisations that responded to the sector inquiry questionnaires. It identifies, for instance, the distribution of respondents in terms of size and areas of activity within the consumer IoT sector. After a global overview in Section 3.1, the chapter describes the main characteristics of the respondents to each questionnaire (Sections 3.2 to 3.6).

3.1 OVERVIEW OF RESPONSES

(81) Overall, as set out in Table 1, the Commission received responses to the questionnaires from more than 200 companies active in the manufacturing of smart devices, provision of voice assistants and/or the provision of consumer IoT services,[26] as well as from 14 standard-setting and industry organisations.

Table 1: Number of respondents to each questionnaire

Smart home device manufacturers	87
Voice assistant providers	13
Wearable device manufacturers	29
Consumer IoT service providers	72
Standard setting and industry organisations	14
Total	**215**

(82) The number of respondents that declared themselves to be active in different categories of consumer IoT products and services is listed in Table 2 below.[27]

Table 2: Distribution of respondents across different categories of consumer IoT products and services

Consumer IoT product or service category	Number of active respondents
(a) Operation of cloud platforms for the IoT	51
(b) Provision of operating systems for smart devices	27
(c) Provision of home automation systems (including manufacturing of hubs or gateways)	50
(d) Manufacturing of smart speakers	31
(e) Manufacturing of connected video entertainment devices	19
(f) Manufacturing of other smart home devices (smart	60

[26] For the purpose of the figures in this chapter, responding companies belonging to the same group are counted as a single respondent.

[27] For the purposes of this table, replies from companies that responded to more than one questionnaire, as well as replies from companies belonging to the same group, are counted only once.

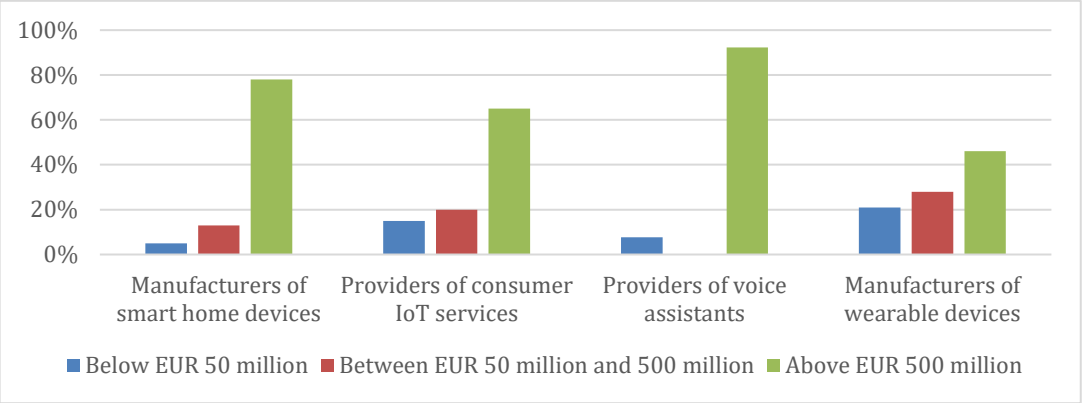
appliances, lighting systems, security devices)	
(g) Manufacturing of smart home user interfaces (e.g. remotes, dedicated touch-screens) other than wearable devices and smart mobile devices	37
(h) Provision of smart home applications which serve as smart home user interfaces	63
(i) Provision of online creative content services	56
(j) Provision of online shopping services	53
(k) Provision of online information and search services	28
(l) Provision of online intermediation services	28
(m) Provision of online security services	12
(n) Provision of online comfort and lighting services	27
(o) Provision of online health and fitness services	27
(p) Provision of voice assistants	13
(q) Manufacturing of wearable devices	36
(r) Manufacturing of smart mobile devices (smart phones and tablets)	18
(s) Other consumer IoT products and services	52
(t) Other non-consumer IoT products and services	54

(83) A significant number of respondents are simultaneously active in several categories. A large majority of respondents (72%) are active in at least two of the listed categories, around half (55%) in at least three, slightly less than half (45%) in at least four categories, and around one third (34%) sell products or provide services in five or more different categories.

(84) Many of the respondents are very large companies, in terms of either turnover or number of employees.

(85) Across questionnaires, only a limited number of respondents (10 to 20%) indicate that they generate (at group level) a worldwide turnover of less than EUR 50 million. A slightly larger percentage (15 to 30%) have turnovers between EUR 50 million and 500 million, whereas a majority of respondents report that their turnover is above EUR 500 million (from 50% of respondents in the case of wearable device manufacturers, and up to 90% in the case of voice assistant providers).

Figure 1: Distribution of respondents by 2019 worldwide turnover (% of total respondents per questionnaire)



(86) Similarly, a vast majority of respondents have more than 1 000 employees, while companies with less than 50 employees account for less than 10% of the total respondents (for each of the questionnaires).

(87) More than two thirds of the addressees are publicly listed companies or, if not listed, belong to larger multinational groups with a significant number of shareholders (including venture capital firms, investment or pension funds and institutional investors), which are active in multiple business areas outside consumer the IoT sector (for example technology and digital services, media, telecommunications, consumer electronics, industrial automation, automotive).

(88) A more limited number of respondents are smaller, often privately owned companies that specialise in a single business area or limited business segments thereof. Among these smaller entities, there are also a number of start-ups and not-for-profit entities.

(89) Aside from the questionnaires that were sent out, the Commission also welcomed spontaneous submissions from stakeholders that showed an interest in participating in the sector inquiry. The public consultation on the preliminary report also offered an additional opportunity for any organisation to submit its views on the Commission's preliminary findings.

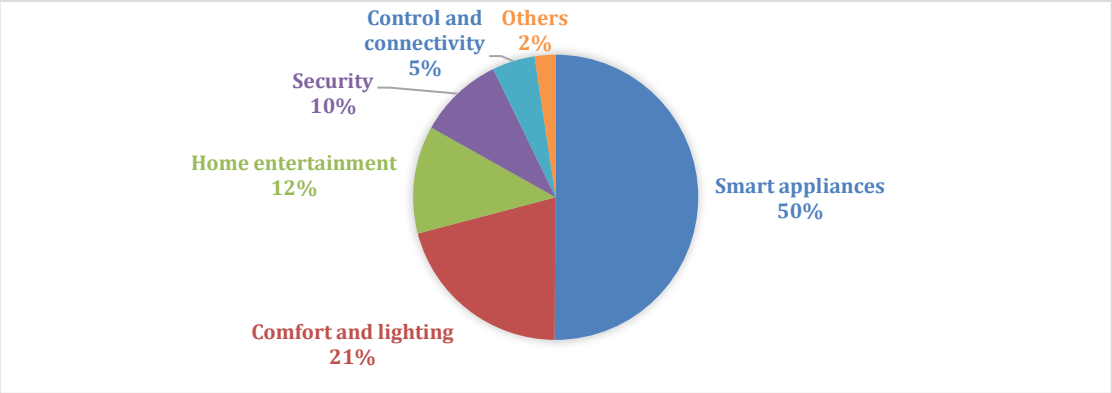
3.2 MANUFACTURERS OF SMART HOME DEVICES

(90) The Commission received replies from 87 companies active in the manufacturing of smart home devices and/or related products such as home automation systems supporting the functioning of smart home devices. Based on figures provided by the respondents, their smart home devices had a combined total of approximately 52 million MAUs in Europe in June 2020.

(91) In terms of the number of smart home devices manufactured by the respondents, smart appliances constitute the largest product category, as illustrated by Figure 2 below, followed by comfort and lighting, and then home entertainment and security. The "control and connectivity" category includes home automation systems, hubs and

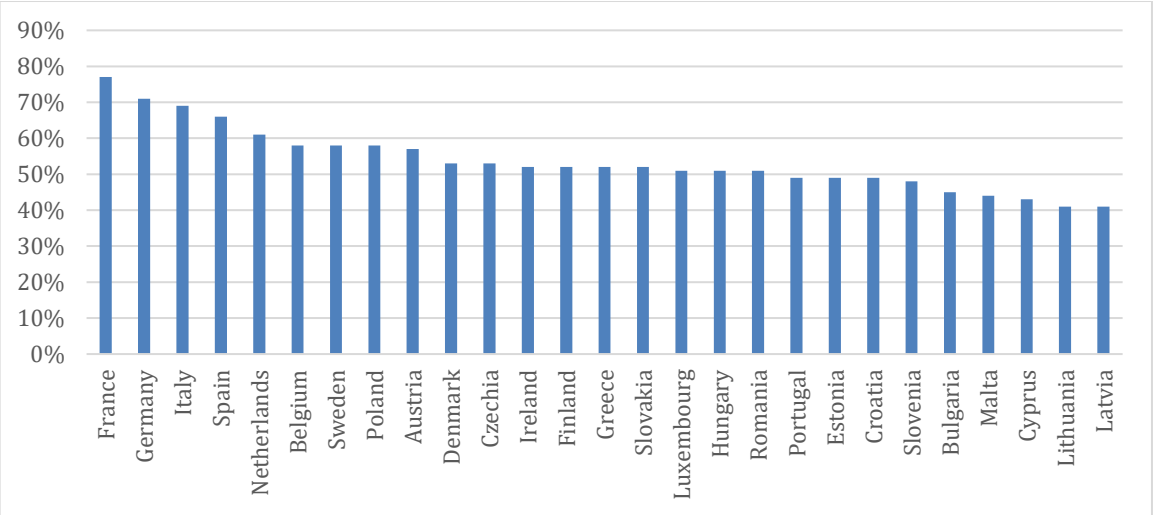
gateways, and all smart home user interfaces other than wearable devices and smart mobile devices. The category "others" includes smart home devices outside the four main product categories outlined above, such as products used for child monitoring, pet care and home healthcare.

Figure 2: Distribution of respondents' products per smart home device category (% of total smart home devices manufactured by the respondents)



(92) Respondent manufacturers were also asked to indicate the Member States in which they make their smart home devices available, and provided detailed replies with regard to a total of over 1 000 different smart home device types. Figure 3 below shows the distribution of available smart home devices across the EU. The availability of the surveyed devices varies significantly, ranging from more than 70% (out of the total number of device types) available in France and Germany, to 41% in Latvia and Lithuania.

Figure 3: Availability of respondents' smart home devices in the EU (% of total devices)



(93) The respondents' replies confirm the growing trend of consumer IoT for this segment. The total number of shipped items for respondents' smart home devices increased both worldwide (by almost 30%) and within the EU (by almost 40%) from 2018 to 2019. Similarly, registered users of respondents' smart home devices more than trebled

between 2018 and 2020 in the EU whereas MAUs of respondents' devices almost doubled in the same period.

3.3 VOICE ASSISTANT PROVIDERS

(94) The Commission received responses to the questionnaire addressed to voice assistant providers from 13 companies, including both general-purpose and specialised voice assistants.

(95) Voice assistant providers generally belong to very large multinational groups. Only one respondent is a smaller privately-owned company, whose activities focus on the provision of smart devices.

(96) The respondents provide a wide range of smart devices and consumer IoT services. On average, each respondent is active in 11 of the 20 product and service categories covered by the sector inquiry (see Table 2 above), showing a strong and growing presence in the overall consumer IoT sector. A particularly high percentage of responding voice assistant providers is also active in the provision of online creative content services (84%), the operation of cloud platforms (76%) and the manufacturing of smart speakers (69%).

(97) The number of registered users of respondents' voice assistants increased across all Member States from 2018 to 2019, and into the first six months of 2020. Separately, the combined total of MAUs[28] that respondents recorded in January 2020 was almost five times higher than in January 2018, showing the growth in both the availability and use of voice assistants. This significant growth in MAUs continued in 2020, with almost double the number of MAUs recorded by respondents in June compared to January. General-purpose voice assistants seem to be driving the take-up of this user interface. Based on figures provided by the respondents, providers of general-purpose voice assistants reported, on average, over 100 times more MAUs in Europe in June 2020 than the providers of specialised voice assistants.

3.4 WEARABLE DEVICE MANUFACTURERS

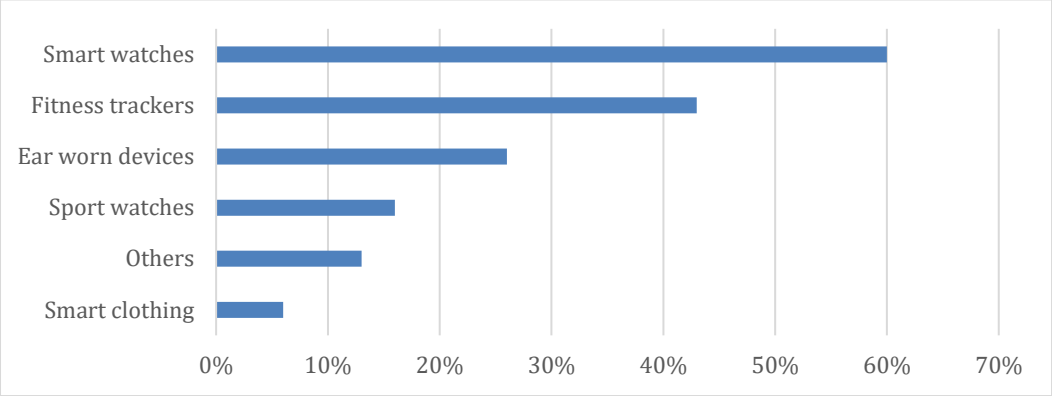
(98) The Commission received responses to the questionnaire addressed to wearable device manufacturers from 29 companies.

(99) Having regard to their activity in the wearables sector, almost half (47%) of the respondents indicate that they manufacture more than one type of wearable device. The most commonly produced wearable devices among the respondents are smart watches, fitness trackers and ear-worn devices (produced respectively by 60%, 43% and 26% of the respondents). Fitness trackers were also the most shipped wearable device among the respondents' devices, representing approximately half of all shipped items in 2019

[28] MAUs are calculated by most respondents as those users who interacted with the voice assistant at least once in the previous month.

and in the first half of 2020. Furthermore, some respondents are active in the manufacturing of sport watches, smart clothing and other types of wearable devices (such as head-mounted displays, wearable cameras and body sensors).

Figure 4: Distribution of manufacturers across wearable device categories (% of respondents)



(100) Based on figures provided by the companies, their devices had a combined total of approximately 14.5 million MAUs in the EU in January 2020. Their MAUs within the EU moreover increased by over 40% between January 2018 and January 2020. Other figures provided by respondents confirm the growing user reach of wearable devices, with about 40% more registered users in 2019 compared to 2018. This growth is set to continue based on figures provided for the first half of 2020.

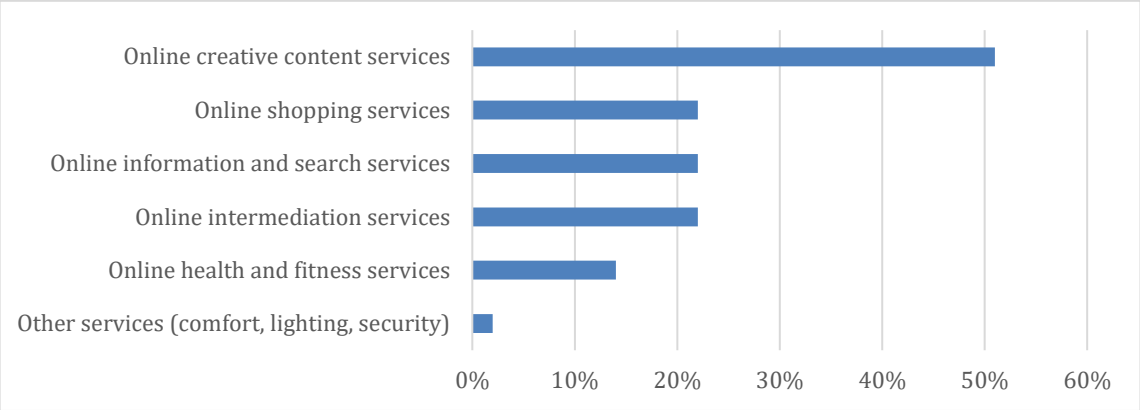
3.5 CONSUMER IoT SERVICE PROVIDERS

(101) The Commission received information from 72 providers of consumer IoT services.

(102) In terms of characteristics, there is great variety amongst the respondents. The core business of respondents ranges from communication and entertainment to banking and financial information services, to operation of digital platforms, as well as book publishing. They often also offer services outside the IoT, for example offline and online media services.

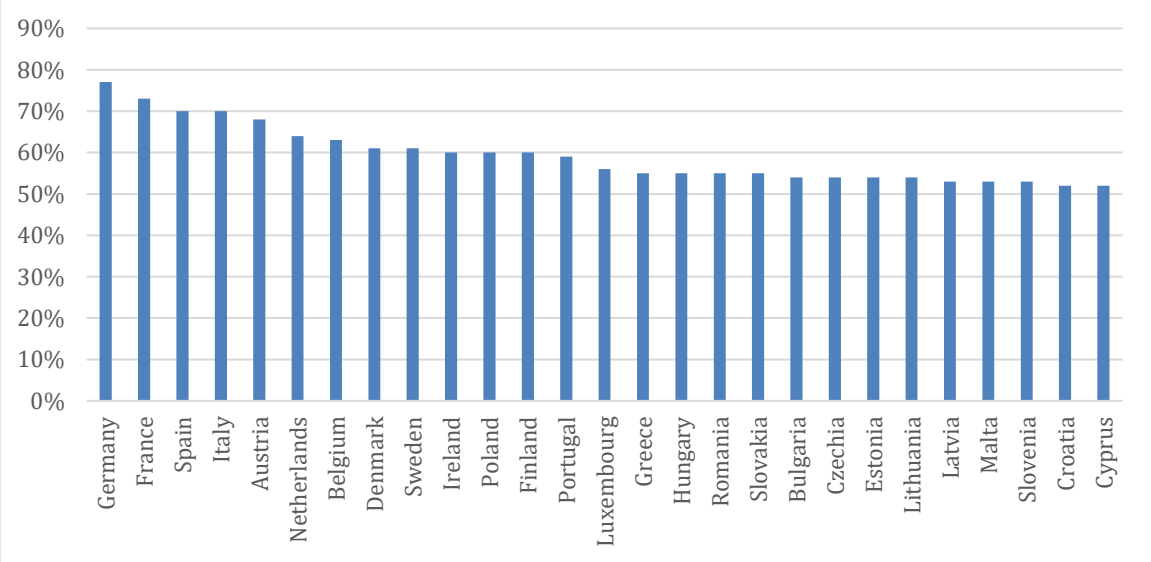
(103) Respondent providers are active in all the service categories covered by the sector inquiry (see Table 2 above), with a quarter active in at least two service categories. Over half of the respondents are creative content providers, such as radio broadcasting companies, music streaming services, video-on-demand (VOD) and e-book providers. This is followed by providers of online shopping services, intermediation services and information and search services (22% in each respective area). Only 2% of respondents provide other types of services (for example online comfort and lighting and security services).

Figure 5: Distribution of providers across consumer IoT service categories (% of respondents)



(104) In each EU Member State, at least 53% of the surveyed services are available. Figure 6 shows the availability of the respondents' services in each Member State. The Member States with the highest availability of respondents' IoT services are Germany (77%), France (73%), Spain and Italy (70% each).

Figure 6: Availability of respondents' consumer IoT services in the EU (% of total consumer IoT services)



(105) As regards the business models used to commercialise IoT services, respondent providers use a variety of these models. For instance, some services are ad-funded, while others are subscription-based; based on single transactions with users; or provided without charge to users (with or without additional paid features).

(106) Around one in four of the consumer IoT services provided by the respondents are provided free of charge to consumers: these mostly include services offered by intermediation platforms (where intermediation fees are charged to businesses rather than to consumers) and online services that are ancillary or complementary to the respondent's main product or service. The "other" category includes mixed business

models, such as “freemium” services (combining ad-funded and subscription-based models) or subscription-based services that offer additional paid features on a per-transaction basis.

(107) The offer of creative content services, such as VOD, radio and music streaming services, sometimes passes through third-party distributors, such as for example telecommunication operators in the case of audio-visual services. The precise nature of such distribution arrangements varies but may include the integration of different first- and/or third-party services into a bundled offer to the user.

(108) The most popular services vary according to the type of device and/or category of service. For example, the most popular creative content services calculated on the basis of the MAUs of these services on the respondents’ smart home devices in June 2020 were Spotify, TuneIn, Amazon Music and Amazon Video, Netflix, Deezer, Disney Plus and YouTube. On wearable devices, the most popular health and fitness applications in terms of the MAUs in 2019, on the basis of respondents’ replies, include different Strava applications, Google Fit, Nike Run Club, Map My Run, My Fitness Pal, Adidas Train, and Calm.

3.6 STANDARD-SETTING AND INDUSTRY ORGANISATIONS

(109) The Commission received 14 responses to the questionnaire addressed to standard-setting and industry organisations. The responding organisations are diverse in nature and with regard to the scope of their activities. Around a third are international standardisation organisations, active in the development of standards relevant for the functioning of the consumer IoT sector and for wider industries, such as telecommunications, internet and electronic technologies. These organisations include, for instance, the European standardisation organisations [29] the International Telecommunications Union (ITU), the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC).

(110) Several respondents are technical professional organisations and international associations whose main purpose is to foster technological innovation, share knowledge and strengthen dialogue and interaction among players in a specific industry. Some of these associations develop and promote open standards relevant for the consumer IoT environment. Generally, their membership is composed of both public institutions and private members (including corporate entities and/or individuals).

(111) Finally, other respondents are private not-for-profit organisations and partnerships (alliances) between undertakings operating in the consumer IoT sector. These organisations and partnerships are committed to enabling and promoting interoperable

[29] Namely, the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI), pursuant to Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation.

consumer IoT ecosystems through the adoption of particular standards and/or protocols, such as standardised wireless technologies; connectivity, data transmission and networking protocols. These organisations and partnerships (which include, among others, EnOcean Alliance, LoRa Alliance, Mioty Alliance and Thread Group) are active internationally and have a substantial membership, ranging from several dozen to more than 100 undertakings.

3.7 KEY FINDINGS

Respondents to the sector inquiry are for the most part large corporations, both in terms of number of employees and in terms of turnover. However, the sample also includes SMEs, start-ups or specialised service providers. Most respondents sell products or provide services in at least two categories covered by the sector inquiry, and around half sell in more than four categories.

Voice assistant providers are among the largest players and have the most widespread presence in all areas of consumer IoT activity, showing a growing tendency towards the creation of integrated consumer IoT solutions (from the operation of cloud platforms, to the manufacture of smart speakers, smart streaming devices, and the provision of related consumer IoT services).

Smart home device manufacturers most commonly produce smart home appliances, comfort and lighting systems and home entertainment devices, including smart speakers, while the majority of consumer IoT service providers are creative content providers, or operators of online shopping and intermediation services.

The availability of the surveyed smart home devices and consumer IoT services varies across the EU, with the highest percentage of them being available in the four largest Member States (Germany, France, Italy and Spain). However, at least 50% of the surveyed smart home devices, and 40% of the surveyed services, are available in each Member State.

Shipments of smart devices, as well as the number of registered users and monthly active users have consistently increased from 2018 throughout the first half of 2020.

4 MAIN FEATURES OF COMPETITION

4.1 OVERVIEW

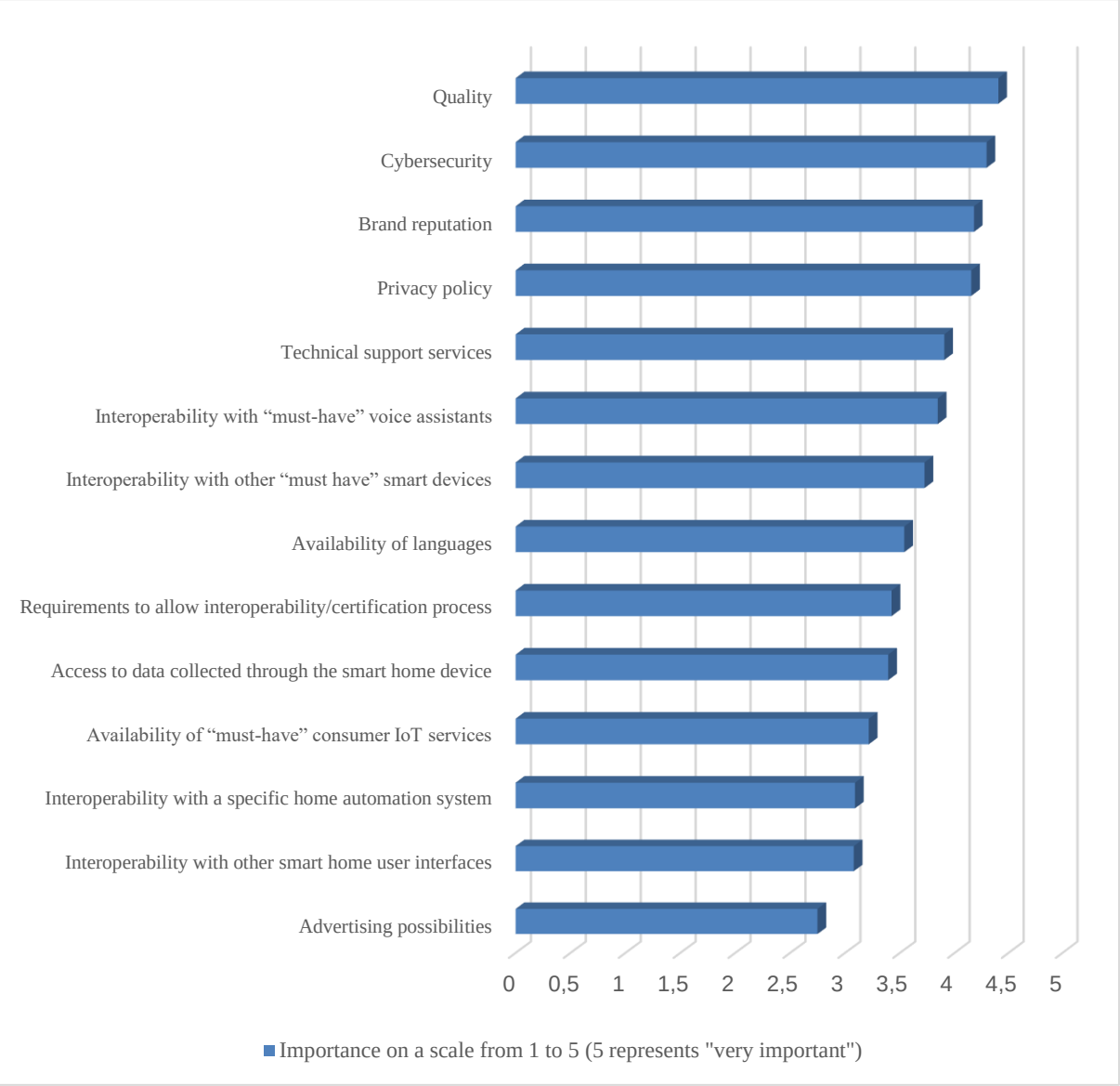
(112) This chapter looks at the main parameters of competition in the consumer IoT sector identified by respondents (4.2), the perceived barriers to entry and expansion (4.3), the competitive position of leading players (4.4), the respondents' acquisitions and business strategies (4.5) and the expected evolution of competition (4.6).

4.2 MAIN PARAMETERS OF COMPETITION

(113) The respondents were asked about the importance of various factors that play a role in competition. First, from the perspective of competing for integration with, for example, smart home devices, consumer IoT services or voice assistants, and second, from the perspective of competing for users.

(114) As Figure 7 shows, the manufacturers of smart home devices indicate that the quality, cybersecurity, brand reputation and privacy policy of their own devices play a crucial role when competing with other smart home devices for integration with other devices, services, voice assistants and other smart home user interfaces.

Figure 7: Smart home device manufacturers - Importance of certain factors for competing with other smart home device manufacturers for integration on or interoperability with other smart home devices, consumer IoT services, voice assistants and other smart home user interfaces

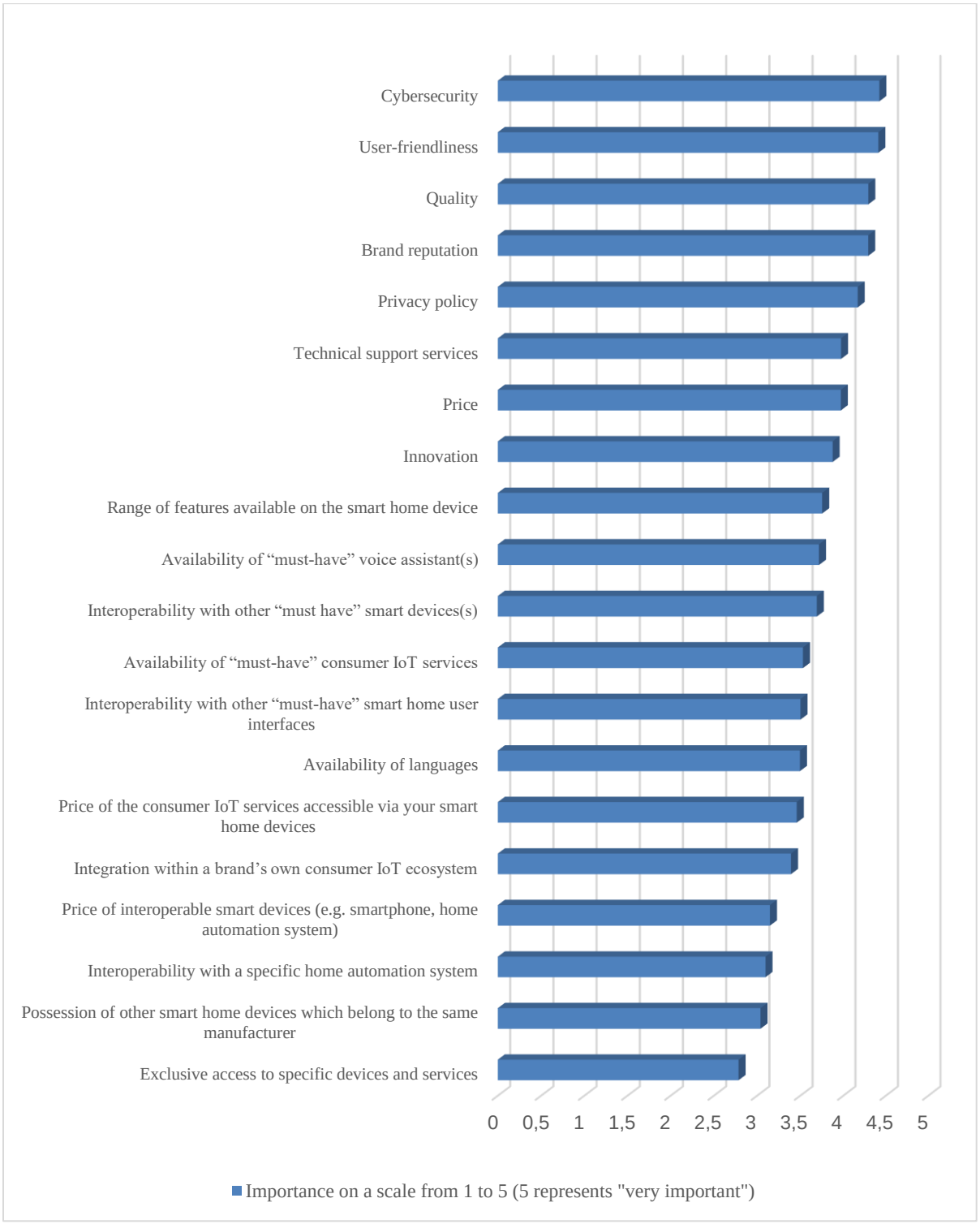


(115) As regards competing directly for users, Figure 8 shows that similar factors play the most important role. However, user friendliness and technical support services are also indicated as among the most important features. This is not surprising, given that many smart home device categories are still relatively nascent and users are still in the learning phase of being able to operate and use these devices with ease.

(116) Price is also an important factor, but it does not feature among the most important. This suggests that competition among smart home device manufacturers is primarily driven by quality. However, several respondents note that there is strong price competition in the smart speakers category, between the so-called first-party device manufacturers (i.e. those which have their own smart home user interface, that is, a voice assistant, and

have launched their own branded smart speakers) and third-party device manufacturers. The prices of the former are much lower than those of the latter.

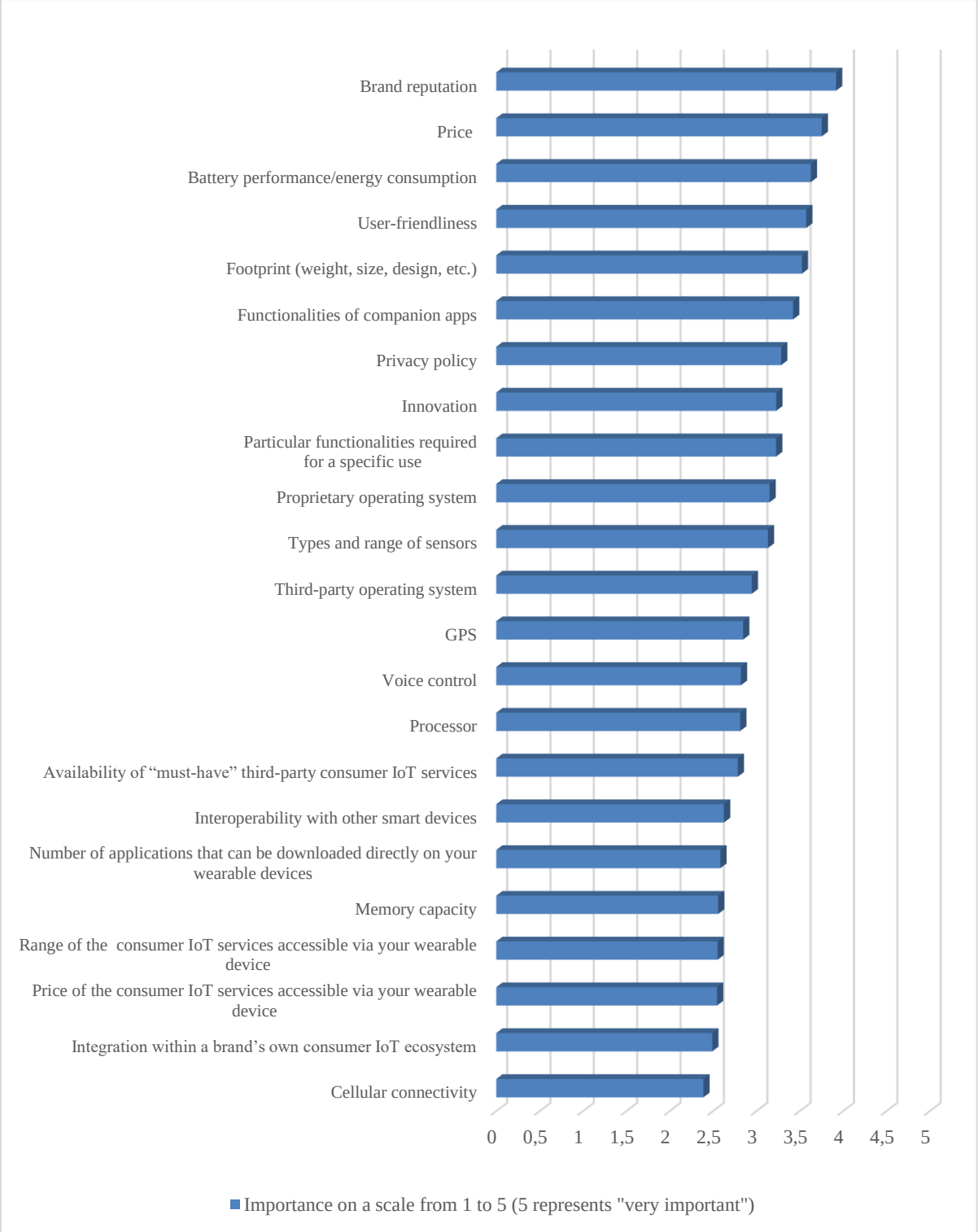
Figure 8: Smart home device manufacturers - Importance of certain factors for competing with other smart home device manufacturers for users



(117) Regarding wearable devices, as Figure 9 shows, brand reputation and price competition are the most important factors when competing for users. This is particularly true for smart watches and fitness trackers. The quality of user experience strongly depends on

the capacity and reliability of the batteries of these devices, as well as on their user friendliness.

Figure 9: Wearable device manufacturers - Importance of certain factors for competing with other wearable devices for users



(118) Regarding consumer IoT services, as Figure 10 shows, the most important factors of competition for the integration of a consumer IoT service with third-party smart devices

are quality, brand reputation, cybersecurity and the number of users of the consumer IoT service. The latter demonstrates that providers of consumer IoT services can benefit from the network effects of a large number of users, including when it comes to integration on smart devices, which may not have, or may not offer, unlimited slots for carrying more than one or a few providers of consumer IoT services. In this context, a broadcaster respondent points out that the large number of users of global over-the-top media service providers gives them unattainable competitive advantages *vis-á-vis* smaller players. As shown by Figure 11, quality, brand reputation, user-friendliness and prices are the most important factors for competition for users.

Figure 10: Consumer IoT Services - Importance of certain factors for competing with other consumer IoT services for presence on third-party smart devices

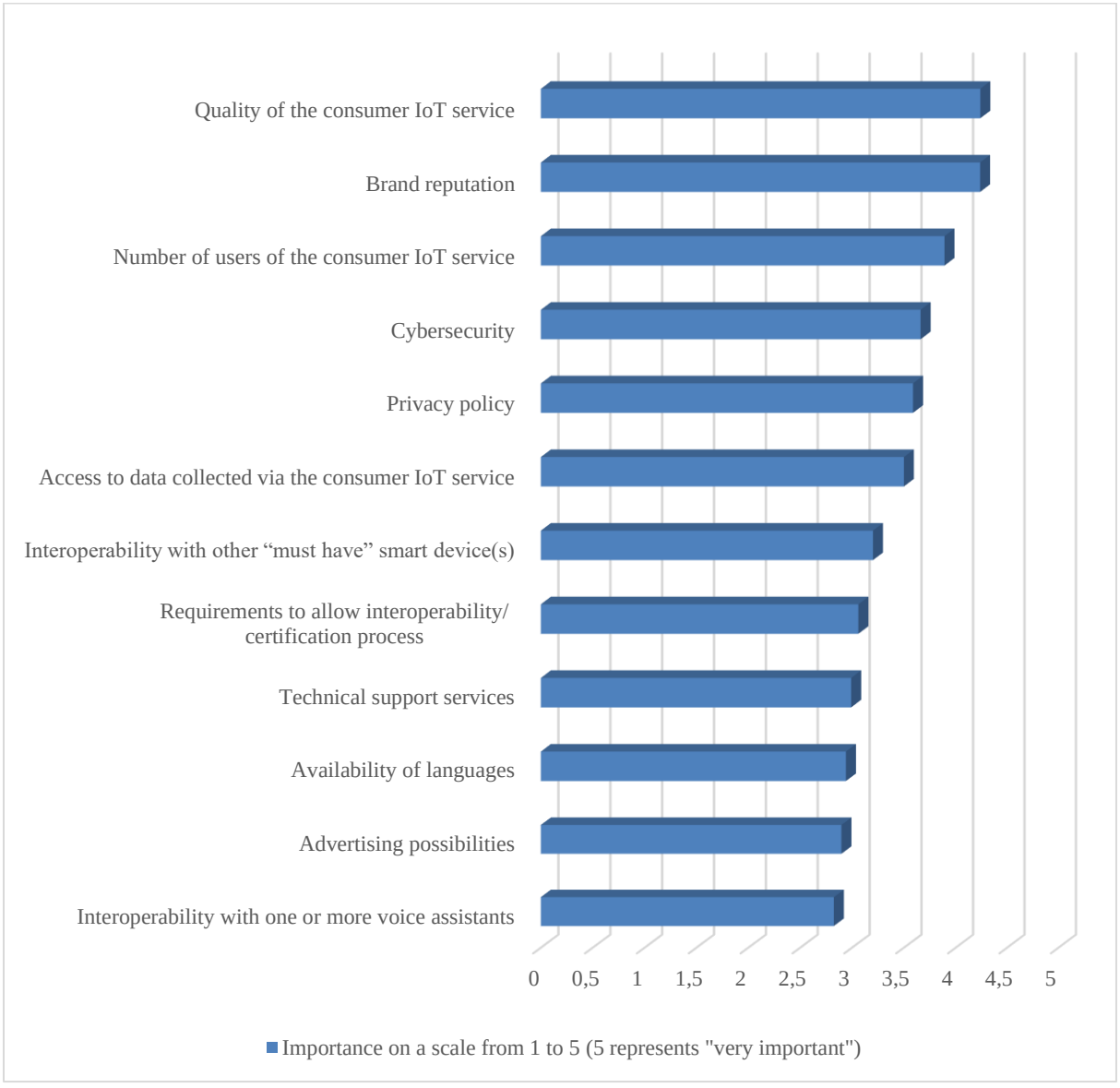
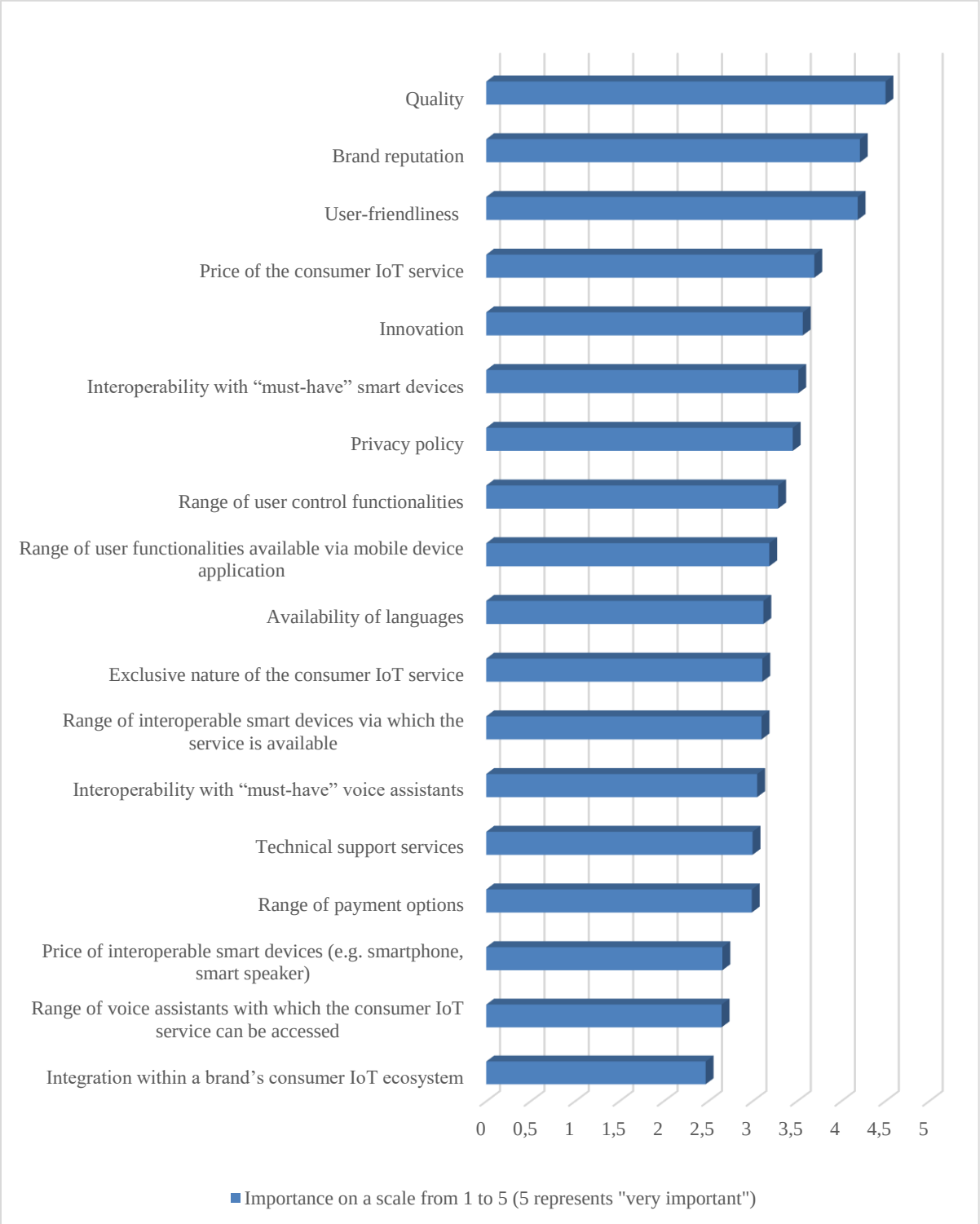
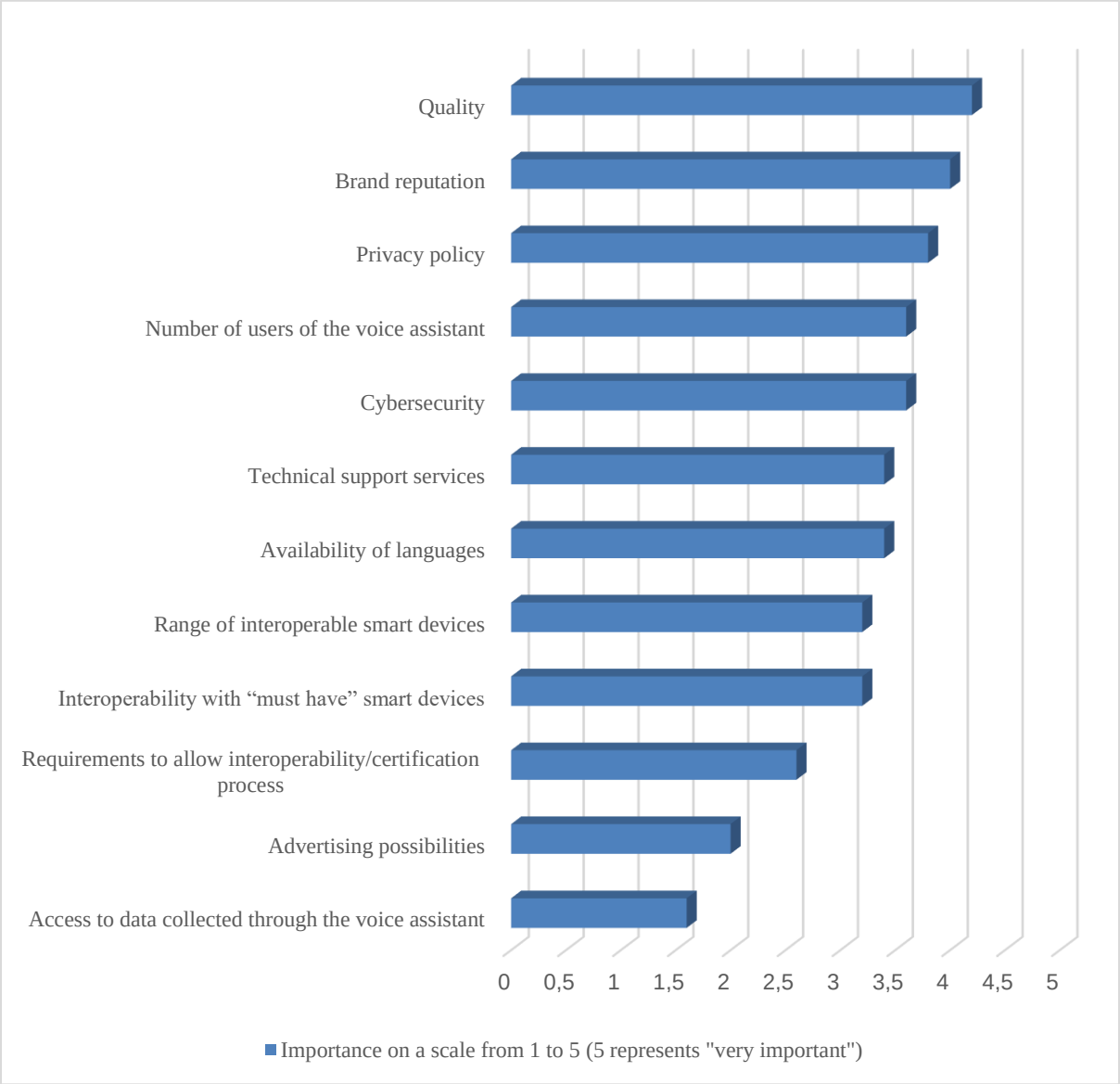


Figure 11: Consumer IoT Services - Importance of certain factors for competing with other IoT services for users



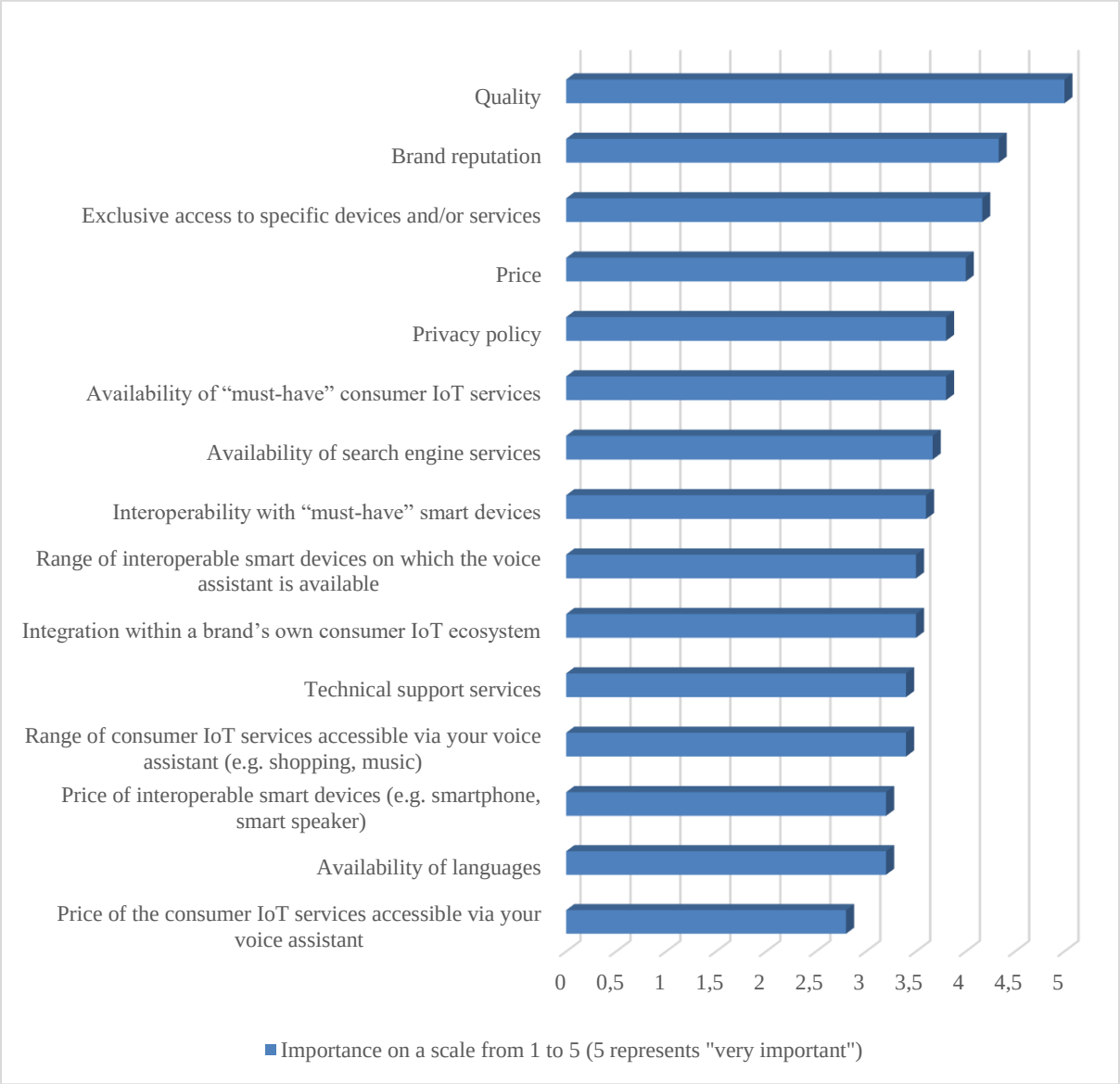
(119) Regarding voice assistants, Figure 12 shows that, in addition to quality, brand reputation and privacy, the number of users plays a crucial role in competition between voice assistants for integration with a third-party smart device. As in the case of consumer IoT services, this demonstrates the network effects from which voice assistants with a large user base benefit.

Figure 12: Voice assistants - Importance of certain factors for competing with other voice assistants for presence on third-party smart devices



(120) When it comes to competition between voice assistants for users, Figure 13 shows the importance of exclusive access to specific devices or services, which suggests that users choose a voice assistant as part of a broader set of devices and services to which they are an important user interface.

Figure 13: Voice assistants - Importance of certain factors of competition with other voice assistants for users



4.3 BARRIERS TO ENTRY AND EXPANSION

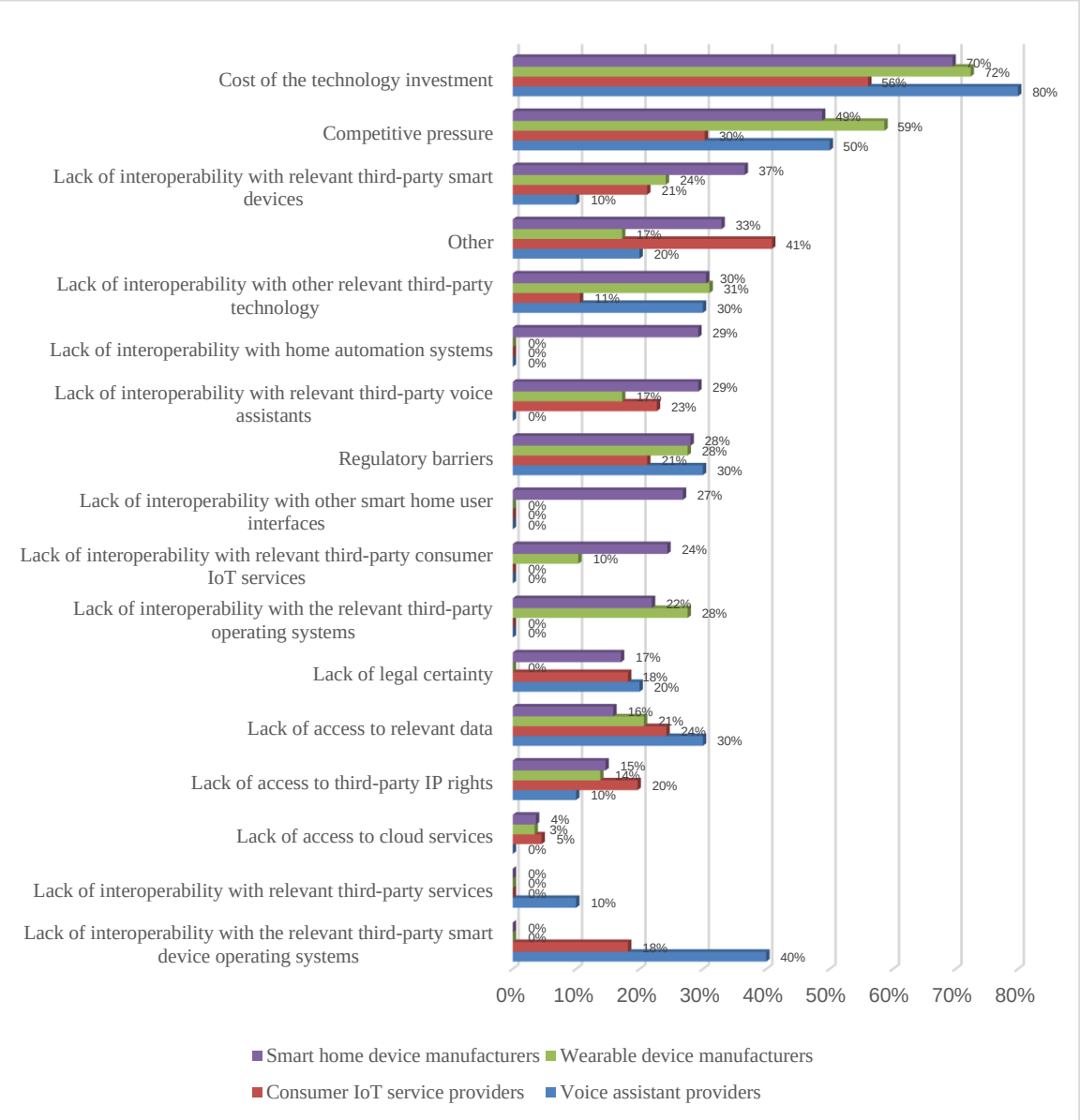
(121) The respondents in each consumer IoT segment covered by the sector inquiry were asked to mark potential obstacles or entry barriers to developing and launching smart home and wearable devices, consumer IoT services and voice assistants.

(122) As Figure 14 shows, in each consumer IoT segment, the respondents to the question indicate the cost of the technology investment and the competitive situation as the main existing barriers to entry or expansion[30]. The replies also show that the various

[30] The figures represent, per consumer IoT segment, the percentage of the respondents to the question that mark a given factor as an existing barrier to entry or expansion.

interoperability issues, the lack of access to data as well as regulatory barriers are also seen as obstacles to entry and/or expansion in the relevant markets.

Figure 14: Barriers to entry or expansion



(123) Several respondents, across all consumer IoT segments, highlight the costs of technology investment as one the highest barriers to entry and/or expansion. In this respect, several manufacturers of smart devices and providers of consumer IoT services point specifically to the fact that the cost of developing cloud storage and computing for their own use is often prohibitively high and rarely justified. Cloud storage and computing are increasingly necessary for the operation of certain smart devices and services, as data storage and resource-intensive computing often cannot be carried out locally on the device. As a result, a significant number of smart device manufacturers and service providers depend on the infrastructure of well-established cloud service providers (for example Amazon, Microsoft, Alibaba and Google). One of the respondents, which also offers cloud services to third parties, points out that the possibility of buying access to cloud services, instead of developing their own, facilitates entry, as it decreases the technological investment barrier. This dependence on the main actors, however, may come at a price: as other respondents note, the lack of interoperability of data stored and processed in the various clouds makes switching very costly.

(124) Most (80%) of the voice assistant providers indicate that the costs of technology investment is a high barrier to entry into the voice assistant market. In particular, general-purpose voice assistants (i.e. those that could compete with Alexa, Google Assistant, Siri and Bixby) are expensive to develop and operate. Their integration with various operating systems and third-party devices would also entail significant expenses. Finally, data is also mentioned as a key input for developing and training a voice assistant.

4.4 THE LEADING COMPETITORS IN THE CONSUMER IOT SECTOR

(125) Across all four consumer IoT segments (smart home devices, wearable devices, consumer IoT services and voice assistants), respondents have pointed to Amazon and Google as their main competitors, alongside – to a slightly lesser extent – Apple. These three players are also considered to be "must-have" brands for certain products and services (for example home automation systems, voice assistants). The features of competition nevertheless vary depending on the product or service concerned. For example, and as already indicated, there are only a few alternative voice assistant providers, whereas quite a large number of companies are active in the manufacturing of smart devices and the provision of consumer IoT services.

(126) A large number of respondents, across all consumer IoT segments, point out that the main obstacle to developing new products and services is the lack of ability to compete with Google, Amazon and Apple. These players have become the leading technology companies and built their own ecosystems within and beyond the consumer IoT sector by combining their own, and integrating third-party, products and services into a branded consumer offering with a large number of users.

(127) In this respect, Google's, Apple's and Amazon's general-purpose voice assistants play an important role as key points of entry to their respective consumer IoT ecosystems.

(128) Google's search engine is integrated with various search platforms such as computers, smart phones and tablets, whether through browsers or dedicated search applications. Voice assistants have the potential to become a new generation of user interfaces to search platforms.

(129) Amazon's Alexa is an access point to shopping services.

(130) Apple's Siri is not available on third-party devices and it uses Google's search engine. However, Siri provides access to a walled garden of fully integrated services, a full-range of branded proprietary smart devices and Apple's application store.

(131) Moreover, Google and Apple are providers of the leading operating systems for smart mobile devices, and as such, they also operate the two main app stores that determine access to consumer IoT services via applications.

(132) Even if other players are present across multiple products and services, Google, Amazon and Apple have a unique position in the consumer IoT sector through their ecosystems combining voice assistants with search and/or marketplaces, and/or operating systems and/or app stores. As respondents point out, with every new smart device or consumer IoT service added, these three consumer IoT ecosystems can realise growth through network effects. A submission to the public consultation on the preliminary report emphasises that such network effects may also benefit small firms and private users. However, the Commission notes that the leading players' unique position may allow them to control other firms' ability to benefit from such network effects. The leading players' position also means that they are well-placed to benefit the most from network effects and obtain unprecedented access to user (and sometimes competitor) data.

4.5 ACQUISITIONS AND COMMERCIAL ARRANGEMENTS

(133) A number of respondents have chosen to expand through vertical integration and grow their consumer IoT business through acquisition(s) and/or joint ventures. Overall, 16.5% of respondents indicate that they made acquisitions and/or created joint ventures since January 2017, with a view to integrating or developing their economic activities in the consumer IoT sector. In total, around 90 different transactions are reported by these respondents, with a total value of around EUR 20.5 billion. Most frequently, the target companies are consumer IoT service providers (content providers, online intermediaries, online shopping services) or manufacturers of smart home devices. Moreover, a significant number of transactions involve developers of software relevant to consumer IoT (such as machine learning or voice recognition) or providers of wireless connectivity solutions for smart home devices.

(134) Another, often complementary, expansion strategy is to establish commercial relationships with other actors in the consumer IoT sector.

(135) The main objective of such contractual arrangements appears to be the integration and interoperability of products and services with the other components of a consumer IoT ecosystem (in particular those of Google, Apple and Amazon), including the operating systems.

(136) Another goal of the contractual arrangements is to promote products and services through purely commercial partnerships. Such arrangements are aimed at expanding the usage and/or sale of consumer IoT products and services and cover various commercial practices, such as bundling, exclusivity, co-branding and revenue-sharing.

(137) For example, almost half of consumer IoT service providers have entered into partnerships with other consumer IoT service providers in order to make their service(s) available to users via an integrated offer and/or via an intermediation service. Examples of this would be a VOD channel made available via an aggregated audio-visual content platform, or an online music streaming service bundled with a mobile telecommunication service.

(138) In addition, a number of the consumer IoT service providers surveyed have revenue-sharing agreements with a variety of partners, including, typically, manufacturers of smart TVs, smart watches and smart speakers. The revenue-sharing agreements have different forms and contractual obligations, but generally include a fee paid by the consumer IoT service provider to the smart device manufacturer for each new customer acquired via the device. In most cases, a "new customer" is defined as a customer who is not an existing subscriber of the service (or who has not been a subscriber within the previous 12 months) and who subscribes to the service via a web address, to which the smart device's users are directed when they download the service provider's application.

(139) The revenue-sharing arrangement is usually: (i) either a fixed fee or a percentage of a fee (the rate ranging between 0 and 30% depending on the relative importance of the parties), per new user acquired by the consumer IoT service via the device; (ii) a percentage of the revenue, which the consumer IoT service provider generates by its service running on the manufacturer's device; or (iii) a combination of these.

(140) A specific form of revenue-sharing between consumer IoT service providers and smart device manufacturers concerning after-markets (spare parts or consumables of the primary product) is provided for in some agreements in relation to automatic product reordering. In these cases, the manufacturers of smart devices participating in the scheme may be eligible to receive revenue-sharing payments depending on the brand of products that the users order through the program.

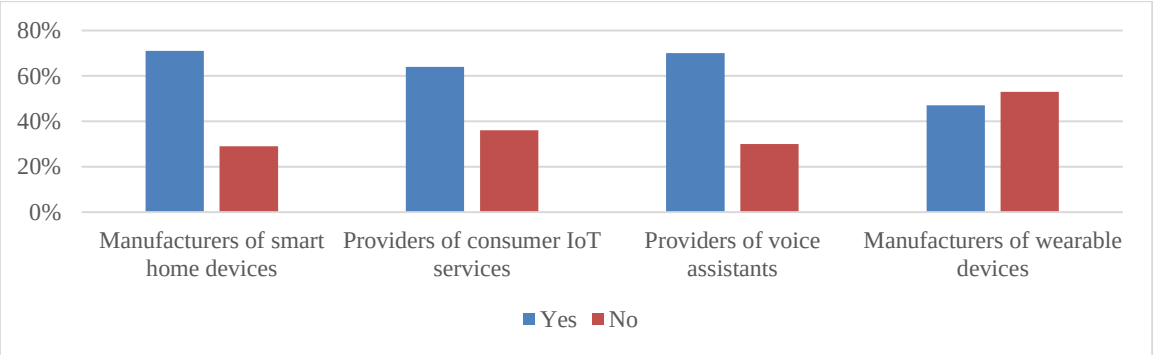
(141) The respondents also mention revenue-sharing agreements between voice assistant providers and consumer IoT service providers, through which the voice assistant provider earns a commission on the transactions processed via the voice assistant.

4.6 FORWARD-LOOKING TRENDS

(142) The respondents were asked to explain in which consumer IoT segments they are currently not active and the underlying reasons for that. The main reason for not being present in a particular segment is lack of interest or that the segment is outside the company's core business area. Other reasons mentioned by respondents include the time required for developing the relevant technology, the high investments needed for entry, or the presence of established players operating in that specific segment, which would make entry more difficult. These reasons are most notably cited for some categories, such as the provision of voice assistants or the provision of operating systems for smart devices, and are in line with the findings regarding barriers to entry and expansion in Section 4.3 above.

(143) In terms of future expansion within the consumer IoT sector, most respondents indicate that they plan to develop and launch other smart devices and/or to expand their business to any of the other consumer IoT segments in the next three years, as shown by Figure 15.

Figure 15: Plans to launch new consumer IoT products or services in the following three years (% of total respondents per questionnaire)



(144) A closer analysis shows that almost half of the manufacturers of smart home devices consider launching new consumer IoT services within the next three years. Most of these services would expand the functionalities of the manufacturers' smart home devices and improve user experience, especially by increasingly relying on artificial intelligence tools.

(145) Of those manufacturers of smart home devices that do not intend to launch their own consumer IoT services, many plan to expand the range of third-party services accessible via their devices. Several manufacturers of smart home devices specifically indicate that their strategy is to expand the range of third-party services by integrating their devices with the leading providers of consumer IoT technology platforms, namely, Amazon,

Apple and Google, which would give the manufacturers automatic access to a large number of consumer IoT services.

(146) Moreover, around half of the surveyed wearable device manufacturers plan to enable users to download and install applications or increase the range of own or third-party applications available on their wearable devices within the next three years.

(147) Similar replies were received from the vast majority of providers of consumer IoT services and voice assistants. On the one hand, around two thirds of the service providers plan to increase the range of smart devices through which users can access their consumer IoT services in the next three years. On the other hand, most voice assistant providers plan to increase the range of consumer IoT services accessible via their voice assistant in the next three years, including by developing their own consumer IoT services.

(148) In relation to voice assistants, only a few respondents plan to launch a specialised voice assistant, predominantly for their own services, in the near future. However, half of the surveyed manufacturers of smart home devices are planning to increase the range of voice assistants through which their smart home devices can be controlled in the next three years. In particular, most of these respondents plan to add Google Assistant, Alexa and/or Siri, whereas a few respondents plan to make their devices controllable via other voice assistants, such as Yandex or Xiaowei, in order to serve non-EU markets.

(149) The respondents were also asked to explain how they see the consumer IoT sector evolving and whether they expect other companies that are not yet active in any of their respective segments to launch products in those segments in the next three years.

(150) Regarding the smart home devices segment, the replies reflect an overall expectation that the segment will remain or become increasingly attractive, as many users are getting familiar with and starting to use these devices, creating a growing demand. Some respondents even expect that almost all home appliances and devices will ultimately become smart and be connected to the Internet, with this therefore becoming the norm. A respondent also mentioned the emergence of the "silver economy" as a driver for innovation, as voice-activated IoT systems and multiscreen and television-enabled monitoring consoles are expected to become quite popular for the purposes of elderly care at home.

(151) This brings an expectation that existing players will also expand into new segments. Views are mixed as to which categories of smart home devices would be affected by this expansion: while further new entry is expected in the segments of home appliances and home energy consumption, the segments of smart TVs and smart speakers appear to be maturing. A large number of respondents expect that Google, Amazon and Apple will continue to expand into different smart home device categories and use cases.

(152) Regarding wearable devices, the majority of respondents expect growing demand, expansion and continued innovation. Some point out a possible convergence of sport

watches and fitness trackers towards smart watches. Many also highlight the importance of elderly care, as well as healthcare in general, as potential drivers of growth for wrist-worn devices.

(153) Regarding consumer IoT services, the majority of respondents expect that this segment will continue to grow dynamically. The emergence of 5G will increase opportunities for businesses in this space. In particular, it is foreseen that new international and domestic players will enter the VOD market, also potentially with new monetisation models (for example purely ad-funded or hybrid), whereas existing providers will keep expanding the scope and territorial reach of their offering. Entry and expansion are expected in the audio streaming market as well, while radio is predicted to remain strong, but to shift from analogue and digital radio receivers to connected smart speakers. The respondents active in the segment highlight that health and fitness services will grow rapidly as they become hyper-targeted to individual users.

(154) Regarding voice assistants, the expectations are remarkably different: the general view is that the segment is already concentrated around Amazon and Google, while Apple is also very important. The scale of these companies, the competitive pressure they exert and the high costs associated with developing voice assistants explain why the majority of respondents do not expect new general-purpose voice assistants to be launched in the near future. Some respondents as well as Amazon in its submission to the public consultation on the preliminary report expect, however, that specialised voice assistants could enter the market, given that users may expect a voice-operated interface for some particular services.

4.7 KEY FINDINGS

A large number of respondents point out that the main obstacle to developing new products and services is the inability to compete effectively with the leading players in the consumer IoT sector, namely Google, Amazon and Apple.

These vertically integrated players have built their own ecosystems within and beyond the consumer IoT sector by combining their own, and integrating third-party, products and services into an offering with a large number of users.

Even if respondents identified quality and brand reputation as the main parameters of competition in the sector, the importance of the few market players combined with the high costs of technology investment suggest that there are significant barriers to entry in the different consumer IoT segments (smart home devices, wearable devices, voice assistants, services).

This is especially true for voice assistants, for which the respondents stress that the cost of developing and operating new general-purpose voice assistants is almost prohibitively high and there is a general belief that there will not be any new entrants in the short term.

Consequently, most respondents' business strategies focus on expanding the accessibility of their smart devices and consumer IoT services via the leading general-purpose voice assistants.

5 INTEROPERABILITY IN CONSUMER IOT ECOSYSTEMS

5.1 OVERVIEW

(155) In the consumer IoT sector, interoperability refers to the ability to interconnect and communicate between the hardware and software components of various consumer IoT products and/or services. In this respect, interoperability is essential to deploy fully the variety of possibilities offered by consumer IoT products and services, enabling and ensuring consumer choice.

(156) This chapter describes the processes consumer IoT players undertake to attain such interoperability. For this purpose, Section 5.2 explains the key role of the leading consumer IoT technology platforms (in particular voice assistants and smart device operating systems) in attaining interoperability and Section 5.3 gives an overview of how interoperability is attained in the consumer IoT sector. The following Sections 5.4, 5.5 and 5.6 describe in more detail how technical interoperability is attained in the smart home device, consumer IoT service and wearable device segments as defined in the sector inquiry. Section 5.7 concerns certification processes as a means to achieve the integration of various products and services with consumer IoT technology platforms. Finally, Section 5.8 outlines the main conclusions of this chapter.

(157) The competition concerns raised by respondents in relation to interoperability in the consumer IoT sector are set out in Chapter 8 (Section 8.2).

5.2 KEY ROLE OF CONSUMER IOT TECHNOLOGY PLATFORMS

(158) Consumer IoT products and services are generally centred on technology solutions, enabling the integration of consumer IoT services and smart devices in a connected system. In other words, consumer IoT technology platforms, such as voice assistants and operating systems, bring together different hardware and software components, enabling communication with those components and increasing their complementarity. They also allow for centralised access to and control of the products and services they integrate. In this regard, consumer IoT technology platforms, including voice assistants, have played a significant role in advancing technology integration.

(159) The leading consumer IoT technology platforms are proprietary and controlled by Amazon, Apple and Google. They are the leading general-purpose voice assistant providers, and also provide leading smart device operating systems.

(160) The majority of respondents acknowledge that access to and good performance on the leading consumer IoT technology platforms is essential to compete in the consumer IoT sector and to make consumer IoT products and services interoperable.

5.3 OVERVIEW OF TECHNICAL INTEROPERABILITY IN THE CONSUMER IOT SECTOR

(161) Respondents report that there are multiple ways to enable interactions between smart home devices, wearable devices, consumer IoT services and third-party consumer IoT technology platforms such as voice assistants. However, in most cases, third-party integration involves technical and business engagement by the parties involved. The costs of these methods, and the degree of joint work between different operators required, varies depending on a number of factors.

(162) Requirements and processes to achieve interoperability are largely determined by the presence of the leading providers of consumer IoT technology platforms. These providers govern the integrations with their products by imposing certification processes, which they control unilaterally (see Section 5.7 on certification processes). Partnership negotiations and case-by-case integration arrangements are also present, but for the most part only between the leading technology platform providers and counterparties with sufficient bargaining power to negotiate, or in situations where the leading technology platforms are not involved (for example integration projects between smaller smart device manufacturers).

(163) Business strategies and approaches that some companies take on issues such as privacy and security also influence integration processes. For example, some respondents do not share technical documentation with third parties and others do not make their devices controllable by third-party user interfaces in order to avoid data sharing with third parties or to wall their systems against external interference.

(164) Although there is no common approach to integration, interoperability, from a technical perspective, is generally based on application programming interfaces (APIs), developed or made available by one of the parties, which allow exchanges of data and functionalities through software interfaces. Parties frequently make software development kits (SDKs) and hardware technical specifications available, to facilitate implementation.

(165) Once the relevant API documentation or SDK is released, smart device manufacturers and consumer IoT service providers can build integration by developing software solutions or applications written for the specific consumer IoT technology platform (for example for a particular voice assistant or smart device operating system). When the integration involves the certification of a smart device, hardware specifications need to be followed. Once the integration is tested and validated internally, it normally needs approval by the provider of the consumer IoT technology platform, following a certification process to verify its correct performance.

(166) Nevertheless, there are exceptions to these integration steps. For instance, some companies have a policy of not sharing their APIs, and integrate third-party APIs or SDKs into their own systems instead. In this way, they customise third-party

applications to their systems and control the integration process of third-party products and services within their systems.

(167) APIs, SDKs and hardware specifications are generally made available to third parties subject to the conclusion of agreements. In this regard, providers of relevant user interfaces, such as voice assistants, have standardised their requirements for integration into terms and conditions, which are generally not open to negotiation with counterparties. Nevertheless, when horizontal collaboration is required or the business partners are on an equal footing, companies negotiate contractual and technical integration on an ad hoc basis and sign customised agreements.

(168) In the following sections, the specific interoperability requirements and integration processes for each of the following consumer IoT segments are set out: smart home devices, consumer IoT services and wearable devices. Such information relating to voice assistants is considered across all of these sections, given their widespread presence in accessing and controlling products and services in the consumer IoT sector.

5.4 SMART HOME DEVICES

(169) According to respondents' replies, the smart home segment is characterised by complex technology and the presence of a significant and growing number of smart home device manufacturers. These players use different communication standards, data models and system architectures. In addition, most smart home systems are built around the leading providers of consumer IoT technology platforms and, in particular, around a few general-purpose voice assistants, namely, Google Assistant, Alexa and Siri, which allow for centralised control of smart devices from different brands and access to a variety of consumer IoT services.

5.4.1 Connectivity

(170) As set out in further detail in Section 6.4, there is a wide variety of communication standards and protocols in the market that facilitate communication with smart devices, but that do not necessarily communicate with each other. In fact, the two most prominent communication protocols according to respondents, the Connectivity Standards Alliance[31] and Z-Wave, do not allow for interoperability between smart devices using one or the other.

(171) Manufacturers must decide how many, and which, communication protocols will run on their devices and implement a certain number of feature requirements (i.e. memory size, low power optimisation and security) to support them.

[31] Previously Zigbee Alliance.

(172) To allow communication between smart home devices that do not support the same communication protocols and/or between smart home devices and the cloud, a hub or a gateway[32] might be necessary to facilitate interconnection and data exchanges.

(173) Moreover, some devices and sensors (for example smart bulbs) use non-IP based networks like Bluetooth, the Connectivity Standards Alliance or Z-Wave, for reasons such as limited battery capacity or to save on costs. In some cases, developers need to support their devices and sensors with dedicated hubs or gateways that translate non-IP based protocols into a format that can be communicated through the internet.

5.4.2 Management and control of smart home devices through first-party vs. third-party user interfaces

(174) As explained in Section 2.3, most smart home devices can be controlled through a first-party user interface without the support of or integration with a third-party technology platform. Nevertheless, the user interface of a sole smart home manufacturer might not be interoperable with third-party devices. For this reason, standalone user interfaces create a fragmented experience for users, who need to navigate through different set-ups and use distinct smart home applications to control each of their smart home devices.

(175) In addition, in certain use cases, interaction and data exchanges with third-party smart devices and services are essential for delivering the smart device functionality. For example, smart speakers depend on interaction with third-party music streaming services; smart TVs on streaming of movies and TV series; smart shutters on integration with a weather app; and smart thermostats on connection with heating systems. Thus, entering the market with a standalone user interface, which only allows control of one device or of devices from one brand, creates inconvenience for the user, makes smart home devices less functional and interoperable and creates competitive disadvantages.

(176) To overcome the shortcomings of only having first-party user interfaces, the majority of respondents make their smart devices operable through third-party technology platforms that incorporate user interfaces and, in particular, through leading general-purpose voice assistants. In fact, once integration with third-party user interfaces has been achieved, the brand's user interface (for example smart home application) usually becomes redundant and thus is employed less frequently by the user.

(177) The integration of smart home devices with voice assistants is typically achieved through various certification programs, which are governed by the voice assistant providers and explained in more detail in Section 5.7 below.

[32] A hub or gateway consists of a piece of hardware or software that connects devices on a home automation network and controls communications between them. There are standalone dedicated hub or gateway devices, but they can also be integrated into smart home devices such as smart speakers.

5.4.3 Smart home device operating systems

(178) Complex and high-end smart home devices such as smart TVs or smart fridges run on operating systems, which allow these devices to not only collect and transmit data but also analyse it and support automatic decision-making. On the contrary, smaller or low-level smart devices such as smart bulbs or smart sensors typically do not run on operating systems but on firmware, a specific class of computer software that provides the low-level control for a device´s hardware of such characteristics.

(179) For those smart devices running on operating systems, smart home device manufacturers choose the operating system that best fulfils their specifications. Many respondents use open source operating systems such as Linux to develop their own operating system adapted to the device's requirements. Others resort to third-party proprietary operating systems.

(180) To license smart device operating systems provided by third parties (for example Amazon Fire TV, Android TV), manufacturers of smart home devices must enter into license agreements (for example, for Amazon's Fire OS and Fire TV, Amazon's Fire TV Edition Program Agreement). The operating system licensor might require that the manufacturer complies with certain requirements set by the licensor.

(181) Smart device operating systems also function as technology platforms for accessing third-party consumer IoT services and voice assistants through applications developed and installed on such operating systems. For this purpose, consumer IoT service and voice assistant providers develop applications to make their services accessible through smart home device operating systems, which function as technology platforms in this sense. This enriches the user experience, since third-party consumer IoT services and voice assistants can be accessed together with the first-party features or functions.

5.5 CONSUMER IOT SERVICES

(182) While leading providers of consumer IoT technology platforms (i.e. Google, Amazon and Apple) are able to offer their first-party services via their own smart devices, operating systems and voice assistants (for example, Amazon's Echo Speakers offer Amazon Music via a first-party Alexa skill), most consumer IoT service providers need to develop integration with third-party consumer IoT technology platforms in order to reach users. For instance, music streaming service providers need to develop voice applications to make their services accessible via voice assistants. Similarly, VOD providers would need to develop applications for smart TV operating systems to be accessible on those consumer IoT technology platforms. Likewise, providers of fitness services would have to develop applications for a certain wearable operating systems to be accessible through a smart watch.

5.5.1 Voice applications

(183) Prior to being made available on a voice assistant, third-party voice applications must initially accept the voice assistant's terms and conditions, and get the approval of the voice assistant provider through its proprietary review process. Once voice applications are approved, third-party consumer IoT services can be found and accessed by users via the voice assistant (see Section 5.7 below for information on voice applications' certification by consumer IoT technology platform providers).

5.5.2 Integration with third-party smart device operating systems

(184) Similarly, many consumer IoT service providers develop specific applications for smart home devices' and wearable devices' operating systems (for example Android TV for smart TVs or Wear OS for wearable devices). This is particularly the case for creative content service providers, which must integrate with third-party manufacturers' operating systems to make their content accessible through smart home devices. For example: VOD providers develop applications that run on the operating systems of smart TVs, streaming devices and gaming consoles; and music streaming service providers develop applications for wearable device operating systems or smart speaker operating systems.

(185) The development of applications for operating systems also follows review and certification processes governed by the smart device operating system providers. Again, operating system licensors and manufacturers of smart home and wearable devices generally make their operating system's APIs and technical specifications publicly available so that consumer IoT service providers can use them to develop the corresponding integration, subject to certain conditions and/or the signing of agreements. Once the application is developed, tested and validated by the consumer IoT service provider it must undergo a proprietary review or certification process governed by the manufacturer or operating system provider to ensure that the integration works correctly.

5.5.3 Exception for prominent consumer IoT service providers

(186) In general, the consumer IoT service providers are in charge of developing integrations for consumer IoT technology platforms, but there are a few exceptions for key service providers, the presence of which might be important for the providers of consumer IoT technology platforms. In such cases, the consumer IoT service provider might, for example, provide APIs or SDKs to the smart device manufacturer for it to integrate the service into its devices, or work together with the smart device manufacturer to build such integration. The manufacturer would then develop the software solution on its operating system, which the consumer IoT service provider would then review to certify that the product meets all of the requirements.

(187) From a contractual perspective, the integration of consumer IoT services with voice assistants and smart device operating systems involves, in most cases, the acceptance by

the consumer IoT service providers of standard terms and conditions stipulated by the voice assistant and operating system providers. Nevertheless, partners can come to ad hoc agreements or negotiate those standardised contracts when more collaboration is involved for building the integration.

5.6 WEARABLE DEVICES

5.6.1 Companion apps and mobile device operating systems

(188) As explained in Section 2.4, wearable devices generally need the support of companion apps running on a smart mobile device operating system to unlock certain functions. Moreover, many wearable devices connect through Bluetooth to the user's smartphone in order to provide internet connectivity, which the wearable device itself would not support in isolation. Such companion apps are available to download on mobile app stores, including Google Play and the Apple App Store.

(189) Companion apps need to be submitted for app review to the app store provider (i.e. Apple and Google) to seek approval. In order to obtain a license for the distribution of the companion apps through the Google Play Store and the Apple App Store, the wearable device manufacturer must comply with Apple and Google's standard non-negotiable terms and conditions and their app review program. The app store operators reserve the right to reject applications that do not meet their standards.

(190) According to wearable device manufacturers' responses, smooth interoperability between the wearable devices and smartphones' operating systems supporting companion apps is essential to provide full functionality and a good user experience.

5.6.2 Wearable device operating systems

(191) Next to mobile device operating systems, wearable device operating systems are also of importance for wearable devices. Only a limited number of wearable device manufacturers have developed or continue to use their own wearable device operating system. The majority of them use operating systems licensed from the leading providers, because the cost of developing and maintaining such an operating system is high. As one stakeholder emphasised in its submission to the public consultation on the preliminary report, the limited number of available wearable device operating systems is likely to limit the parameters of competition between wearable devices manufacturers.

(192) For instance, Google licenses its "Wear OS" operating system, which is the most successful wearable device operating system among manufacturers; on the contrary, Apple does not license its operating system for wearable devices.

5.6.3 Voice assistants and consumer IoT services' availability on wearable devices

(193) Wearable devices generally come with first-party features, applications and voice assistants pre-installed on their operating system, which are accessible either directly on the device or through its companion app.

(194) In addition, third-party developers can also make their services available for wearable devices by developing applications compatible with wearable operating systems. Nevertheless, some respondents report that their wearable devices do not support third-party applications.

(195) In order to access those third-party consumer IoT services, users must download the applications they wish to use. Wearable device manufacturers report different technical ways of making applications downloadable by users onto their wearable device or alternatively, onto the user's smartphone to be used in connection with the wearable device. In particular, some wearable device operating systems integrate a built-in wearable app store. Wearable device manufacturers might also make available their own app stores for wearable device operating systems. In some cases, it is also possible to access third-party applications through the wearable device's companion app or by downloading third-party applications on a connected mobile device.

5.7 CERTIFICATION PROCESSES

(196) As the preceding sections illustrate, leading providers of consumer IoT technology platforms control and determine access to their platforms; mainly voice assistants and smart device operating systems. Through certification processes, such providers impose specific contractual and technical requirements on smart device manufacturers and consumer IoT service providers that wish to make their products accessible through the consumer IoT technology platforms of these leading providers[33].

(197) In the case of voice assistants, the leading providers, namely Google, Amazon and Apple, govern certification processes and impose different review processes depending on the type of integration that the smart device manufacturer or consumer IoT service provider wishes to achieve. In short, there are three categories of certification processes for integration with voice assistants:

a. *"Works with" programs or connected device certifications* allow smart device manufacturers to make their smart home devices controllable through a voice assistant embodied on another device (i.e. smart speaker) or support (i.e. smartphone application). For smart home device manufacturers, these programs generally involve reviewing the voice assistant provider's documentation on API functionality for smart home device interoperability and developing a voice application following the voice assistant provider's requirements. The voice assistant provider then tests the developed integration to ensure a good user experience. If certification is granted, manufacturers can use "works with" logos or badges in their packaging or for online marketing. Examples of these

[33] Several comments received during the public consultation on the preliminary report confirm that few players determine interoperability and third-party access to relevant consumer IoT ecosystems through certification processes, which can become a burden especially for smaller players.

certification processes are the "Works with Alexa", "Works with Google Assistant" and "Works with Apple Home kit" programs.

b. *Built-in certification processes* allow third-party smart device manufacturers to support Amazon or Google's cloud-based voice assistants on their devices and gain the "Alexa built-in" or "Google Assistant built-in" badges. Apple, on the contrary, does not offer built-in certifications, as Siri can only be built-in on Apple's own devices. Through built-in integration, users can access all the features supported by the third-party voice assistant from the manufacturer's smart home device, including smart device control and access to third-party services through voice applications. In this regard, built-in solutions are different from works-with programs, which are limited to smart device control functionalities. Built-in certification processes involve a thorough testing of the smart devices in which the voice assistant will be embodied by the voice assistant provider. On a technical level, manufacturers need to integrate a built-in microphone and comply with the required hardware requirements specified by the voice assistant providers.

c. *Development of voice applications*, such as "Alexa skills", "Google actions", "Siri' shortcuts" or "Capsules" for Bixby, which run on the voice assistant for which they have been developed. Voice applications make consumer IoT services accessible to the user via voice assistants. From a technical perspective, voice assistant providers make available SDKs to build custom voice applications. Developers must follow the voice assistant guidelines on how to write an application and also comply with the natural language understanding (NLU)[34] rules of the voice assistant. The voice application is then submitted for certification before it is published and made available through the voice assistant.

(198) Providers of operating systems for smart devices also impose review processes to consumer IoT service providers and smart device manufacturers that develop applications or software solutions running on their technology platforms.

5.8 KEY FINDINGS

Interoperability in the consumer IoT sector is essential for the full deployment of a variety of use cases and functions that the various types and brands of consumer IoT products and services provide.

Interoperability requires technical and business engagement among consumer IoT players in order to provide meaningful integration and smooth functioning of smart devices, consumer IoT services, voice assistants and smart device operating systems. The technical integration processes are generally based on application programming interfaces (APIs), which are either

[34] Natural language understanding refers to natural language processing involving the transformation of human language into a machine-readable format.

developed or made available by one of the parties, and which allow exchange of data and functionalities through software interfaces.

In practice, consumer IoT products and services are generally centred on a few proprietary consumer IoT technology platforms, namely Amazon's, Apple's and Google's voice assistants and/or smart device operating systems. The majority of respondents consider that leading technology platforms are key entry points to first and third-party services and products in the consumer IoT sector. To achieve interoperability with those technology platforms, smart device manufacturers and consumer IoT service providers need to follow certification processes to gain approval for their customised integrations and abide to the, mostly non-negotiable, terms and conditions of these platforms.

6 STANDARDS AND THE STANDARD-SETTING PROCESS

6.1 OVERVIEW

(199) Section 6.2 provides an overview of the Standards Developing Organisations (SDOs), as well as the private partnerships and independent alliances, reported by the respondents as most prevalent in the consumer IoT segments covered by this sector inquiry. Section 6.3 provides a comparison of the different intellectual property rights (IPR) policies of the relevant SDOs and alliances, and Section 6.4 a short description of the role of open standards vs. proprietary technologies in consumer IoT. Section 6.5 provides an overview of the way respondents see the evolution of standardisation[35] in consumer IoT in the near future.

6.2 SDOS AND INDEPENDENT ALLIANCES

(200) The consumer IoT sector covers a significant number of different services, devices and technologies that need to connect and communicate seamlessly in real time. An important number of SDOs and private partnerships/independent alliances have developed and are currently active in the joint development of technologies that consumer IoT products and services may rely on to ensure such seamless but effective connection.

(201) In view of the potential of the consumer IoT sector and the importance of the easy integration of, communication between, and navigation among devices and services, various SDOs, working groups within those SDOs, and independent alliances have recently been initiated with the precise purpose of enabling and facilitating interoperability in this sector. Standards in the consumer IoT sector include not only those needed to integrate and connect devices and applications, but also standards that ensure the quality and security of the IoT communications.

(202) This section gives an overview of recognised European or International standardisation bodies (6.2.1.) and relevant other SDOs, independent alliances and partnerships (6.2.2.). The references to non-formal SDOs, independent alliances, organisations and private partnerships developing, deploying and maintaining standards relevant to consumer IoT are not exhaustive. These are based on the responses to the questionnaires and the submissions to the public consultation, and identify the broadest partnerships and alliances that were most often referred to by respondents. The list of SDOs contained in this report is not exhaustive and may evolve over time as other SDOs may become active in the field in the future.

[35] For the purposes of this report, references to standardisation are not limited to European standardisation as set by Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation. OJ L 316, 14.11.2012, pp. 12–33.

(203) Also of relevance, in 2015 the Commission initiated the Alliance for Internet of Things Innovation (AIOTI). While AIOTI is not an SDO as it does not adopt standards, its purpose is to strengthen the dialogue and interaction among IoT players in Europe, to contribute to the creation of a dynamic European IoT ecosystem and accelerate the uptake of IoT. AIOTI members include key European IoT players – large companies, successful SMEs and dynamic start-ups – as well as research centres, universities, and associations.

6.2.1 Most relevant formal SDOs[36] for consumer IoT

(204) The European Committee for Standardization (CEN) and European Committee for Electrotechnical Standardization (CENELEC)[37], the European Telecommunications Standards Institute (ETSI)[38], and the International Telecommunication Union (ITU), the International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC)[39] all have work streams for the development of standards relevant to particular areas of consumer IoT.

(205) CEN and CENELEC actively cooperate with ISO and IEC to reach agreements on common standards that are applicable worldwide, thereby facilitating the development of consumer IoT technologies. Various CEN and CENELEC Technical Committees have been developing standards that relate to the communication and interoperability between smart home devices, voice assistants and wearable devices, as well as consumer IoT services[40].

[36] As recognised by Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation. OJ L 316, 14.11.2012, pp. 12–33.

[37] CEN and CENELEC are two distinct private non-profit international organisations. CEN and CENELEC are also officially recognised European Standardisation Organisations by the European Union and by the European Free Trade Association (EFTA) as being responsible for developing and defining voluntary standards at the European level. The CEN and CENELEC Members are the National Standard Bodies and the National Electrotechnical Committees in the EU, EFTA and official candidate countries to the EU.

[38] ETSI is a leading standardisation organisation for Information and Communication Technology (ICT) standards. It is an officially recognised European Standardisation Organisation. ETSI has more than 900 member organisations worldwide, drawn from 65 countries and five continents. Members comprise a diverse pool of large and small private companies, research entities, academia, and government and public organisations.

[39] The ITU is a specialised agency of the United Nations responsible for all matters related to information and communication technologies. ISO is an independent, non-governmental international organisation with a membership of 165 national standards bodies. IEC is an international organisation with members from 170 countries, and which coordinates the work of more than 20 000 experts.

[40] See for instance the standards developed by CEN/TC 294 'Communication systems for meters', or standards developed by CLC/SR 124 'Wearable Electronic Devices and Technologies' for standardisation in the field of wearable electronic devices and technologies which include patchable materials and devices, implantable materials and devices, ingestible materials and devices, and electronic textile materials and devices. CLC/TC 79 'Alarm Systems' prepares European Standards for detection, alarm and monitoring systems for protection of persons and property and for elements used in these systems.

(206) ETSI works across all sectors of industry and society that make use of or rely on Information and Communications Technology (ICT). It also addresses the development of standards relevant to voice assistants, wearable devices and smart home devices[41].

(207) ITU has established a Joint Coordination Activity on IoT and Smart Cities and Communities (JCA-IoT and SC&C) to coordinate the ITU Telecommunication Standardisation Sector's (ITU-T) work on the "Internet of Things and Smart Cities and Communities" and provide a visible contact point for IoT and its applications, including smart cities and communities (SC&C) activities within the ITU-T. ITU is also collaborating on developing OneM2M technical specifications (see Section 6.2.2 below). In areas of information technology falling within ITU-T's purview, the necessary standards are prepared collaboratively with the ISO and the IEC.

(208) ISO and IEC have a dedicated joint technical committee (ISO/IEC JTC 1) that deals with Information technologies. ISO/IEC JTC 1 is composed of sub-committees addressing the development of standards for voice assistants, smart home devices and wearable devices[42].

6.2.2 Most relevant other SDOs, independent alliances and private partnerships[43]

(209) The respondents to the different questionnaires identify various long-established SDOs, alliances and partnerships as running programs and activities highly relevant to the consumer IoT sector. In particular, the Institute of Electrical and Electronics Engineers (IEEE)[44], the Internet Engineering Task Force (IETF)[45], OASIS[46], the Open

[41] See for instance TS 122 243 Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Speech recognition framework for automated voice services; Stage 1 (3GPP TS 22.243 version 16.0.0 Release 16). This Technical Specification contains core requirements for the Speech Recognition Framework for automated voice services. See also TS 103 504 Speech and multimedia Transmission Quality (STQ); Methods and procedures for evaluating performance of voice-controlled devices and functions: far talk voice assistant devices.

[42] JTC 1 SC 6: Telecommunications and information exchange between systems
JTC 1 SC 17: Cards and security devices for personal identification (some activities are mirrored at European level by CEN/TC 224)
JTC 1 SC 25: Interconnection of information technology equipment
JTC 1 SC 41: Internet of Things and related technologies. JTC 1 SC 41 develops International Standards on IoT and related technologies. It serves as the proponent for JTC 1's standardisation programme on the Internet of Things and related technologies, including Sensor Networks and Wearables technologies. ISO/IEC JTC /SC 41 also provides guidance to JTC 1, IEC, ISO and other entities developing Internet of Things related applications.
JTC 1/SC 41 published foundational standards on IoT, such as ISO/IEC 30141:2018 Internet of Things (IoT) - Reference architecture and ISO/IEC 20924:2018 Internet of Things (IoT) – Vocabulary.

[43] Relevant alliances, organisations and partnerships, independent of their size and importance, that are not officially recognised as standardisation organisations under Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, are listed under this point.

[44] IEEE is the world's largest technical professional organisation composed of engineers, scientists, and allied professionals. It has over 400 000 members in over 160 countries. It runs several programs and activities in the IoT sector. These include the IEEE IoT Initiative and Community where stakeholders can learn, share knowledge, and collaborate on the growing convergence of technologies, markets, and applications. Main areas of activities and achievements in the setting of technical standards include: (i) Architectural frameworks: IoT architectural frameworks assist with connectivity, interoperability, and integration of IoT systems; (ii) Harmonisation and security: for data sharing and the authorisation by the owner of devices to access the devices' data including control of these devices; and (iii) Sensor performance and quality.

Connectivity Foundation (OCF)[47], and the GSM Association (GSMA)[48] have been singled out for their relevant achievements.

(210) Similarly, more specialised alliances, such as the ioXt Alliance[49] (developing cybersecurity standards for the safety and security of IoT products, with a corresponding cybersecurity certification program), the Hybrid Broadcast Broadband TV (HbbTV) Association[50], the Z-Wave Alliance[51], the Mioty Alliance[52] and the

---

[45] IETF is an Internet standards body that began as an activity of the US Government over 50 years ago and since 1993, has acted as a standards setting organisation funded through the Internet Society. It published protocol specifications as Request For Comments (RFCs), some of which it categorises as standards, while others are informational/experimental or draft/proposed standards. At the time of the submission of the IETF's response, over 8 900 RFCs have been published, including RFCs relevant to consumer IoT. See for instance RFC 8428 "Sensor Measurement Lists (SenML)". This specification defines a format for representing simple sensor measurements and device parameters in Sensor Measurement Lists (SenML). RFC 8790 "FETCH and PATCH with Sensor Measurement Lists (SenML)" The Sensor Measurement Lists (SenML) media type and data model can be used to send collections of resources, such as batches of sensor data or configuration parameters. The Constrained Application Protocol (CoAP) FETCH, PATCH, and iPATCH methods enable accessing and updating parts of a resource or multiple resources with one request. See also RFC 8798 "Additional Units for Sensor Measurement Lists (SenML)".

[46] OASIS is a long-established open standards development consortia in the transactional internet space. Its development activities have hosted approximately 5 000 active participants, representing about 500 member organisations and individual members in over 80 countries. It runs many projects covering a wide range of methodologies, including projects relevant to IoT. Major OASIS standards relevant to consumer IoT include the messaging and telemetry specifications Message Queuing Telemetry Transport (MQTT, also approved as ISO/IEC 20922), the Advanced Message Queuing Protocol (AMQP, also approved as ISO/IEC 19464); the Classification of Everyday Living (COEL) specification for human behaviour and object interaction classification, and the suite of smart grid/smart device transaction standards developed in cooperation with the US National Institute of Standards and Technology (NIST) and Department of Energy smart grid programs. OASIS open standards, specifications and code, usually developed by globally diverse expert groups, are often contributed to and re-issued, or jointly issued with ISO, ITU-T, ISO/IEC JTC1 and similar bodies. OASIS has been a member of the EU Commission's Multistakeholder Panel on ICT Standards (among others) since its inception, and holds Accredited Standards Developer status from the American National Standards Institute (US-ANSI). It also enjoys active expert participation from public administrations around the world.

[47] OCF is an industry organisation with a focus on developing specification standards, promoting a set of interoperability guidelines, and providing a certification program for devices involved in IoT. It has become one of the biggest industrial connectivity SDOs for IoT. It currently has more than 300 member companies, including Samsung, Intel, Qualcomm, Microsoft, Cisco, Huawei, Panasonic, LG, Resideo and Electrolux. OCF's Specifications provide connection mechanisms between devices, as well as between devices and the cloud, and manage the flow of information among devices, regardless of their form factors, operating systems, service providers or transports. OCF submitted various IoT specifications to JTC 1 for publication as ISO and IEC standards. The OCF Smart Home Project, with its user base of over 300 companies, creates common data modelling for secure interoperability between smart home devices of different brands. See for instance the OCF 2.0.2 release, including OCF Device Specification (2.0.2), OCF Wi-Fi Easy Setup Specification (Core Specification Extension) (2.0.2), OCF Cloud Specification (Core Specification Extension) (2.0.2).

[48] The GSMA represents the interests of mobile operators worldwide, as well as of companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. It aims at achieving scale and interoperability for new mobile technologies. It units more than 750 operators with almost 400 companies in the broader mobile ecosystem.

[49] Individual companies such as Amazon, Google, T-Mobile, Motorola, Logitech, Legrand, NXP, Schneider Electric, as well as other industry alliances such as Z-Wave and Connectivity Standards Alliance (previously Zigbee) are also members.

[50] HbbTV aims at harmonising the broadcast and broadband delivery of entertainment services to consumers through connected TVs, set-top boxes and multiscreen devices. Products and services using the HbbTV standard can operate over different broadcasting technologies, such as satellite, cable, or terrestrial networks, and can show digital television content from a number of different sources, including traditional broadcast TV, internet,

EnOcean Alliance[53] are consistently identified throughout the questionnaires for their programs and achievements in different fields relevant to the consumer IoT sector.

(211) Some of the organisations most recently developing standardised technologies and protocols relevant to this sector inquiry are briefly referred to below:

(212) OneM2M[54] is an international partnership formed of regional formal SDOs whose goal is to create a global technical standard for interoperability concerning the architecture, API specifications, security and enrolment solutions for Machine-to-Machine (M2M) and IoT technologies based on requirements contributed by its members.[55] There are currently nearly 230 members (some of which are supporting companies from partner SDOs), including Amazon, Samsung, Broadcom, IBM, Intel, LG, Nokia, Qualcomm, Panasonic, Orange, Deutsche Telekom, Vodafone, and T-Mobile. OneM2M technical specifications are transposed by the member SDOs in formal standardisation deliverables.

(213) The LoRa Alliance® [56] is responsible for creating, developing and sustaining the LoRaWAN general connectivity standard that covers transmission of very low data rate messages to enable IoT applications. The goal of the LoRa Alliance is to standardise

---

and connected devices in the home. The HbbTV specification is developed by industry players to improve the video user experience for consumers. It is based on elements of existing standards and web technologies, such as OIPF (Open IPTV Forum), CEA-2014 (CE-HTML), W3C (HTML etc.) and DVB Application Signalling Specification (ETSI TS 102 809) and DASH. Amazon, Google, Samsung, LG, Panasonic, BBC, RTL, Rai, Sky, TCL and Dolby are, amongst many others, members of the Association.

[51] The Z-Wave Alliance consists of over 700 members, including Silicon Labs, ADT Corporation, Viva Labs, Homey, Vodafone, Jasco, Leedarson, LG Uplus, Ring, SmartThings, and Vivint. Established in 2005, it is designed to achieve reliable communication and operation between devices manufactured by its members. Z-Wave is a wireless communications protocol used primarily for home automation, allowing for wireless control of residential appliances and other devices, regardless of their brand or vendor, such as lighting control, security systems, thermostats, windows, locks, swimming pools and garage door openers. To guarantee interoperability, each Z-Wave product must pass a stringent conformance test to assure that it meets the Z-Wave standard for complete compliance with all other devices and controls.

[52] The Mioty Alliance was founded in November 2019 to promote wireless LPWAN technology standardised under ETSI TS 103 357. It provides connectivity for low power, low data rate end points (e.g. sensors or any data acquisition device relying on low data rate). Mioty aims at building end-to-end solutions across the entire IoT value chain. The Mioty technology is widely adopted in particular for massive IoT deployments.

[53] The EnOcean Alliance is an international association of leading companies in the building and IT industries founded in 2008 and headquartered in Germany. It is an open, non-profit organisation, committed to enabling and promoting interoperable eco-systems for smart homes, smart buildings and smart spaces. EnOcean is the inventor of the patented resource-saving wireless technology for use in building automation and consumer IoT. EnOcean produces maintenance-free, self-powered solutions such as wireless switches and sensors, which gain their energy from the surroundings – from movement, light or temperature, for example. The Alliance is partnering with more than 350 leading product manufacturers worldwide to build energy harvesting solutions.

[54] OneM2M is an international partnership between eight of the world's leading SDOs seeking to develop IoT relevant standards, namely ARIB (Japan), ATIS (United States), CCSA (China), ETSI (Europe), TIA (USA), TSDSI (India), TTA (Korea) and TTC (Japan).

[55] OneM2M develops technical specifications for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect devices with M2M application servers worldwide. See for instance the Release 2A deliverables, such as TS 001 to TS 0032.

[56] LoRa Alliance is an open, non-profit association launched in March 2015 that has grown to have more than 500 members. The LoRa Alliance is composed of individual member companies from around the world who collaborate to develop and sustain the Long Range Wide Area Network (LoRaWAN) protocol.

LPWAN specifications for LoRaWAN connectivity and to enable large-scale volume of IoT deployments through standardisation.

(214) The LoRa Alliance is similar to the WiFi Alliance and the Bluetooth SIG, in that all three organisations: (i) develop the requirements and protocols of the relevant technology (LoRaWAN, WiFi and Bluetooth/BLE); (ii) establish test and certification programs to ensure products utilising these technologies adhere to the performance and security rules of the protocols; and (iii) promote adoption of each technology through advocacy, leadership and industry collaboration. LoRaWAN, as well as WiFi and Bluetooth, are all connectivity standards, providing the rules on how to transmit data wirelessly using these technologies.

(215) The Connectivity Standards Alliance aims at developing open, global standards for wireless device-to-device communication for IoT, certifying products to help ensure interoperability through the certification program of the alliance, and to promote the use of its standards around the world. Leading members ("Promoters") of the Connectivity Standards Alliance include, among others, Amazon, Apple, Google, Samsung, Huawei, IKEA, Resideo, Signify (formerly Philips Lighting), Somfy, Legrand, and NXP Semiconductors. As a result of its membership, it has a high adoption rate in many of the most popular ecosystems in consumer IoT markets.

(216) In December 2019, Amazon, Apple, Google and the (then) Zigbee Alliance joined together to promote a new working group under the (now) Connectivity Standards Alliance, the Connected Home over IP (internet protocol) or CHIP Project, today operating under the name "Matter". The plan was to develop and promote the adoption of a new, royalty-free connectivity standard to increase compatibility among smart home products, thereby simplifying development for manufacturers, and increase compatibility for consumers. Based on the standardisation framework, Matter defines a multi-layer framework supporting existing standards on several layers. In particular, the project aims to make it easier for device manufacturers to build devices that are compatible with smart home services and voice assistants such as Alexa, Siri, and Google Assistant. Today, Matter has over 145 active member companies.

(217) The working group takes an open-source approach for the development and implementation of the new, unified connectivity protocol: the reference implementation and its supporting tooling will be developed and maintained on the GitHub open source platform. The Project plans to define a specific set of IP-based networking technologies for device certification. Compliant devices would need to implement at least one supported technology but not necessarily all.

(218) Thread is an Internet Protocol[57]-based network protocol for IoT products. In July 2014, the Thread Group alliance was formed as a working group to aid Thread in becoming an industry standard by providing Thread certification for products. Thread members

[57] Internet Protocol version 6 (IPv6).

include Google-subsidiary Nest Labs, Samsung, Silicon Labs, Somfy and Qualcomm. Apple joined the group in 2018 and released its first Thread based products in 2020[58].

(219) The Voice Interoperability Initiative (VII) is an Amazon-led initiative launched in September 2019. Today it has approximately 80 members. The VII aims at providing customers with the ability to choose their preferred voice assistant for any task, by using multiple voice assistants concurrently on a single device. Customers could activate any of those voice assistants by saying the relevant activation word for that assistant. This customer experience principle is called "multi-simultaneous wake word" (or MSWW). The VII's members commit to enabling MSWW customer experiences.

(220) The VII has four areas of focus: (i) Customer choice – building voice-enabled devices that promote customer choice and flexibility through MSWW; (ii) Secure interoperability – developing voice assistants that can work alongside others while protecting the privacy and security of customers; (iii) Technology solutions – developing and releasing technologies and solutions that make it easier to integrate multiple voice assistants on a single product; and (iv) Research and development – accelerating machine learning and conversational AI research to improve the breadth, quality and interoperability of voice assistants[59].

(221) The Open Voice Network (OVN)[60] is a non-profit industry association, started in 2019, which operates as a directed fund[61] of the Linux Foundation. It works on the proposal, development, and implementation of standards in the field of voice assistant-related technologies and 'conversational AI'. The OVN aims to bring user trust to the forefront of artificial intelligence-enabled voice assistance and to create a future of voice that is open, standards-based, interoperable, accessible, and data-protected.

6.3 THE RELEVANT IPR POLICIES

(222) The above SDOs and private partnerships/independent alliances apply different IPR policies for the licensing of the specifications they develop. Many SDOs' and alliances' IPR policies stick to high-level definitions, typically limited to a general FRAND[62]

[58] Thread's IP foundation is application layer agnostic, offering product manufacturers the flexibility to choose one (or multiple) app layers for their use case to connect devices across multiple networks. For instance, a single application layer (such as the smart home standard being developed by Project Matter) could run on devices connected via both Thread and Wi-Fi. This would create a seamless network of interoperable products, while allowing device manufacturers to choose the right networking technology for their application. Developers can select from a number of Thread certified components to build their products or choose from an array of certified Thread products to build an ecosystem.

[59] In September 2020, Amazon published the first version of a Multi-Agent Design Guide. The Multi-Agent Design Guide is intended to help establish a common framework and lexicon for discussions about MSWW experiences, and to present design principles and best practices for multiple voice services to work concurrently on the same device.

[60] OVN brings together communities of voice developers, designers, strategists, practitioners and influencers, ethical experts and those working for the Health & Life Sciences industry.

[61] I.e. subject to the discretionary management and control of the Linux Foundation.

[62] Fair, reasonable, and non-discriminatory licensing. Licensing is also commonly granted on RAND (reasonable and non-discriminatory) terms.

licensing commitment, without significant additional detail. The formal SDOs (CEN, CENELEC, ETSI, ISO/IEC/ITU) essentially belong to this category. A number of SDOs have developed their IPR policies further. Some of them commit themselves to the outcome (for instance warranting a royalty-free outcome), while others introduce different rules without committing to a specific outcome, for instance by offering an optional choice (typically (F)RAND commitment or royalty free or non-assertion covenant).

(223) The table below provides a largely simplified comparison of the licensing and other access rules under those IPR policies, as reported and/or publicly available. The full texts of the relevant IPR policies are available on the websites of the relevant SDOs and alliances.

Table 3: Comparison of formal SDOs licensing policies

NAME	**FRAND/RAND**[63] **other reasonable non-discriminatory licensing**	**ROYALTY-FREE licensing only**	**ROYALTY-FREE licensing with possibility to opt out**	**Open option between FRAND/RAND and royalty-free licensing**	**OTHER terms for access to standard**
CEN/CENELEC	X	X N.B. For full implementation or reproduction by a member National Standard Body			Member organisations are bound to implement the adopted European Standards as national standards, and withdraw conflicting national standards.
ETSI	X				
ITU/ISO/IEC joint IPR policy				X	

[63] FRAND/RAND terms can also cover royalty-free licensing. This table makes a distinction to highlight existing typical differences. The IPR policy of several SDOs, such as ETSI, requires identification of individual patents as potentially essential.

Table 4: Comparison of other licensing policies

NAME	FRAND/RAND or other reasonable non-discriminatory licensing commitment	ROYALTY-FREE licensing only (Typically with other terms being (F)RAND)	ROYALTY-FREE licensing with possibility to opt out	FRAND/RAND or royalty-free licensing commitment	OTHER licensing terms
IEEE	X Or covenant not to enforce the SEP[64].				Non-binding reference to value based on smallest saleable compliant implementation.
IETF				X Or covenant not to enforce the SEP. No mandatory commitment, but lack of commitment may lead to choice of alternative technology.	
OASIS					Depends on the Technical Committee (TC) that develops the standard : 1. RAND mode TC with RAND licensing; 2. Royalty free mode TC; 3. Royalty free with other terms being RAND; 4. Non-assertion mode TC where the SEPs are unenforceable.
OCF					OPEN SOURCE implementation
LoRa		X			Membership and reciprocity requirement
Z-Wave			X Royalty-free and otherwise		

[64] SEP or Standard essential patents are patents that cover technology to which a standard makes reference and that implementers of the standard cannot avoid using.

NAME	FRAND/RAND or other reasonable non-discriminatory licensing commitment	ROYALTY-FREE licensing only (Typically with other terms being (F)RAND)	ROYALTY-FREE licensing with possibility to opt out	FRAND/RAND or royalty-free licensing commitment	OTHER licensing terms
			RAND license, but possibility to signal that there is no guarantee for granting the license ("withholding of license") to the SEP		
Connectivity Standards Alliance (previously Zigbee Alliance)	X So-called RANDz license. Possibility to opt-out ("Necessary Claims Notice"), but opt-out may lead to choice of alternative technology.				RANDz terms also apply to SEP claims that "directly relate" to the relevant specification, even if those are subject to other SDOs' IPR terms.
Matter (previously CHIP) working group within the Connectivity Standards Alliance		X			Royalty-free terms also apply to SEP claims that "directly relate" to the relevant specification, even if those are subject to other SDOs' IPR terms. Membership linked to membership within the Connectivity Standards Alliance.
Thread			X		Membership requirement
VII	*Not yet applicable*				
EnOcean		X			Membership requirement (check)
Mioty					Company SISVEL manages IP
OVN					Largely OPEN SOURCE
OneM2M	X Via its partner SDOs that all support (F)RAND terms.				

NAME	FRAND/RAND or other reasonable non-discriminatory licensing commitment	ROYALTY-FREE licensing only (Typically with other terms being (F)RAND)	ROYALTY-FREE licensing with possibility to opt out	FRAND/RAND or royalty-free licensing commitment	OTHER licensing terms
GSMA	X (only exceptional, justified opt-out)				
ioXt Alliance	No unified IPR Policy. Certification only to members.				
HubbTV Association	Based on a combination of elements of existing standards. No unified IPR Policy.				

(224) As the indicative tables above suggest, IPR policies of SDOs and independent alliances vary greatly, impacting contributors to the standard development, as well as implementers of the standards.

(225) SDOs and private alliances that, as a matter of principle, have a royalty-free approach, may either decide to accept technical contributions for which the contributor would request a royalty and allow the contributor to declare in due time its intention to opt out from the royalty-free licensing, or not allow for an opt-out and exclude any royalty-claiming contribution.

(226) Where an opt-out is made possible (see the examples in the above table), the IPR/licensing policy of the SDO or private alliance would typically allow members to replace the royalty-claiming contribution (following the declaration of the opt-out) with an alternative, royalty-free contribution. SDOs and private alliances that intend to warrant a royalty-free outcome exclude any royalty-claiming contribution.

(227) SDOs and private alliances that operate under IPR rules that do not allow for the exclusion of royalty-claiming contributions are not able to warrant royalty-free terms for their specifications.

(228) Respondents report that some SDOs and independent alliances do not have sufficiently clear patent declaration or licensing rules to duly assess the likelihood of open source elements or royalty-free/royalty-bearing (standards-essential) patents in the standard or specification.

(229) In addition, royalties are not the only costs implementers face. Many alliances only license to members that pay membership fees. These range from a couple of hundreds of dollars or euro a year, up to, for instance, USD 75 000 yearly "Promoter" membership fees in the Connectivity Standards Alliance (in addition to USD 15 000 for a yearly "Participant" membership), a USD 100 000 yearly "Platinum Sponsor" membership in the OVN, (or USD 7 500 for the lower implication "OVN Advocate"

membership), USD 65 000 yearly "Sponsor" membership in the Thread group (USD 15 000 for yearly "Participant" membership), and a similar amount (USD 65 000 for "Founding" or "Principal" membership and USD 10 000 for "Manufacturer" membership) in Z-Wave Alliance. Implementer-only memberships are typically less expensive (from a couple of hundred to a couple of thousand dollars or euros). Moreover, certifications are also costly, based on a direct certification fee or dependent on a yearly membership to the relevant organisation or alliance. As a result, the implementation of royalty-free or open source technologies may in fact still generate significant costs for implementers.

6.4 THE ROLE OF STANDARDS AND PROTOCOLS VS. PROPRIETARY TECHNOLOGIES IN CONSUMER IOT

(230) Responses to the questionnaires reflect a highly heterogeneous environment: devices and services rely on a combination of open standards, protocols, and proprietary and open source technologies. For the purposes of this report, proprietary technology refers to technology owned by a company and not subject to an open source licence. Proprietary technology may be licensable or not licensable to third parties. Technologies in the consumer IoT sector are typically mixtures of the above, with components relying on open standards or open source technologies, and others on proprietary technologies: either own technologies or licensed from third parties. The combination of standards, proprietary and open source technologies largely varies depending on the different technology layers incorporated in devices and software programmes.

(231) On the one hand, basic enabling technologies are mostly based on open standards. Some of the most prevalent categories of standards in the consumer IoT sector are:

- Lower level connectivity standards, such as Bluetooth, WiFi, 802.11 a/b/g/n/ac, IEEE 802.15.4 (WPAN), Ethernet, USB, HDMI, Connectivity Standards Alliance, Thread or Z-Wave;
- Audio codecs (for example MP3)[65] and Video codecs (for example MPEG-2, Open XR that is an open standard for access to virtual reality and augmented reality platforms and devices)[66], or the HEVC video compression standard;
- Transfer/streaming/messaging standards and protocols such as HTTP, Bluetooth TCP/IP, RTP, HLS, MPEG-DASH, SIP, LoRaWAN, MQTT (Message Queueing Telemetry Transport), TLS (Transport Layer Security), SCEP (Simple Certificate Exchange Protocol), AMQP (Advanced Message Queuing Protocol); DDS (Data Distribution Service);
- Content Standards (HTML, JSON);

[65] Other examples include AAC-LC, HE-AACv1, HE-AAC-v2.
[66] Other examples include H.265, H.264, H.263, MPEG-4 parts 2, 10, 29.

- Cybersecurity (ETSI EN 303 645, ETSI TS 103 701)[67]; and
- Other: IEEE P360 (overview, terminology and categorisation for Wearable Consumer Electronic Devices), IEEE P1708 (Wearable Cuffless Blood Pressure Monitors Working Group), Wireless payment standards (such as NFC), ISO 22810:2010 (water resistance for wearables), ISO 6425 (specifications for divers' watches).

(232) While the above technologies are specified in standards, their implementation can be proprietary or open source (for example the implementation of a video codec by the hardware/software to perform the encode/decode function may be proprietary or open source). In the same vein, those standardised technologies may also have proprietary enhancements for the purposes of specific devices or applications, such as enhancements for security reasons, in order to control access on network level.

(233) Such proprietary or open source implementations and enhancements of standardised technologies further add to the complex and heterogeneous technical environment.

(234) Many respondents find access to certain standards, such as to the major lower level connectivity standards (for example Bluetooth, WiFi, Connectivity Standards Alliance), essential to their ability to compete. However, depending on the profile of the respondents, most of the standards are not seen as essential for them to compete. This is due to the existence of other, competing technologies, and the relatively limited user base for many of those competing technologies.

(235) On the other hand, device definitions, application layers and user interfaces rely more often on *proprietary technologies*.

(236) Examples of proprietary-based technologies relevant in the segments covered by the sector inquiry are: audio components (microphones, speakers/transducers); display components (LEDs); sensors (cameras, light sensors, passive infrared sensors); mechanical components (enclosures, frames, brackets, light pipes, heat sinks and other thermal Management); integrated circuits (IC): analog-to-digital converter ICs, digital-to-analog converter ICs, power management ICs, amplifier ICs, switch ICs, electrical components (buttons, switches, connectors); software settings and updates, personalisation, catalogues, parental control systems, launcher (including app launching, UI/UX, browsing, search features), UI Library, information architecture, customer support services, app store services; cloud services management; mesh routing and management; access point management; firewalls.

(237) However, device definitions and application layers may also be standards-based (see for instance the widely used Connectivity Standards Alliance and KNX standards). User

[67] Some national authorities in the EU have published specific security recommendations on critical consumer IoT devices. One example is BSI (Bundesamt für Sicherheit in der Informationstechnik) in Germany with TR 03148 on broadband router for smart home and building application.

interfaces however are at least combined with the provider's proprietary technology in order to bring a differentiated offering to users.

(238) Respondents to the sector inquiry were asked about the most widely adopted proprietary technologies in the areas covered by the sector inquiry. These were referred to as "*de facto* standards" in the questionnaires and defined as "proprietary technology with a large user base that competes with standards". The proprietary technologies of the following products have been highlighted as the main *de facto* standards:

- For voice assistants : Google Assistant, Amazon Alexa, Apple Siri
- For smart home devices: Google Home and Weave,[68] Amazon Echo, Prime Video API and AVS,[69] Apple HomeKit and Apple MFi,[70] and Dolby Digital. Many respondents also highlight the large user base of the Open Connectivity Foundation Smart Home Project and the Open Voice Network.
- For wearable devices: Apple Watch, Samsung Galaxy Watch, ANT+ (by Garmin)

(239) Nearly all respondents find full interoperability with these technologies and ecosystems essential to compete[71], as these technologies are identified as enablers for consumer IoT products and services. Due to the popularity of the above voice assistants and devices, offering products or services in the consumer IoT sector that could not integrate or interoperate with the above technologies does not seem to be a viable option. Rather, the integration and interoperability of hardware and software with the above proprietary technologies is mostly presented as a "must have" for consumer IoT hardware manufacturers and software developers.

(240) However, the owners of the above technologies generally stress that the existence of such proprietary technologies does not mean that any IP rights would prevent third parties from developing and/or implementing technologies with comparable functionality. In the same vein, various SDOs also express the view that the above proprietary technologies are not essential, as other open standards/protocols and proprietary technologies with similar functionality are available to compete in the consumer IoT sector.

[68] Google's Weave is an open source network application layer protocol and the implementation toolkit for consumer IoT applications. It is an "information schema" that defines common types of devices to have a common language and be able to communicate with each other. It is fully integrated with Android, so products that use it will be instantly recognised by users' mobile devices.

[69] Amazon AVS (Alexa Voice Service) is an API that enables developers to integrate Alexa directly into their smart products. The AVS Device software development kit (SDK) enables smart devices to process audio inputs and triggers, establish persistent connections with AVS, and handle all Alexa interactions. The SDK also allows adding third-party wake word engine and audio player.

[70] Apple's MFi Program offers a broad range of wireless and wired technologies that can be used to connect hardware accessories to Apple devices.

[71] The owners of these technologies typically do not find their own technologies essential to compete.

6.5 THE EXPECTED EVOLUTION OF STANDARDISATION IN THE NEAR FUTURE

(241) Approximately 60% of the respondents to the different questionnaires express the need for further standardisation in consumer IoT, while approximately 40% would not prioritise further standardisation over proprietary developments. Those that consider there is a need for further standardisation, however, largely acknowledge the difficulties and potential risks relating to it, which may lead to a slowing down of future standardisation.

(242) On the one hand, many see standardisation as crucial for achieving true, fully functional, "plug and play" interoperability: for hardware and software to be able to fully integrate and communicate, thereby offering a greater choice to consumers and building consumer trust in the various segments of consumer IoT markets. Amongst others, telecommunication service providers express the need to support commonly developed, open technical standards instead of relying on *de facto* standards, developed by a limited number of large players. Communication standards are highlighted as particularly important, with an ever-growing variety and number of devices and applications that need to rely on them.

(243) The fact that proprietary technologies are not subject to FRAND terms further reinforces the views supporting the need to prioritise standardisation over proprietary developments.

(244) In that context, the rules and procedures of SDOs in terms of contributions and IPR policies are seen as an important factor that may impact the future of standardisation in consumer IoT. Recognised SDOs that are open to all participants, and "*de jure*" standards, are identified by some SDOs as warranting an inclusive process that would not be monopolised by the private initiatives of large corporations.

(245) On the other hand, many argue that standardisation is not necessarily the best solution for interoperability in the consumer IoT sector. Standardisation would be desirable when it solves customer, business, and technical problems more effectively and more cost-efficiently than other approaches, such as proprietary solutions or open source solutions. Respondents argue, among other points, that open source and other proprietary solutions can be equally efficient to standards, as long as they are well-documented, and allow for an easy, less costly and full integration of, and interoperability with, devices and applications.

(246) While most respondents acknowledge the importance of standardisation for the future evolution of consumer IoT, many plead for the need to consolidate the already existing standards, rather than developing even more competing and potentially conflicting standards. Increasing the number of competing standards would not necessarily lead to better choice for consumers, but rather generate the risk of even less interoperability between the different hardware and software technologies.

(247) The number and the cost of existing standards are put forward as disadvantageous to smaller players, creating barriers in terms of overall production costs and procedural/administrative and legal burdens. In addition, various respondents claim that the leading role of large technology platforms in the standardisation processes leads to them pushing their own technologies, thereby concentrating innovation within the leading players that "own the standards", and generating a barrier to wide standardisation in the longer-run.

(248) A few respondents expect patent pools to gain significance in IoT, as they may reduce transaction costs, also possibly reducing the aggregate royalty for the total number of SEPs present in consumer IoT products.

(249) In terms of the proprietary technologies, many respondents single out the Matter and the VII projects as having the potential to bring together sufficiently wide user bases to address technology fragmentation challenges in consumer IoT. A few players identify a move towards two, well-differentiated types of partnerships as a potential option. In this situation, a first type of partnership would group players around the large ecosystems and a second type of partnership would group together more specialised hardware manufacturers and/or application developers for the development of technologies, allowing for better integration and interoperability of their products, both among each other and into the large consumer IoT ecosystems.

(250) Overall, over 80% of the respondents to the different questionnaires nevertheless expect standardisation to develop further in consumer IoT segments in the coming years, in particular for basic, enabling technologies. A slower development of standards (including for other technology layers) is however expected as a result, among others, of newly emerging technologies (including AI/Machine learning) and continuously evolving use cases, generating ever-changing requirements and challenges for standards (including in terms of related, crucial aspects such as secure data exchange or energy efficiency of large data-transfers).

6.6 KEY FINDINGS

As a result of the nature of the segments covered by the sector inquiry, where an unprecedented number of different hardware and software technologies need to interconnect in real-time, the market for "isolated", standalone smart devices is more limited, and ecosystems are more prone to achieving high market penetration.

The integration of stand-alone technologies into such ecosystems is reported as a "must-have" for consumer IoT hardware manufacturers and app developers. This, in turn, leads to an environment in which proprietary technologies of such eco-systems play a major role, in particular at the level of device definitions, application layers and user interfaces. While standardised technologies prevail at the level of basic enabling technologies, formal standards are currently not in a position to compete effectively with proprietary technologies of the leading providers of operating systems and voice assistants for other types of technologies such as device definitions, application layers and user interfaces.

7 DATA

7.1 OVERVIEW

(251) This chapter concerns the role of data in the consumer IoT sector. This role is explained based on answers provided by respondents on the part data plays in the operation of their businesses, and the functionality of their devices and services.

(252) The first part of this chapter looks at the role of data in the context of the business-to-consumer (B2C) relationship, addressing how and when devices and services collect data, what type of data they collect, what access users have to their data and what ability they have (or do not have) to port it between different devices and services.

(253) The second part of the chapter focuses on business-related aspects of consumer IoT data. This includes the circumstances in which data flows between third-party devices, services and/or voice assistants, how the data is processed and what format it takes, the purposes for which the respondent companies use the data, and whether and to what extent respondents monetise the data they collect.

7.2 USER-RELATED ASPECTS OF CONSUMER IOT DATA

(254) Manufacturers and providers of consumer IoT products and services collect data in a variety of circumstances, including through the manual input of a user, in the context of the use of a device or service, or automatically, for example as part of them functioning in the background. Many types of data are collected.

(255) Consumer IoT products and services collect data to facilitate their connected nature. In many cases, data collected in a B2C relationship, between a device manufacturer or service provider and the user, will come under the definition of personal data for the purposes of the GDPR. More information about the access to personal data for individuals and the definition of personal data is provided in Section 7.2.4 below. Collection of data from terminal equipment, that is a device connected to a public communications network, is only allowed with the consent of the user or subscriber concerned, or for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary for the provision of an information society service explicitly requested by the user or subscriber[72]. Several respondents specify that such data are only collected with the knowledge of the user and, in particular instances, only when the users have opted in to have additional data collected (for example, as part of a research programme or where they agree to contribute to data analytics).

[72] Article 5(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ L 337, 18.12.2009, p. 11.

7.2.1 How data is collected

7.2.1.1 User input

(256) A device or service can collect some data through the direct manual input by the user. This can include the personal and contact information entered when a user sets up an account to use a service for the first time or when installing a device. Other examples of when a device or service receives data via this direct input include when users enter their height, weight, or information about their activities into their wearable fitness device or its companion app.

7.2.1.2 Through use of the device or service

(257) Other data is collected by the device or service through its use, with or without direct interaction with the user.

(258) For example, a smart TV collects device usage data whenever a user carries out certain actions, such as turning the device on or off, moving from one service to another, or when the user is navigating a selection on the TV. Consumer IoT services also collect data when the user interacts with that service, for example, the interactions involved in carrying out a search or making a purchase.

(259) The device can also collect data when it is in use without direct user interaction. For example, robotic vacuum cleaners store maps of houses in their internal memory made up of data they collect while cleaning, and a music streaming service may collect data about the songs playing while the service is active.

7.2.1.3 Automatic or background data collection

(260) Smart devices can also collect data automatically as part of their 'background' functioning or when in standby mode, and can passively collect data in situations where the user has not taken any action. Examples of such types of data include functional background tasks such as error logs or diagnostics or data required to calculate analytics. Providers of consumer IoT services state that they do not generally collect data when the service is not active.

(261) Some smart devices, such as some types of security devices, do not require user interaction to carry out their function but have sensors that collect data, including visual and acoustic data when they are triggered. This can include motion sensors registering movement, a device equipped with facial recognition identifying a person, or devices with voice recognition registering a command.

7.2.2 Types of data collected

(262) Contact details such as names and email addresses, location information, and IP addresses are the most commonly collected data points indicated by the respondents. Payment information in the form of credit card details may also be collected, along with

other discrete items of data about the users themselves, including their gender, profession, and level of education.

(263) Other types of data collected vary depending on the consumer IoT segment concerned. This data can include personal or other user data, whether in the form of information input by the user, or of user behaviour information collected through the operation of the device or access to the service. In addition, smart devices and consumer IoT services can gather data about how they function themselves and about their surroundings.

7.2.2.1 Smart home devices

(264) The data collected by smart home devices can relate generally to user behaviour and the usage history of the device, by collecting data each time the device is used or a consumer IoT service is accessed via the device.

(265) The data can also include specific information on operational parameters relating to that particular device. For example, a smart washing machine may collect data on the washing cycle chosen and how often the user chooses this setting. A smart coffee maker may collect data on the settings selected when brewing coffee, collecting data on the preferred beverages and times for making coffee. An electric smart toothbrush can collect data on the pressure applied when brushing and the time taken.

(266) A smart home device can also collect data about the task it is carrying out, enabling it to carry it out more efficiently, such as the example provided above of automated robotic vacuum cleaners storing a map of a house in their internal memory for future use.

(267) Other smart home devices collect data on their environments and status. Examples include a smart connected refrigerator noting the temperature, or the status of the water filter. A smart thermostat or heating system can collect data on household temperature and air quality, movement, the heating system being switched on and off, and can register when users leave and arrive home. Home security devices collect information on users' interaction with the system, as well as gathering audio or video data when, for example, a sensor is triggered.

(268) Respondents indicate that smart home devices can also gather more general behavioural data, such as the user's preferred times for using the device and how often the device is used. For example, when a smart home device is accessed via a voice assistant, the device may collect data related to the specific instruction or command given to the device (for example on/off, temperature increase/decrease) as well as the date and time of the command.

(269) Smart home devices can also collect information confined to the device itself and its use, such as device type and ID, or software status. For instance, this can be the case where there are no user profiles associated with the device. Such general device data can also include usage history of an account, error logs (abnormal information) and technical interventions.

7.2.2.2 Consumer IoT services

(270) Providers of consumer IoT services indicate that the services collect account data, behavioural and usage data, and technical data related to the service and/or other consumer IoT components (for example the device on which it runs), or whether it is connected to the internet.

(271) Whether or not a user has an account with the consumer IoT service is relevant for the purposes of data collection. Where a service provider requires users to have an account in order to use the consumer IoT service, as is often the case, information such as personally identifiable information and contact details are collected when the users set up their account. In different instances, users may or may not need to be signed in to use a service, and certain data may only be collected when they are signed in. When the users do not sign in, respondents indicate that the data collected may be limited to technical information such as IP addresses and analytics data.

(272) Where a user has an account and signs in to this account to use the consumer IoT service, the service will typically collect data such as login details (user ID, email address and password), profile information (username, language, profile picture), and settings (communication preferences, editorial preferences, personalised advertising, public/private profile).

(273) Consumer IoT services may collect behavioural and usage data, including the user's usage history and habits. For example, an audio streaming service collects data on which podcasts the user has listened to in the past and added to their list, and a VOD service will collect data on viewing history, favourites and ratings on titles.

(274) Other services collect technical data on interaction with the service and how the user navigates it, such as data on paths taken to access content, the time the user initiates and finishes a session with the service, and search queries. Other technical data mentioned by respondents include information on the device (type of device used, hardware model, version of the operating system), information on the internet connection (internet service provider, type of connection), and analytics data (usage trending over time, number of recurring users, errors).

7.2.2.3 Voice assistants

(275) Voice assistant providers indicate that voice assistants collect data related to their interactions with users. This includes voice and language recognition data and audio of the queries and commands received, as well as conversation history between the user and voice assistant in text format.

(276) Voice assistants also collect data beyond the content of the user query itself. For example, a voice assistant may collect contextual data on when the query was made, what device the query was made from (such as its location or IP address), and whether or not the query was successful.

(277) Depending on the purposes for which the voice assistant is used, it may be able to access data in consumer IoT services linked to the voice assistant account, for the purposes of, for example, reading emails aloud to the user or making appointments in the user's calendar.

(278) Where there is this link between voice assistants and consumer IoT services, a voice assistant may collect location data enabling it to tailor its responses to the most suitable options or to provide accurate responses on geographically specific queries, such as those about the weather. In addition, as one respondent indicates, the user can provide data such as locations and other supplementary information unconsciously. For example, when a user asks a voice assistant to order a taxi to a location, he or she will consequently provide an address to the voice assistant. One submission to the public consultation on the preliminary report refers to the fact that the human voice may provide some insight into a wide range of information about the user and its behaviours, including socio-demographic aspects or even on certain physical and mental health conditions.

(279) Voice assistants can also collect other technical information not related to queries, such as data about the device on which they are installed (for example IP address and operating system), and technical logs used for support purposes.

(280) As voice assistants are frequently used in connection with smart devices and/or consumer IoT services, they will collect different data in these use cases. This will be discussed in detail in Section 7.3.2 below.

7.2.2.4 Wearable devices

(281) Wearable devices, particularly those of fitness or health trackers, commonly collect biometric data about users and data about the activities they carry out. This can include information such as height and weight, heart rate during exercise and while at rest, body temperature, data on sleeping patterns, calories burned, and location data for the purpose of for example logging distance or altitude gained during an activity.

(282) Wearable devices other than fitness or health trackers can collect data on the settings used (such as volume for headphones, or data on whenever certain features are used for a smart wearable camera). Wearable device manufacturers also indicate that their devices collect data about the device itself, such as serial numbers and connectivity. Wearable devices can also collect data through, and in conjunction with, their companion apps installed on mobile devices. More advanced smart watches can also access and collect data from consumer IoT services such as calendars, email or other messaging applications.

7.2.3 User access to data

7.2.3.1 Types of data to which the users have access

(283) Users have the right to access personal data collected about them according to Article 15 of the GDPR. The right to access personal data also includes a right to obtain information about for example the purposes of the data processing, the categories of personal data concerned and the recipients or categories of recipients with whom the personal data is shared.

(284) The findings of the sector inquiry show that most respondents, across all consumer IoT segments, give users access to their personal data collected via the respondents' smart devices, consumer IoT services and voice assistants. Article 4 of the GDPR provides that in order for data to qualify as "personal data", the user must be "identified" or "identifiable". Most respondents indicate that the data collected via their smart devices, consumer IoT services and voice assistants is linked to a specific user via a user ID or user account, and that the user can thereby be identified and linked to data collected about him or her. A few respondents indicate that they do not register users or that they only collect data on an aggregated and anonymised basis. Therefore, the data cannot be linked to a specific user or be subject to an access request.

(285) The data points to which a certain company gives the user access depend on what data the company collects and this is determined individually by each company (see also Section 7.2.2.).

(286) A few smart device manufacturers indicate that the data generated via the use of their device is actually not or only to some extent collected by them. An example given by respondents is the situation when a smart device is controlled via a voice assistant. In that case, most data concerning the use of the smart device is collected by the voice assistant provider. Consequently, the smart device manufacturer either does not have access to the data related to the device usage or has access only to some of it and can therefore not provide users access to it.

(287) Most respondents indicate that users generally do not have access to more technical, non-personally identifiable information, such as data collected for security purposes, for the purpose of customer support or for problem analysis, as well as data collected through cookies and other automated technologies. Others explain that they only give access to this type of non-personal data in an aggregated form.

(288) Where a user is connected to several smart devices from the same manufacturer or to consumer IoT services of the same service provider, the user often has access to all the data collected by that manufacturer or service provider, via the user's ID or the user account. Some respondents indicate that they design their smart devices and consumer IoT services with a view to minimising the amount of data collected by the devices and services, and that it is the user who controls what data is collected. According to these respondents, data minimisation enhances privacy and security while also promoting user

control, by limiting the parties with access to the data and who could therefore use the data in a manner not approved by the user.

7.2.3.2 Ways in which the user can access data

(289) The findings of the sector inquiry show that companies give users access to their data in different ways, which will depend on factors such as the type of smart device or consumer IoT service that the company provides and its intended use. The replies to the sector inquiry indicate that the following are the most common ways in which the respondents provide users access to their data:

a. Many respondents explain that the users have access to their personal data **via the user account** that can be accessed in a smart mobile device application or on the company's website. A user would in general need to synchronise the smart device or consumer IoT service to the smart mobile device application and log into the account in order to get access to the data. One example provided by respondents is that certain models of smart watches must be synchronised with the companion app, via which the user must log into the user account in order to access the data collected via the smart watch.

b. Respondents explain that users can also access their personal data via **user interfaces other than smart mobile device applications and web-based applications**, for example, the screen of a smart home hub. In order to do so, the user needs to synchronise the smart device or consumer IoT service with the user interface before being able to access the data.

c. Users can sometimes access part of their personal data **directly on the smart device**. For example, the user can access fitness- and activity-related data such as steps, distance, calories consumed and the user's heart rate on a wearable device.

d. Some respondents explain that they have developed **specific tools or technology** that facilitate users' access to data. One example is Google's data retrieval platform "Google Takeout". It allows users to import and export data from a number of Google products and services. Another respondent explains that it has developed a specific technology that facilitates data reporting. It enables the user to manage easily his or her personal data in order to control data privacy and security. Via this tool, the user can also download the data in the format of a PDF report.

e. Users also have the option to make a **data export request directly to the data processor**, in order to access their data. As set out in Article 15 GDPR, such requests can be made by electronic means[73]. Most respondents indicate that they provide users with access to their personal data following a request by the user via email or the

[73] Article 15 of the GDPR provides that: "*Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form*."

company's website. For example, users of Amazon's services and devices may access their data by submitting a Data Subject Access Request via the "Request My Data" feature on the Amazon website.

7.2.4 Data portability

(290) According to Article 20 of the GDPR[74], users have the right to receive a copy of their personal data that was collected by one company, and "transmit" that data to another company. Such data portability must, according to the same article, be based on the user's consent or on a contract. Article 20 GDPR also specifies that the user shall receive the data "*in a structured, commonly used and machine-readable format*" and that, "*where technically feasible*", the data shall be ported directly from one company to another.

7.2.4.1 User managed data portability

(291) A majority of consumer IoT service providers and smart device manufacturers indicate that they give users the possibility to access and download their personal data and that the user can also port this data in accordance with Article 20 GDPR to third-party service providers and device manufacturers. In order to enable data portability between services and devices of different providers and manufacturers, the user would either need to access and download his or her data via an application or another user interface, or make a direct request to the data processor to access and take possession of his or her personal data.

(292) However, a few respondents across questionnaires state that it is currently not possible to port the data collected via their devices or services. One reason is that the data cannot be linked to a specific user, which is necessary for the data to qualify as personal data. One respondent states, "*As we do not require an account registration or a user profile, there is no mechanism to port any data tied to a specific user."*

(293) A few respondents report that their data cannot be ported because their consumer IoT service or smart device is unique and there are therefore no other services or devices to which the data could be ported in a meaningful way. Moreover, a few respondents

[74] The full text of Article 20 of the GDPR is the following: "1. *The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:*
(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
(b) the processing is carried out by automated means.
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17.
4. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others."

indicate that they have so far not received any data portability requests from users of their services or devices.

(294) As regards voice command data collected by voice assistants, some voice assistant providers explain that such data is specific to each voice assistant provider, all of which have their own technology to process such data. Commands already given to one voice assistant constitute "old" speech data, which cannot be used to train a different voice assistant, because of for example, the lack of industry-wide standards for natural language understanding APIs. Some voice assistant providers claim that portability of such data would therefore not be useful for them.

(295) Moreover, in relation to other data collected by voice assistants, it appears from the replies to the sector inquiry that there are currently limited possibilities for the portability of such data by the user. Some voice assistant providers explain that the data they collect via their voice assistants is anonymous and not associated with a specific user (account), and that the data therefore is not portable. Other voice assistant providers state that they do associate data collected via their voice assistant with user accounts, and that the user could access, download and port that data to third-party voice assistant providers but that those third-party voice assistant providers would not necessarily be able to receive or import their data.

(296) Overall, most respondents explain that they in general, as required by Article 20 GDPR, give the users access to their personal data in a structured, commonly used machine-readable format that the user can port to third-party consumer IoT service providers or smart device manufacturers. For the purposes of enabling portability, many respondents state that they make the data available in one or the more commonly used formats (that is JavaScript Object Notation (JSON),[75] comma-separated value (CSV), PDF).

(297) Furthermore, several respondents indicate that they only enable portability of their users' personal data provided that certain requirements are met, in particular that the accessing party respect all the requirements of the GDPR, as well as the exporting party's internal privacy rules.

7.2.4.2 "Direct" portability between data controllers

(298) The direct transmission of data to another data controller is set out in Article 20(2) GDPR, according to which "*[i]n exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible"*.

(299) A few providers of consumer IoT services state that their data could be ported *directly* from one service provider to another by automatically transferring the data between the applications of the two service providers. Such transfer requires, as set out in Article 20(2) GDPR, that the user has requested the transfer and that the two service providers

[75] The JSON and CSV file formats can be understood by both computers and human beings.

have made the transfer possible through API integration. The necessity of a user's explicit request was highlighted by submissions to the public consultation on the preliminary report.

(300) One example mentioned by respondents of such direct data transfer is the transfer of workout and nutrition data between different health and fitness applications.

(301) However, most respondents explain that they currently do not have a mechanism in place for such direct portability between data controllers. Developing the necessary integration for such direct transfer can require significant development efforts, to ensure security of personal data and a stable user experience. During the public consultation on the preliminary report, stakeholders emphasised the fact that, due to different formats used by different data controllers, there is currently no guarantee that the recipient of the data can directly use it in its systems. Several respondents explain that direct portability of content from one consumer IoT service provider or smart device manufacturer to another would require the development of industry-wide standards. With such standards in place, direct transmission of data between different service providers could take place in a secure and reasonable manner.

(302) Smart device manufacturers also explain that in order to enable direct portability of data between devices from different manufacturers, such as different smart devices in the same home environment, these devices would need to be integrated via APIs in order to enable data exchange between them. As regards data collected via voice assistants, several respondents to the sector inquiry explain that each voice assistant provider has created its own ecosystem and limits the transfer and portability of data outside of this ecosystem.

7.3 BUSINESS-RELATED ASPECTS OF CONSUMER IOT DATA

7.3.1 Data Formats and Processing

7.3.1.1 Data formats

(303) Across questionnaires, respondents report that there are no industry-wide standardised formats for collecting and sharing data between companies active in the consumer IoT sector. Instead, data is collected and processed either in a company-specific proprietary format, or in a non-standardised but commonly used non-proprietary file format that enables the data to be directly shared with and used by third parties.

(304) In particular, several respondents explain that they collect and share data in commonly used non-proprietary file formats such as JSON-formatted files or CSV files. Respondents also explain that certain data types such as IP addresses are in a standard format, which is directly sharable and usable by third parties. Several wearable device manufacturers explain that they collect and share data in the commonly used FIT file format, which has become a *de facto* standard data format for data sharing on the wearables market.

(305) Other respondents report that they and their business partners in the consumer IoT sector share data in a proprietary format that is unique to each partner. In such cases, different actions such as data cleaning, processing, validation, decoding etc. are needed to reformat the data into a directly accessible format usable for third parties, for example CSV. Where data that was stored in a proprietary format is shared with a third party, the data holder might need to give access to its APIs and/or SDKs in order for the third party to be able to use the data. The format of the data is then decided on the basis of those APIs/SDKs.

(306) Consumer IoT service providers explain that when their services are integrated with a voice assistant and data is shared as a necessary functional part of that integration, the data must be in a format that is directly usable by the voice assistant (provider). In those cases, the data format is determined by the APIs of the voice assistant provider.

(307) Many respondents to the sector inquiry explain that when they share data with a contractual party, they often agree with that party on a format for data collection or sharing. That agreed data format may be contractually regulated between the parties. Other respondents explain that data formats are sometimes determined via the APIs and SDKs of one company. There are indications that some companies, such as the leading voice assistant providers, impose the use of a certain data format for access to and sharing of their data via their APIs and SDKs.

7.3.1.2 Data processing

(308) Voice assistants, consumer IoT services and smart devices collect significant amounts of data, such as millions of interaction data points and billions of logs monthly. Depending on the circumstances, the companies collecting this data then share, store, aggregate, clean, normalise, format or process the data[76] in other ways in order to create value for the company, and possibly also for third parties.

7.3.1.2.1 Data processing locations used by the respondents to the sector inquiry

(309) Across questionnaires, respondents explain that they process data mainly in the following locations: (i) on the smart device, (ii) in a companion app on a smart mobile device, (iii) in third-party cloud service providers' processing infrastructure ("in the cloud")[77] and (iv) in company-owned processing infrastructure ("on-premise").

[76] For the purpose of this section, "data processing" refers to an operation or set of operations which is performed on data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data as well as the storage of data".

[77] Respondents use the term "cloud" in different ways in their replies to the sector inquiry. Some respondents refer to a broader category of processing locations as the "cloud". For the purpose of this report, the definition of "cloud computing services" provided in Article 4(19) of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1–30), is used and which defines "cloud

7.3.1.2.1.1 On-device processing

(310) According to the replies, typical examples of on-device processing include data processing on a wearable device and temporary data storage on a hub in a smart home environment. Several respondents refer to the following three reasons for processing data on-device:

a. A first reason for data processing on-device is response time, that is, the time needed for a signal to reach another processing location, and for the result to return to the device. Respondents choose to process data on a smart device if the response time is too long to allow for a desired user experience. For example, as regards wearable devices, the response time might be too long to allow for the fast display of data collected by sensors on a wrist-worn device.

b. A second reported reason for on-device processing is that some smart devices are less dependent on a permanent and fast internet connection for data processing, such as wearable devices, which might not have permanent internet access.

c. A third reason for on-device processing mentioned by some respondents is smart device battery consumption. Manufacturers of wearable devices explain that the sending of data to a server consumes significant battery power of the sending device, which some manufacturers of wearable devices characterise as scarce.

(311) Respondents indicate that data is transferred from the smart device to other processing locations such as smart mobile devices, the cloud, or company-owned infrastructure, in particular when data processing involves complex computations, or if data aggregation is necessary. Respondents indicate that they may aggregate data from one smart device and/or across several devices and consumers to compute anonymous business metrics in other storage locations, such as company-owned processing infrastructure or the cloud.

7.3.1.2.1.2 Processing in a smart mobile device application

(312) A second location for data processing mentioned in replies to the sector inquiry is the smart mobile device application. For example, data may be processed in a smart mobile device application for the purpose of temporary storage of data, in order to transfer data to other locations such as the cloud or company-owned infrastructure, or to give users access to their data via such applications on smart mobile devices.

7.3.1.2.1.3 Processing in the cloud

(313) Most respondents indicate that they process at least some of their data in the cloud. Examples of data processing mentioned by respondents are sensor measurements, audio and video recordings, and device statistics. The findings of the sector inquiry show that

---

computing service" as "*a digital service that enables access to a scalable and elastic pool of shareable computing resources*".

the cloud services most frequently used by the respondents are Microsoft Azure, Amazon Web services and Google Cloud.

(314) Several respondents indicate that data processing in the cloud typically takes place via different specialised software solutions. Two frequently named examples are data lakes, which are repositories of raw data, and data warehouses, which are repositories of more structured data that allow for fast analysis. Respondents report that they use data lakes in order to combine raw data in a common storage solution, before data is prepared for further analysis using other solutions. A respondent explains that a data lake is a storage area that gathers data from multiple sources. Another respondent indicates that their "*data lake stores [all] the raw and non-aggregate data*". Examples of solutions used by respondents as data lakes are Microsoft Azure's Gen2 Data Lake and Amazon Web Services' Simple Storage Service. Respondents name speech data, log files or sensor data as examples of raw data stored in data lakes.

(315) Data warehouses are according to many respondents used to process more structured data to which fast access is needed. A respondent highlights as a difference between the use of a data warehouse and a data lake: "*Due to the volume and velocity of data, a Data Lake is suited to collect and store data, the data warehouse is well suited for high speed reporting*." Examples of data warehouse services used by respondents are Snowflake and Amazon AWS' Redshift or third-party software hosted on Microsoft Azure.

7.3.1.2.1.4 Processing on-premise

(316) Respondents explain that they generally opt for processing in company-owned infrastructure for smaller datasets, since this would be cheaper than using a cloud service, balancing fixed costs, variable costs, and service fees charged by cloud providers. As explained by one respondent, "*[t]he cost of on-premise [processing] is lower than cloud's when data size is smaller*".

7.3.1.2.2 Choice of processing solution

(317) Most respondents indicate that they use several data processing and storage locations and solutions simultaneously. Their choice of processing solutions depends on different factors, such as the characteristics of the data as well as the efficiency and costs of the specific solution.

(318) Respondents indicate that when choosing data processing solutions, performance is an important parameter, that is how fast a certain volume of data can be accessed and processed. For example, respondents indicate that for processing of complex data that needs to be statistically analysed, they would use more flexible processing solutions. For the ability to process large data volumes, respondents refer to data lakes. Data warehouses are used, for example, where fast analysis of data is necessary.

(319) Moreover, respondents report that they use different storage and processing solutions depending on the sensitivity of the data to be processed. As an example, sensitive data

such as payment-related data would in general be processed and stored on on-premise servers. Respondents also indicate that they often use encryption technology when processing sensitive (personal) data, and indicate health or location data as examples of data that would often be encrypted. Some respondents also explain that they use separate data storage solutions for personal data and for non-personal data.

(320) The findings of the sector inquiry also provide other reasons for the simultaneous use of multiple processing solutions. Respondents explain that cost is an important factor for their choice of processing solution. For example, the desire to reduce "managed overheads", that is, reduce the fixed cost of (temporarily) unused processing resources, would govern their choice of processing solution. Given that cloud services are on-demand, that is the user pays only for the services used, the operational costs of company-owned servers are absent, independent of dataset size, for companies using cloud services, and cloud services reduce managed overhead.

(321) Other reasons mentioned by respondents for simultaneous use of multiple processing solutions are the regulatory environment, the cost to change the location of data and business continuity. For example, changes to the company structure play a role for the choice of processing location. Some respondents explain that data processing and storage solutions used by the different companies involved in a concentration are not immediately combined after the transaction. Therefore, the companies would, at least during an initial period, continue using the different storage solutions used prior to the transaction. Some respondents also indicate that their decision-making regarding data processing and storage is decentralised within their companies and that sub-teams can make their own decisions regarding data storage.

7.3.2 Data collection from and data sharing with third parties

(322) As explained in Section 7.2., manufacturers and providers of consumer IoT products and services collect a broad variety of data, the types of which differ depending on the circumstances and use cases. Given that the consumer IoT sector is based on the interconnection of and communication between smart devices, voice assistants and/or consumer IoT services, data is – at least potentially – also collected from third parties within the same consumer IoT ecosystem and/or otherwise shared between these companies.

(323) In this regard, respondents indicate that, in general, consumer IoT data flows have a very functional nature, with data shared to allow smart devices, voice assistants and/or consumer IoT services *"to interact with each other"* and *"in order for the user interface to operate".*

(324) When voice assistants are involved, data flows allow for the processing and execution of the voice command. For example, when a user gives a command through a voice assistant to a connected lighting system, the voice assistant will collect data required to link user accounts and set up the lighting system, as well as data on the lighting system itself.

(325) Other examples of this functional data include smart device status information (for example on/off status shared by smart home manufacturers with voice assistant providers), user validation and authentication data, the time and duration of user access, or login data where a user sign-in is required. Similarly, providers of creative content services may share their catalogue metadata with voice assistant providers.

(326) Non-aggregated data related to errors or trouble-shooting problems may also be shared.

(327) According to a few replies, the voice assistant or other user interface provider is also managing data flows between smart device manufacturers and consumer IoT service providers. Indeed, several respondents indicate that there is no direct data sharing between smart device manufacturers and consumer IoT service providers.

(328) In the case of account linking (see Section 2.5.2), the data is typically made available to the third party as a result of this link between for example the user's consumer IoT service account and the user's voice assistant account.

(329) Access to data plays a specific role in the context of the provision of certain consumer IoT services that have revenue-sharing agreements with a variety of partners, including smart device manufacturers (see Section 4.5). Again, these data flows can be said to have a functional nature as they allow for the calculation and payment of the agreed revenue shares. In this context, partner services may also provide individual user identification data to facilitate the user's activation of a specific service within a bundled offer. For example, a consumer IoT service provider may provide the number of new subscribers who have signed up to the service on the specific partner device and/or service.

(330) Besides functional data provided on a continuous basis, some respondents have referred to aggregate performance data being shared on a recurrent (for example monthly) basis. One creative content service provider, for example, requires device manufacturers to provide monthly data in relation to how many times a service is launched or downloaded on a specific device, and other aggregate monthly metrics, while also requiring voice assistant providers to report aggregate metrics about voice usage data when users are interacting with the service.

(331) When data collected by one company (for example a consumer IoT service provider or voice assistant provider) can be accessed by a third party, this usually happens in practice via a central dashboard. Examples include the Apple App analytics, Actions on Google analytics console, and Amazon's Developer Portal. Typically, this data is aggregated and anonymised.

(332) Only a few examples of individual agreements to share additional or more granular information are mentioned. The parties concerned seem to be relatively prominent market players, which presumably have a better negotiation position. Yet, even in these cases, the data is said to be shared mainly in view of improving system performance and troubleshooting.

(333) However, even in the absence of active data sharing, some players will have access to data that relate to a third party's activities in the consumer IoT ecosystem. For example, smart device operating system providers may be able to collect information about a consumer's interaction with their service by virtue of the application being on the operating system. Aside from the operating system provider, such players with extensive data access seem to include voice assistant providers in particular. For example, for consumer IoT services accessible via voice applications, the relevant voice assistant provider will typically have insights on the user queries asked.

(334) Many respondents indicate that, in general, they do not share any data with other types of third-party stakeholders. If any data flows to other entities are mentioned, these mainly serve a functional or legal purpose. Firstly, several respondents indicate that government, judicial or regulatory authorities may require them to disclose data, including personal information, when legally required or otherwise necessary, for example to verify or enforce compliance with the applicable terms and policies or for security and safety reasons. Secondly, a number of respondents indicate that data may be shared with entities contracted by the company to execute certain tasks or provide certain services. Examples include the provision of an outsourced customer service, the provision of marketing assistance, of cloud services, the processing of payments or other technical services. Specific data-sharing arrangements in relation to (targeted) advertising are mentioned a few times as well, usually by consumer IoT service providers. Data-sharing for research purposes is mentioned by a limited number of players in the health and fitness market.

7.3.3 Contractual provisions governing business-related aspects of consumer IoT data

(335) Several contractual provisions seem to govern business-related aspects of consumer IoT data. One of the underlying objectives is to comply with applicable law, in particular the GDPR. For example, data transmission is governed by the applicable data processing agreement as required by Article 28 GDPR or a Controller to Controller agreement (Article 26 GDPR).

(336) Firstly, the technical specifications that allow the interoperability of devices and/or services, such as the applicable APIs and SDKs (see Chapter 5), describe in detail the data that is shared between the relevant parties. Contractual clauses regarding data processing are also generally included in licensing agreements governing the use of APIs and SDKs. Typically, these agreements specify that rights over data remain with the respective parties, and include clauses that prohibit certain uses of data (for example use of data with malicious intent) or limit the volume of requests to the API.

(337) Moreover, when the integration of the different consumer IoT segments is subject to a certification process (see Chapter 5), the relevant data sharing process and format are among the elements assessed.

(338) Secondly, given that much of the data concerned is of a personal nature, the privacy policies of each of the parties involved are also of relevance, including for data flow management.

(339) Thirdly, data flows seem to be governed by the (often standard) agreements between the parties. Contractual arrangements may nevertheless differ depending on the parties involved and, among other things, on the nature of the integration. For example, the provisions on data between a smart device manufacturer and voice assistant provider may be different depending on which technical connectivity solution is used. Different standard agreements may apply depending on the underlying operating system as well.

(340) In relation to personal data protection, respondents mention several clauses, which are typically based on the requirements set out in the GDPR. Such clauses often concern the scope and purpose of the data processing, user consent, security obligations linked to certain processing, such as data transfers, and liabilities in cases of privacy incidents. Moreover, many respondents explain that they require their data to be processed at certain geographical locations. Several EU-based companies explain that they require that their data, and in particular personal data, be processed on servers or in a cloud with a storage location located in the EU or the EEA only.

(341) Some contractual clauses prohibit the processing and storage of data that a company collects or receives based on the users' interaction with third-party consumer IoT products and services. In this context, several respondents indicate that companies with more market power, in particular the leading general-purpose voice assistant providers, can often impose their standard contractual clauses concerning data, with no possibility for the other party to negotiate deviations from them.

(342) Respondents to the sector inquiry explain that voice assistant providers often require smart device manufacturers and consumer IoT service providers not to record, process or store data related to the use of the voice assistant, and in particular, not to create user profiles based on such interactions. According to examples of such clauses, smart device manufacturers must not "*collect or store copies of any audio, transcripts, voice, metadata or other content either intended for or delivered by*" the voice assistant.

(343) Furthermore, agreements between voice assistant providers and smart device manufacturers limit the manufacturers' possibilities to store or modify data collected by voice assistants. For example, some clauses require smart device manufacturers not to alter audio that is recorded after an activation word is recognised and before the devices send the audio recording to the voice assistant provider's data centre. Some agreements also require device manufactures to delete all data they collect through the use of the voice assistant concerning a user if the voice assistant provider asks them to do so, even if this data is not personal data as specified in the GDPR.

(344) At the same time, agreements often allow voice assistant providers to use data received through the consumption of third-party smart devices and consumer IoT services to improve their own products or services. There are some exceptions to this, as some

respondents indicate that they have contractually limited the use of data by third parties to develop competing services. However, one respondent notes that there is little visibility as to what the voice assistant providers use the shared data for in practice.

7.3.4 Data use within IoT Companies

(345) The Commission asked addressees of the sector inquiry to detail the five most frequent ways in which they use the data collected through their smart home devices, wearable devices, voice assistants and consumer IoT services. The five most recurrent data use cases reported by respondents are: (i) the normal functioning of IoT products and services; (ii) personalisation of the user experience; (iii) business analytics; (iv) product maintenance and development; and (v) other use cases including marketing communications and safety and fraud prevention.

7.3.4.1 Normal functioning of IoT products and services

(346) The vast majority of respondents report that collected data is used primarily in order to provide and deliver the services and functionalities requested by the user that can be enjoyed through smart home devices, wearable devices, voice assistants or consumer IoT services. For instance, voice assistants use the voice commands that a user provides in order to fulfil the user's request, such as turning smart lights on or off.

(347) According to respondents' replies, personal data and data related to triggering events is essential for the functioning of consumer IoT products and services. Indeed, consumer IoT functionalities typically require interaction with the user or with the user's environment to execute requests (for example voice commands) or to detect the triggering events that would spark actions (for example motion sensors triggering the activation of smart lights).

7.3.4.2 Personalisation of the user experience

(348) In the second place, the majority of respondents employ data to evaluate the interests and preferences of users and make suggestions based on consumer behaviour. This allows respondents to personalise the user experience when using the smart device or consumer IoT service by recommending services, content or features, which increases the user-friendliness of the device or service and the perception of its value by consumers.

(349) The user's activity record or content consumption history is what enables companies to customise the experience and interaction of a particular user. Moreover, some respondents also analyse general patterns within groups of users, such as popular content among users of a certain age or gender, or frequent users of a particular service or device feature, in order to categorise users by segment and make targeted recommendations to clusters of users.

(350) Consumer IoT service providers emphasise the increasingly important role of data in the provision of content and media services. Content providers such as music streaming

providers, radio stations or video streaming providers typically personalise the experience by displaying content recommendations directly on the user interface or by content promotion via newsletters, e-mails or push notifications addressed to user clusters.

(351) With respect to voice assistants, providers indicate that they use collected data to suggest certain consumer IoT services and/or specific content. Given the key role that voice assistants play in the consumer IoT sector, leading providers of general-purpose voice assistants get an overview of the services and devices the user interacts with, which puts these players in a privileged position to personalise their offerings.

(352) Some respondents indicate that vertically integrated companies present in various consumer IoT segments (that is manufacturing smart devices and/or providing consumer IoT services and/or voice assistants) might connect information across their ecosystem to provide a more tailored and consistent experience for the user. This concerns mainly leading voice assistant providers (i.e. Google, Amazon and Apple), which also provide smart devices and consumer IoT services.

7.3.4.3 Business analytics

(353) The majority of respondents also report that they use data collected through their products to create statistics about the usage of their smart devices, consumer IoT services and voice assistants in order to better understand users' interactions and preferences, and take strategic business decisions on this basis.

(354) For this purpose, it is relevant for respondents to know how much time users interact with a service or feature; which features are most used on a device; the number of times a certain action or query is triggered; the audience of certain content and the quality of the services and features provided. By analysing these elements, consumer IoT players can get an overview of the usage frequency of different device features and consumer IoT services, in order to prioritise them for maintenance, upgrades and product development, or decide to withdraw a certain feature or service due to low usage.

(355) In particular, many respondents indicate that they collect and analyse data concerning which type of hardware and operating system version is the most common to access their consumer IoT services and/or to control their smart home and wearable devices.

(356) Data can also be used to monitor smart mobile device application engagement. In particular, data collected through the application can be used following an application update to analyse whether the improvements have led to a better experience. Some respondents also conduct satisfaction surveys about their applications. Likewise, data is also used by some respondents to determine the effectiveness of a particular marketing campaign or promotion.

(357) Looking at business analytics in particular consumer IoT segments, some wearable device manufacturers indicate that they analyse how people typically wear their product (for example duration of wear) and how they engage with their companion apps. On the

other hand, some smart home device manufacturers and voice assistant providers analyse data collected to understand the distribution of smart home devices and models within the household.

7.3.4.4 Product maintenance and development

(358) The majority of respondents indicate that they use data for product maintenance in order to ensure that their smart devices and consumer IoT services are working as intended and to plan upcoming upgrades. Data is also used in order to ensure communication with the customer to provide technical support and aftersales maintenance (that is appliance malfunctions, component defects, problems with cloud registration).

(359) Further, the majority of respondents report that the data collected through their smart devices and consumer IoT services is used for improving their products and developing new functionalities and offerings through their existing devices and services. For this purpose, respondents monitor the functioning of their devices and services and how users interact with them.

(360) In the case of voice assistant providers, voice recordings consisting of voice commands (questions, requests and instructions given by users) and the feedback provided by the assistant (such as responses, answers and content) may be processed for the improvement of natural language understanding and speech recognition technology. This can enhance the accuracy of the assistant's interactions with users and reduce the number of mistaken activations. Voice assistant providers might also monitor unanswered queries so they can build capabilities to respond better in the future.

(361) In this regard, voice assistant providers with a large user base are better placed to collect and use customer speech data in order to improve their service, while smaller providers and newcomers on this segment face a shortage of these type of data to develop their technology.

7.3.4.5 Other use cases

(362) Respondents report various additional ways in which they use the data collected by their consumer IoT services and smart devices, including the following:

a. First, many respondents use data to detect, prevent and respond to fraud and security risks. In particular, companies conduct analytics aiming at foreseeing fraudulent activities and security breaches.

b. Second, the majority of respondents indicate that they use data collected through their smart devices, consumer IoT services or voice assistants to provide promotions and offers through marketing communications via emails, newsletters or push notifications within the app environment. However, respondents indicate that they only send these communications when the user has given separate prior consent to receive marketing content in line with the GDPR rules.

(363) Other use cases mentioned by respondents concern the usage of data for digital advertising purposes (this is particularly the case for online content providers), for enabling online payments and for sharing data with public interest organisations, (for example wearable device manufacturers sharing anonymised metrics for public health research projects).

7.3.5 Data monetisation

(364) Respondents indicate that they do not charge third parties for making available the data they collect through smart devices and consumer IoT services. Thus, respondents have not provided the Commission with figures regarding the revenue generated by data monetisation. Looking forward, the majority of respondents indicate that they do not plan to monetise in a direct way the data they collect (that is selling data to third parties for remuneration). Some of them express concerns as to the lawfulness of such practices in the light of data protection rules and others point to privacy regulations as limitations on exploring possible data monetisation possibilities.

(365) Nevertheless, there is consensus among respondents that data brings value to their smart devices and consumer IoT services, since it allows personalisation of the user experience by making recommendations based on usage history, to improve the functionalities of current consumer IoT products and services, and to develop new ones.

(366) Although virtually all respondents explain that they do not monetise data in a direct way, many refer to two particular cases in which data collected through smart devices, voice assistants and consumer IoT services constitute a relevant input for providing services to third parties: digital advertising and user profiling. Some respondents refer to these as indirect data monetisation cases, since the data concerned is used as an input to third-party services in the form of providing interest-based digital advertisements and user profiles (as opposed to selling data directly for remuneration).

7.3.5.1 Digital advertising

(367) Some respondents indicate that they use the data they collect from their consumer IoT products and services to offer digital advertising services. This concerns in particular those companies operating in the digital advertising business that also offer leading general-purpose voice assistants such as Google and Amazon. Also, some respondents indicate that they share the consumer IoT data they collect with third parties for advertising purposes and that they monetise advertising space on consumer IoT products and services.

(368) Digital advertising is based largely on the collection of data on consumer preferences, as such data is an essential input used to attribute advertising space to advertisers. In particular, digital platforms running consumer-facing online services such as search engines, social media platforms and marketplaces have become key providers of digital advertising services to third parties.

(369) The consumer IoT sector has unlocked new advertising space possibilities. In particular, some types of smart home devices can show advertisements through displays (for example a smart fridge incorporating a display that might advertise food products). Likewise, voice assistants can serve digital audio advertisements. In this regard, given the increasingly central role of voice assistants, digital audio advertising could play a more important role in the future.

(370) Consumer IoT players receive valuable input through the operation of smart devices and consumer IoT services to identify consumer lifestyles and preferences and provide personalised digital advertising services. This is especially the case for those companies that were already present in the digital advertising business and expanded to the consumer IoT sector, such as Google. According to some respondents, the data collected from consumer IoT products and services allow these companies to attribute advertising space to third-party advertisers in a more accurate manner taking into account user preferences.

(371) In this regard, some leading general-purpose voice assistant providers seem to use the audio records of users' queries for providing such services to digital advertisers for remuneration. However, these companies consider that digital advertisement constitutes a separate business in which data is just one element, among others, in the advertisement generation process.

(372) In this respect, those leading voice assistant providers understand that their digital advertising businesses enable third-party advertisers to serve personalised advertisements by attributing advertising space (on digital platforms, on publisher's websites or on new advertising space in the user's IoT ecosystem supported by smart devices) according to data-driven attribution models and tools that target users in a personalised and efficient way. In this scheme, they argue, data is only one input, together with the advertising space and the internet-based advertising tools, that allows digital advertising service providers to serve interest-based ads.

(373) In addition, some consumer IoT service providers offering creative content services (for example music streaming, VOD, radio) indicate that they share data collected through their services with digital advertising companies for targeted advertising purposes. Some of these creative content service providers also explain that they generate revenue through (for example digital audio) advertising space displayed on their own services. Those respondents using data as an input in their digital advertising services to third-party advertisers specify that the data used for this purpose is anonymised, secured and maintained in dedicated and distinct systems.

7.3.5.2 User profiling

(374) A few respondents refer to the possibility of using data for user profiling, in order to evaluate or predict particular aspects about users. Such profiling might be of interest to third parties such as insurance companies or banking institutions.

(375) Indeed, data collected by smart home devices, wearable devices, voice assistants and consumer IoT services can be used in order to predict future user behaviour or triggering events concerning the user's environment and make projections about a user's situation or certain aspects of his or her life.

(376) The pervasiveness of smart devices and consumer IoT services in users' homes and personal lives can provide valuable input for this purpose. Data collected from various smart devices surrounding users can be used to better understand their personal situation. For example, a smart fridge can detect whether the user buys fresh food on a regular basis and a smart watch will record whether he or she exercises periodically. With this input, a company might build a user profile concerning the healthy habits of users, which could then be sold to health insurance companies to determine how much such users should pay for their insurance premium. In addition, data collected through smart home devices in a user's house might be useful to determine the appropriate premium for property insurance that such a user should pay.

(377) Some respondents indicate that they see an interesting business opportunity in monetising user profiling. However, they consider that the industry is not fully mature and there is still a long way to go before the data is generated in the necessary amounts and of a sufficient quality to develop a product that could be sold and used by third parties. Moreover, respondents indicate that privacy concerns and data protection regulations limit the development of this monetisation possibility.

7.4 KEY FINDINGS

Connectivity and communication, which are key characteristics of the consumer IoT sector, build upon the collection and flow of large amounts of data concerning consumer IoT products and services as well as their users. This includes the collection of and sharing of data with third parties within the same consumer IoT ecosystem[78].

Respondents indicate that such consumer IoT data flows typically have a very functional nature and are designed to make the system work properly for the user. Other types of data-sharing between companies cover non-aggregated data in relation to errors and aggregate performance data. Such data is usually made accessible through a central dashboard.

Even in the absence of active data sharing, some consumer IoT players have access to data in relation to a third party's activities in that consumer IoT ecosystem: these are typically the smart device operating system provider and/or the voice assistant provider, which are able to collect certain information about a user's interaction with for example a consumer IoT service by virtue of their position in a consumer IoT ecosystem. The findings of the sector inquiry indicate that, in particular, the leading voice assistant providers can impose standard terms

[78] Any processing of personal data is framed by the GDPR and the Directive on privacy and electronic communications, including access to the smart devices and the possible use and sharing of the personal data generated or stored on such devices. As already noted in paragraph 17, nothing in this report should be read or construed as an endorsement of the practices reported, nor as an assessment of their compatibility with applicable Union or national law.

and conditions that limit data access and use for third parties, while themselves having extensive data access and associated use possibilities.

In relation to data use cases within consumer IoT companies, respondents report that they use the data collected for (i) the normal functioning of consumer IoT products and services; (ii) the personalisation of the user experience; (iii) business analytics; (iv) product maintenance and development; and (v) various other use cases (for example marketing communication, safety and fraud prevention).

Respondents report that they do not make data available to third parties for remuneration. However, respondents refer to digital advertising and user profiling as current indirect data monetisation cases and future monetisation possibilities. Using consumer IoT data for digital advertising purposes may be of particular value for those leading consumer IoT players with an existing digital advertising business. The pervasiveness of smart devices and consumer IoT services in users' homes and personal lives can increase the value of consumer IoT data for user profiling purposes, but respondents indicate that this business opportunity is not very developed yet and would need to comply with data protection rules.

8 CONCERNS RAISED DURING THE SECTOR INQUIRY

8.1 OVERVIEW

(378) The present chapter sets out concerns raised by the respondents about practices that could potentially have a negative impact on competition, innovation and consumer choice in the consumer IoT sector in the EU. These concerns relate to:

a. interoperability (Section 8.2),

b. standardisation (Section 8.3),

c. data (Section 8.4),

d. pre-installation, default settings and prominence (Section 8.5),

e. exclusivity, concurrency and tying (Section 8.6)

f. disintermediation (Section 8.7), and

g. contractual issues (Section 8.8).

(379) Section 8.9 outlines the main conclusions of this chapter.

8.2 INTEROPERABILITY CONCERNS

(380) In relation to interoperability, respondents raise concerns in relation to two main issues: (i) obstacles regarding access and integration of their products with consumer IoT technology platforms and (ii) the limitation of functionalities for third-party products and services on such technology platforms as compared to the performance of first-party products and services.

8.2.1 Obstacles concerning access and integration of products on consumer IoT technology platforms

8.2.1.1 Certification processes governed by consumer IoT technology platform providers

(381) As explained under Section 5.2, leading consumer IoT technology platforms (i.e. Google, Amazon and Apple) control and determine access to relevant voice assistants and smart device operating systems. Those providers impose specific contractual and technical requirements on smart device manufacturers and consumer IoT service providers, through certification processes governing the integration of devices and services on their technology platforms.

(382) From a technical perspective, a common feature for these integration processes is that the smart device manufacturers and service providers need to customise their products and services according to the APIs, SDKs and hardware technical specifications released by the voice assistant or operating system provider.

(383) From a contractual point of view, participation in these certification processes involves the acceptance of non-negotiable standard terms and conditions imposed by the technology platform providers. Respondents indicate that a refusal to accept these standardised agreements is generally not an option, since the majority of manufacturers and service providers lack bargaining power to negotiate contractual and technical requirements with the leading technology platform providers.

(384) Generally, certification also requires creation of developers' accounts and/or agreeing to license and development agreements. Some certification processes also require payment.

(385) Some comments received in the context of the public consultation on the preliminary report indicate that these mandatory terms and certification processes ensure the quality of apps, security within IoT ecosystems, and consumers´ trust. The Commission acknowledges the benefits of standardised terms and certification processes, especially in the case of platforms that attract a large number of developers. Nevertheless, the findings of this sector inquiry show that such terms and conditions as well as certification processes imposed by some consumer IoT technology platform owners may be disproportionate towards smaller players. For instance, the concern was raised in the public consultation on the preliminary report that some consumer IoT technology platform providers require access to smart home devices' data for their own usage, restrict access to real-time data to service providers as part of their interoperability certification programs and/or limit the functionalities of third-party products through technical constraints. Many respondents to this sector inquiry and stakeholders participating in the public consultation on the preliminary report consider such requirements as unfair.

8.2.1.2 Diversity of technical requirements for integration with consumer IoT technology platforms

(386) As explained in Chapter 5, technology platform providers develop and make available APIs, SDKs and hardware specifications to third parties for developing technical integration, subject to compliance with the specific guidelines imposed by each provider and to gaining approval through the appropriate certification process.

(387) Due to the lack of widely adopted common standards or unified technical solutions for integration with voice assistants and smart device operating systems, smart device manufacturers and consumer IoT service providers are required to customise their products and services to make them compatible with each different consumer IoT technology platform into which they wish to integrate. Respondents indicate that this is costly and time-consuming given the heterogeneity between APIs available for each proprietary technology platform[79]. Respondents also indicate that they need to follow parallel certification processes, involving different steps and timelines, and adapt their integrations following updates by the technology platform.

(388) As indicated by one consumer IoT service provider in relation to smart device operating systems, "*each smart device manufacturer has their own proprietary technology for integration and therefore we have to work with them to customize our integration for each one*". In the same vein, a smart device manufacturer respondent explains with respect to voice assistants that "*interoperability with the different voice assistants need a specific development in order to be compatible one by one to each proprietary description (one for Google Assistant, one for Alexa…)"*. Some respondents indicate, in this regard, that their devices and/or services need to be accessible at least via Google Assistant and Alexa, given that their user base interacts with both.

(389) Respondents explain that they must dedicate resources and specialised technical teams to work on the implementation and maintenance of such integrations. The costs of hardware resources needed for API integration (that is memory size, low power optimisation, CPU chipsets, microphones, encryption materials, and connectors) further increases the burden placed on manufacturers. Hardware requirements may even require changes to products during the development or production process.

(390) In the case of technical integration with smart device operating systems, respondents explain that there are multiple operating system versions and each device has its own set of release cycles (with different timelines and software updates – see Section 8.7.3.) and requirements with which interoperability has to be maintained. In addition, the

[79] One stakeholder indicates, in the context of the public consultation on the preliminary report, that APIs allowing interoperability are necessarily heterogeneous (i.e. technically different), since "homogeneous" APIs are neither practical nor technically feasible. However, the Commission uses "heterogeneity" to refer to the lack of standardised APIs that leads to a significant diversity of technical solutions in the consumer IoT sector, that are not compatible with one another.

requirements for interoperability can also change over time, affecting the ongoing development and updating of products.

(391) Specifically in relation to applications, some respondents indicate that the app store review process is complicated; that there is limited feedback available in case of technical issues; and that the appeal process in case of disagreements is slow and non-transparent.

(392) Respondents also indicate that they generally lack technical support and guidance from the leading providers of consumer IoT technology platforms in the integration process. Some explain that they even need to resort to software development agencies to outsource application development and the conduct of certification processes. Other respondents indicate that platform providers impose intermediary "integration partners" for developing interoperability and do not allow respondents to do the integration themselves, which increases their costs.

(393) Ultimately, the majority of respondents submit that this situation increases the costs and complexity of interoperability, since they cannot develop software solutions or applications exploiting multiple technology platforms. This scarce reusability of technical solutions not only hinders interoperability but also slows down the introduction of new consumer IoT products and services.

8.2.1.3 Divergent user experiences across consumer IoT technology platforms

(394) Smart device manufacturers and consumer IoT service providers explain that due to the disparity of requirements of providers of consumer IoT technology platforms when approving or certifying integrations, they need to adapt the features of their products and services to many different technical environments. There is a significant diversity among the APIs and functionalities available for each voice assistant and smart device operating system, which leads to a divergence of user experiences across consumer IoT technology platforms.

(395) Indeed, many respondents report that the customisation requirements and functionality limitations imposed by each provider make it impossible to offer the same functionalities to the user across various consumer IoT technology platforms.

(396) Comments from various respondents capture this consideration: *"technological fragmentation of these platforms in the market makes it practically impossible to offer one´s own services equally to the entire retail market*"; "*heterogeneity exists in between APIs available among the different OS which leads to complexity to provide a homogeneous and coherent user experience*"; "*each IoT device comes with its limitations and functionalities. The hardest part is to find the best possible user experience for the customer while acknowledging the limitations of the device itself. The development efforts can vary from project to project and from device to device*".

(397) These constraints could prevent providers of consumer IoT products and services from offering a consistent and homogeneous user experience across different consumer IoT

technology platforms, which reportedly leads to consumer frustration when the user cannot access specific features of certain consumer IoT services or smart devices on a particular technology platform.

8.2.2 Limited functionalities on consumer IoT technology platforms for third-party products and services

(398) Many respondents indicate that the good performance of their consumer IoT products and services on relevant voice assistants and smart device operating systems is essential for competing in the consumer IoT sector.

(399) However, as explained in Chapter 5, the leading consumer IoT technology platforms are generally vertically integrated companies (Google, Amazon, Apple) that also offer first-party smart devices and consumer IoT services in competition with third parties present on their technology platforms. These leading consumer IoT players may therefore have incentives to restrict the operability of third-party products and services by limiting their access to the full functionalities of their technology platforms, thus influencing the functionalities and user experience they are able to provide. One respondent summarises this concern as follows: *"competition threats arise from the fact that access to such interfaces can be hindered or limited discriminating negatively those companies that compete with voice assistant providers in other markets. For example, a company that manages Voice Assistants or other Interfaces can refrain others from full access to all its features or from customization possibilities, which would reduce competition possibilities*".

(400) From a technical perspective, respondents explain that providers of consumer IoT technology platforms permit fewer capabilities and features for third-party smart devices and consumer IoT services (compared with their first-party products and services) by exposing fewer functionalities through the APIs available for third parties. Meanwhile, technology platform providers have unrestricted access to their own APIs, which makes interoperability with their first-party products more reliable and enables a richer user experience and smoother functioning. Although certain restrictions at the API level might be justified by security aspects, the Commission notes that the majority of respondents believe that many interoperability limitations are unjustified or could at least be significantly reduced without affecting security. In addition, the set-up processes and on-boarding experiences of first-party products and services are generally more straightforward than for third parties.

(401) With respect to voice assistants in particular, third parties may have limited access to the voice assistant's APIs, reducing the richness of voice-control functionalities for their products and services as compared to the first-party offer.

(402) Similarly, some wearable device manufacturers submit that providers of smart mobile device operating systems provide limited access to APIs for the companion apps on which their wearable devices rely. At the same time, smart mobile device operating system providers themselves have unrestricted access to APIs with respect to the

companion apps for the wearable devices that they offer in competition with third parties.

(403) One stakeholder argues, in its submission to the public consultation on the preliminary report that preferential access to the consumer IoT technology platform for the technology platform's own services tends to be a temporary phenomenon and should be expected to cease at a certain point, since consumer IoT technology platforms are more attractive to consumers when they host third parties. However, overall, respondents indicate in their replies that it is generally not possible to provide richer functionality and user experiences through third-party consumer IoT technology platforms than that provided by the first-party products offered by these technology platform providers themselves. This makes it difficult to compete directly with many of the consumer IoT services and smart devices provided by leading providers of consumer IoT technology platforms.

(404) These limitations risk disincentivising innovative efforts by smart device manufactures and consumer IoT service providers, which might not be able to offer innovative products or ground-breaking functionalities through third-party consumer IoT technology platforms. This could ultimately limit intra-platform competition within the consumer IoT sector and impede product and service differentiation.

8.3 STANDARDISATION RELATED CONCERNS

(405) Respondents to the questionnaires identify a number of concerns in relation to standardisation. These relate in particular to the standardisation process, to SDOs' rules on membership and participation, SEP declarations, IPR policies and licensing terms[80]. While these respondents consider that such elements may have an impact on the evolution of standardisation, they are not specific to the segments covered by the sector inquiry, and may thus impact standard-setting more broadly.

8.3.1 The high number of standardisation bodies and competing standards

(406) The high number of SDOs and private partnerships/industry organisations active in the segments covered by the sector inquiry is identified by many respondents as potentially problematic for the future evolution of these segments, as it may (i) become a barrier to reaching a broader user base, and so result in the wide acceptance of a more limited number of technologies; and (ii) generate a lack of transparency in terms of the organisations and alliances relevant for hardware manufacturers and software developers, in particular for SMEs and new entrants.

(407) Respondents also highlight the existence of various standards for largely identical technological results. These partially and fully overlapping standards are reported to

[80] Similar, and other related concerns have been identified by a Group of Experts on Licensing and Valuation of Standard Essential Patents ('SEP Expert Group', E03600) that published its findings and proposals on 10 February 2021.

generate a lack of transparency in the standards and protocols relevant for hardware manufacturers and software developers, in particular for SMEs and new entrants.

(408) In addition, the lack of clarity in terms of the potential open source, royalty-free or royalty-bearing IPR embedded in a standard or specification is reported to further add to the lack of transparency in terms of the IPR related obligations for new devices and applications.

(409) Various respondents put forward the need to consolidate the existing standards. However, the highly complex standardisation landscape in the consumer IoT sector generates a barrier to such consolidation, as it hampers the ability of a smaller number of standards to reach a broader user base and thus a wide acceptance.

(410) Certain respondents consider that the complex standardisation landscape, combined with a similarly fragmented landscape of proprietary technologies, negatively effects the growth potential of consumer IoT segments, where a seamless consumer experience in navigation through the various smart devices and applications is crucial. Such easy integration of, and smooth communication between, devices and applications is being hampered by the above fragmented landscape, thereby endangering consumer trust.

(411) Many respondents, throughout the different questionnaires, single out the Matter Project as a promising attempt to consolidate existing technologies, in view of the co-leadership by Google, Amazon, Apple and Samsung, the open source implementation, and the resulting potential of the future standard to reach a broad user-base.

(412) In addition, Amazon's VII is also seen as having the potential to bring together a broad user-base and grow into a leading proprietary technology (de facto standard), as a result of the interest of many industry players and consumers to allow for a swift interaction with more than one voice assistant on the same device.

(413) The high number of SDOs and standards is at the same time put forward in a few submissions to the public consultation on the preliminary report as a sign of healthy competition between standardisation efforts, which may also contribute to the development of better and more successful standardised solutions.

8.3.2 The cost of standardisation – the leadership of large technology companies in standardisation

(414) Several respondents put forward the argument that membership fees in the relevant SDOs and independent alliances are very high and even prohibitive for smaller players, which makes it more difficult to enter the consumer IoT sector, where reliance on widely adopted technologies is crucial. Large technology companies are reported to be much better placed to sustain active memberships in most of the relevant organisations.

(415) The cost of SEP licensing for all relevant standards, as well as the costs of other specifications (for non-members), is also seen by various respondents as a potential barrier to entry by smaller entities. Implementers of standards face substantial

transaction costs when they need to deal simultaneously with numerous SEP owners. For some standards, there are hundreds of patent owners to deal with. Entering into licensing negotiations with all these owners requires considerable resources and time that smaller structures may not be able to afford.

(416) Overall, respondents express the view that, whether via standardisation or independent alliances, major technology companies mostly take the lead and impose their own technology solutions. This, in turn, hampers the general willingness of other, smaller, companies to invest in collaborative innovation, and may enable major technology companies to leverage their market power as patent owners into downstream markets.

8.3.3 Differences between the rules of SDOs relating to membership and participation / lack of transparency regarding relevant SEPs

(417) Various respondents, including a number of SDOs, identify the differences between the IPR policies of SDOs and the lack of transparency of IPR obligations relating to the implementation of a given technology as a barrier to a faster and broader development of standards in the consumer IoT sector.

(418) Some SDOs' SEP declarations do not provide any information with regard to specific SEPs. Other SDOs, such as ETSI, require more detailed declarations, but these are also not regularly updated to reflect changes to the SEPs (such as invalidations, changes to the patent, expiry). In practice, the difficulties in identifying the actual licensing obligations and costs relating to the implementation of a given technology in a new smart device or application reportedly increase the barriers for new entry.

(419) SDOs and other respondents also point to tensions between SDOs/major independent alliances, potential contributors and/or licensees. These tensions exist as a result of: (i) the exclusion by some SDOs/major independent alliances of contributions where the contributor would not commit to royalty-free licensing; and (ii) the requirement of FRAND commitment for the developed standard, where the actual terms of such commitment are subject to diverging interpretations (see Section 8.3.4 below).

(420) In particular, the Connectivity Standards Alliance (especially in view of the Matter Project) is identified by several respondents for its IPR policy that also applies to SEPs for standards that relate to the Connectivity Standards Alliance specifications, including standards and SEPs for which IPR policies of other SDOs and independent alliances would apply, thereby de facto overwriting those IPR policies of related SEPs.

(421) In addition, IP enforcement of SEPs by Non-Practicing Entities[81] is another factor identified by respondents that may negatively affect stakeholders' willingness to rely on standardised technologies.

[81] Non-Practicing Entities are companies that hold and manage patents or patent portfolios for the purposes of collecting patent fees, but without the intention of using the inventions those patents protect. Patent litigations by Non-Practicing Entities, including litigation over SEPs, may represent a threat to practicing businesses.

(422) According to a number of respondents, the above factors could limit the full potential of standardisation in consumer IoT sector.

8.3.4 Diverging views in relation to FRAND licensing

(423) Various respondents to the sector inquiry and the public consultation on the preliminary report, including large associations of companies active in consumer IoT and related standardisation, also express concerns resulting from the diverging interpretations of FRAND licensing terms, in particular with respect to the royalty base or the level in the value chain at which the royalties would be due, and the valuation of SEPs and SEP portfolios. These potentially significant differences of interpretation and related litigation risks reportedly have a chilling effect on future standardisation.

8.3.5 Growing proprietary ecosystems vs standardisation

(424) Many respondents emphasise the importance of further standardisation in the consumer IoT sector. As one respondent active in the smart home sector put it, "*the lack of a standard communication protocol between different appliances directly influences the choices of the final customer: if many different devices are compatible between them, the user would be more willing to integrate new products under various brands in their own home systems*".

(425) In the same vein, respondents also report that there is currently no industry-wide standard on data format, for the collection and sharing of data between companies active in consumer IoT sector. According to some respondents, effective data sharing would require the adoption not only of standardised data formats, but also of a system with unified and common user, device and possibly content identifiers, to "pseudonymise" such data. Because of the current lack of standards in relation to data formats, respondents fear that owners of the most widely used proprietary technologies would end up imposing their data formats to the industry. In addition, further concerns are reported in relation to seamless data-flows between devices and applications of various stakeholders, as a result of the lack of standard naming or referencing of similar types of data by the different stakeholders.

(426) More generally, SDOs reportedly often lag behind proprietary technical development by major consumer IoT technology platforms, which may lock users into proprietary ecosystems. Many respondents claim that such lock-in may lead to a perpetuation of a fragmented technology landscape that largely relies on proprietary solutions by the parallel ecosystems, thus increasing the barriers to inter-system communication. In addition, many respondents put forward that such a perpetuation of parallel ecosystems would allow large ecosystems a significant margin of control over the level and quality of inter-system interoperability.

(427) Apple expresses the view that it is nonetheless important to distinguish between enforcing commitments to license SEPs on FRAND terms that were voluntarily given by participants in collaborative standard-setting, and forcing owners of a proprietary

technology to license their IP. While owners of proprietary technology may find it in their interest to license their IP and enable interoperability to make their products or services more attractive, a mandatory licensing to enable "full interoperability" may risk stifling innovation.

(428) SDOs on the other hand argue that they typically need more time and a more advanced level of technological framework in the specific industries to identify and understand the exact use cases that can be best addressed by standards. Standards may thus develop and replace previous proprietary technologies at a later stage in the technical progress of the different consumer IoT applications.

(429) As a limit to standardisation, various respondents however make the point that large platforms have a higher incentive to capture users for their proprietary ecosystem rather than to promote standardised technologies. They would have a more limited interest in investing in standardised technologies, thereby not only limiting the future evolution of standardisation, but also leaving a number of already existing standards poorly deployed and, in view of their limited user-base, not "giving them a chance" to grow into broadly deployed standardised technologies.

8.4 DATA RELATED CONCERNS

(430) A concern frequently raised by respondents to the sector inquiry, and in submissions to the public consultation on the preliminary report, relates to do with the accumulation of data by voice assistant providers[82].

(431) More specifically, smart device manufacturers and consumer IoT service providers express concerns about the voice assistant providers' access to certain types of data. Typically, voice assistant providers are the only ones to have full access to users' voice queries. Moreover, and linked to the search and recommendation functions of the voice assistant, voice assistant providers also typically need detailed knowledge of the consumer IoT services they make accessible, such as catalogue data. Finally, a voice assistant provider generally has access to this type of data for several consumer IoT service providers, with the ability to gather data across services.

(432) One particular concern raised in relation to this is that voice assistant providers may be able to use the data that they collect on the use of third-party consumer IoT products and services to develop or improve their own competing offers in those segments.

(433) As one respondent explains, *"access to relevant data is key to sustain the design and development of new (…) devices or solutions. Being able to access to customer behaviour data and operational data from the market itself and related markets from different products and brands constitutes a huge competitive advantage. The advantage*

[82] In relation to personal data processing through voice assistants, the European Data Protection Board published Guidelines on virtual voice assistants in July 2021, which are retrievable via https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022021-virtual-voice-assistants_en

in this regard offered to companies in a gateway function (…) such as Voice Assistants is enormous. It is clear that these companies have a paramount competitive advantage over, not only new entrants, but over the rest of the players in the sector that will not be able to access to such sources of information in a similar way".

(434) In their contractual agreements with third parties, the leading consumer IoT technology platforms often seem to reserve for themselves very broad rights in relation to data collected from other consumer IoT segments, which according to some clauses, can be used and monetised by any department of the company.

(435) According to some replies, this competitive advantage is amplified by the fact that third-party manufacturers and service providers often only obtain anonymous usage data from the leading voice assistant providers, which in some respondents' view, in turn, hinders them in their future business development.

(436) In addition to this concern, a few respondents raise privacy and/or security concerns in relation to the extent to which the data that they collect is accessible to third parties. More specifically, a few smart home device manufacturers mention these concerns in relation to the continuous sharing of device status data with voice assistant providers. One respondent quotes the imposition of this requirement as a contributing factor leading to the company's abandonment of its full integration with some of the leading voice assistant providers. In terms of data sharing, privacy considerations are important to take into account as a means of maintaining consumer trust, confidentiality, access to and integrity of data. However, privacy protection claims may also be used by market players to justify "locking up" certain data for themselves.

(437) Another data-related concern is linked to data monetisation. Even if the majority of respondents consider that sharing and using data for digital advertising purposes does not constitute a direct way to monetise data, they do consider that data collected through smart devices, consumer IoT services and voice assistants is a valuable input for providing digital advertising services to third parties. Allegedly, this benefits in particular the few companies that were already present in the digital advertising business and expanded to the consumer IoT sector, thereby raising the already high barriers to entry into the digital advertising market.

(438) Moreover, some smaller IoT players consider that leading providers of consumer IoT technology platforms are able to use their digital advertising business to monetise the data they collect from users through various consumer IoT products and services. In their view, these bigger firms draw economic benefits from advertising, allowing them to subsidise their consumer IoT products and services, thus expanding their presence in all consumer IoT segments. According to some respondents, these strategies put smaller players at a disadvantage and raise barriers to entry.

(439) In their comments to the public consultation on the preliminary report, a few content service providers have pointed to the risk that voice assistant providers insert sponsorship or advertising around third-party content without the consumer IoT service

provider´s consent. Voice assistant providers' position as intermediaries and related competition concerns are discussed further in Section 8.7.

8.5 CONCERNS IN RELATION TO PRE-INSTALLATION, DEFAULT-SETTINGS AND PROMINENCE

(440) Respondents raise a number of potential competition concerns in relation to the out-of-the-box features that are available to users. The issues raised relate predominantly to consumer IoT services and their integration on smart devices and/or voice assistants. Respondents indicate that pre-installation, default-setting and prominence practices impact the discoverability of consumer IoT services to the extent that it becomes a competitive (dis-)advantage. The large creative content service providers, active on a global scale, are said to particularly benefit from this situation. However, other respondents do not seem very concerned by these practices, often because they perceive the importance of consumer IoT - including voice assistants in particular - for their business to still be relatively limited.

(441) Comments submitted in the context of the public consultation on the preliminary report confirm diverging views on these practices, with a number of submissions repeating the concerns that certain (voice assistant) providers may use default settings, pre-installation or prominence to promote their own services or the services of selected third parties. Other submissions emphasise the potential benefits that such practices – dependent on the circumstances – may have, referring to their "standard and legitimate" nature, noting more generally the usefulness of recommendation systems to the user and/or emphasising the options available to the user to override these settings.

8.5.1 Pre-installation and default settings for voice assistants

(442) Smart device manufacturers that also offer a voice assistant typically build that first-party voice assistant into their smart devices. Although a few manufacturers build in a third-party general-purpose voice assistant on some of their devices in addition to their own voice assistant, the first-party voice assistant is reportedly always set as the default.

(443) Likewise, only a few third-party smart devices offer several voice assistants built into their device, allowing the user to choose which voice assistant is the default.

8.5.2 Pre-installation and default-setting of consumer IoT services

(444) The voice assistant, and/or the operating system on which it runs, often come with a number of proprietary applications integrated or "pre-installed". For example, Amazon positions its consumer IoT services relating to e-books and shopping as a feature of Alexa.

(445) The pre-installation of consumer IoT service applications also occurs quite frequently on third-party smart devices. Some types of devices lend themselves more to this practice, namely, smart TVs, streaming players and wearable devices, but other examples have occasionally been mentioned as well. A few respondents describe

specific promotional actions that involve their consumer IoT service's application being pre-installed on a device for a limited amount of time. The pre-installation of a service's application on a smart device is usually reflected in contractual agreements.

(446) The technical form of the pre-installation practices may differ. For example, in the case of smart TVs, some respondents distinguish between the presence on the device of *pre-loaded* applications and *pre-downloaded* applications. Whereas the latter are fully downloaded or installed on the smart device, using a pre-loaded application requires user action, i.e. downloading.

(447) Not all consumer IoT service providers have the opportunity for their applications to be pre-installed on a smart device and/or voice assistant. Very often, voice applications have to be added by the user manually. A few respondents indicate that the decision to pre-install an application lies solely in the hands of the relevant smart device manufacturer. A few others explain that pre-installation comes at a price (that is a flat fee or and/or revenue sharing), which at least some consider to be too high.

(448) Consumers expect certain devices to come with certain functionalities pre-installed. Moreover, pre-installation of a consumer IoT service does not necessarily mean that the service is the default accessed by the smart device or voice assistant, nor that it is the only one available "out of the box". In fact, several respondents have provided examples of multiple applications being pre-installed on a smart device. Pre-installation may also provide nascent or lesser-known competitors with an opportunity to reach new audiences.

(449) Nevertheless, a few respondents explain that pre-installation constitutes a competitive disadvantage for consumer IoT service providers whose applications are not pre-installed, as a user has to take additional steps to access a service that is not included in the "out of the box" offer. In contrast, pre-installed services profit from higher levels of user discoverability.

(450) Most smart devices - especially when accessed via a voice assistant - are inherently limited in the number of options they can present to the user. That explains in part why many respondents single out default settings as an important competitive (dis-) advantage. Indeed, whereas several pre-installed applications on the same device/voice assistant may benefit from an equal level of visibility, this is different in the case of a default position, which provides an advantage to a single player.

(451) Default-setting practices of consumer IoT services on smart devices are widespread. For example, Apple, Amazon and Google seem, generally, to set their own music services as default on their smart speakers. Only a few respondents provide examples of smart devices directing the user to a third-party default service provider when a user performs a certain action. This may also be temporary, in the context of a promotional offer, and/or only on specific (co-branded) devices.

(452) Typically, however, default settings seem to be managed via the provider of the user interface (such as voice assistants). For smart devices that cannot be accessed via voice commands, this is often the mobile device application. When voice activation is possible, the voice assistant provider will determine the default settings in relation to specific user actions. This may be dependent on the user's registration of an account with those providers.

(453) In general terms, the leading voice assistant providers direct the user to their own consumer IoT services if they offer one in the relevant service category (for example music, podcasts, books, audiovisual content, shopping).

(454) In the absence of a proprietary service of their own, these voice assistant providers may agree to direct the user to a third-party consumer IoT service for that category of user request. This sometimes happens for a limited period, for example in the context of a marketing campaign or may occur on a more structural basis. From the replies of consumer IoT service providers, it seems that such arrangements have been made, particularly for information or creative content services. Default settings do not always seem to be reflected in written arrangements.

(455) The reasons for selecting one third-party consumer IoT service provider over another are not always clear. One respondent indicates that in their case it was based on a competitive selection process, whereas another explains it had been contacted by the voice assistant provider, but did not know based on which criteria its services had been chosen. A few other service providers point out the quality of their service as a determining factor, while others explain that other considerations may play a role, for example the content popularity in the user's location, past user preferences, or the exclusive availability of certain content.

(456) Some of the responses to the questionnaires and submissions to the public consultation on the preliminary report emphasise that, despite default settings, users continue to have the choice to switch to an alternative service using, for example, voice commands or a mobile device application. In this context, users may have various levels of opportunities to override the default settings established for their smart device and/or voice assistant, for example during set-up and/or in the device settings.

(457) In any case, some respondents emphasise that accessing a non-default consumer IoT service involves at least some effort from the user: this is the case for example if the user wants to select a different default service during the set-up process, but also more generally, for example through required additional account association/authentication steps. As a whole, the user experience for non-default services is said to be considerably worse than for the default service.

(458) It is also alleged that defaults are 'stickier', meaning that they result in users staying with the default service for longer.

(459) Moreover, many respondents explain that, to access a non-default consumer IoT service provider via a voice assistant, a user will typically have to add a specific invocation name to their voice commands (for example "listen to song x on service y"):

"We have learned that voice command users use very generic commands and seldom include brands in their commands. In our case, 'generic' searches for music channels are directed to the 'preferential' […] app. Only when consumers ask very specific questions for our services, they get directed to us, making 'discoverability' of our services very hard."

(460) Some consumer IoT service providers report that the invocation of third-party voice applications is generally poorer than the invocation of first-party and/or default voice applications and functionalities.

(461) As a result, default-setting practices are said to generate extra traffic for the default service(s) in question and make multi-homing, that is switching between different consumer IoT service providers, more difficult.

(462) Moreover, a few respondents link default-setting practices to competitive disadvantages in terms of data access (see also Section 8.4), as the non-default service provider does not know the user as well as the default service provider, making it difficult to offer an equally attractive user experience.

(463) For those consumer IoT service providers that are part of an aggregated (bundled) offer, as is mostly the case for creative content services, the default position of that aggregated offer may be an advantage, while at the same time reinforcing certain alleged disadvantages - linked to the relinquishment of control vis-à-vis the aggregator (for example over the user relationship and advertising) - that seem to be a consequence of entering into this type of partnership.

8.5.3 Prominence of consumer IoT services and voice assistants

(464) Some respondents indicate prominence arrangements as among the most often negotiated clauses in applicable agreements and sometimes the most difficult ones to find an agreement on.

(465) These prominence arrangements are singled out by respondents as important factors that determine the visibility and findability of a service. While most of the remarks made by the respondents in this respect relate to audiovisual services and, to a lesser extent, to music/radio content, other consumer IoT services as well as voice assistants may also be concerned by such settings.

(466) Firstly, these may include parity settings in relation to advertising of the smart devices concerned: some consumer IoT service and voice assistant providers request that manufacturers of smart devices advertise the availability of their service or voice assistant on the device(s) by, for example, including their logo, comparably or at least as

favourably as compared to other competing services or voice assistants available on the smart device.

(467) Secondly, once a user has purchased a smart device, the latter may display some of its accessible consumer IoT services or features in a more prominent way, using various practices, for example in the context of smart TVs:

a. Typically, in the context of the pre-installation of applications, consumer IoT service providers may negotiate with smart device manufacturers how their service is presented. For example, the presence of an audiovisual service can be presented more or less prominently in app galleries or other types of content menus on smart TVs. In this sense, according to one respondent, international players typically have stronger bargaining power, as they can negotiate multi-national agreements. This would mean that local content service providers usually compete for less attractive positions. One smart device manufacturer emphasises that users can nevertheless override the order of consumer IoT services in the smart television's menu.

b. Prominence arrangements play a role when it comes to displaying search results. The order of these search results may be determined, unilaterally or based on agreements, on the basis of various factors in relation to for example the user profile, the service characteristics and/or usage history. A respondent has suggested that leading providers of consumer IoT technology platforms may be able to exploit applicable algorithms to their own advantage, for example by associating specific search terms to their first-party content so that it appears higher up in the ranking.

c. Additional prominence can be achieved for certain consumer IoT services via on-device marketing, for example via featured reels on smart TVs.

(468) Finally, in addition to the above types of prominence practices in relation to the positioning of content and/or applications of consumer IoT services, the replies also identify a prominence practice that builds upon hardware features. Indeed, certain consumer IoT services and voice assistants may be given enhanced visual prominence or placement on smart devices or their user interfaces, such as dedicated remote buttons on connected video entertainment devices that provide direct access to certain consumer IoT services or voice assistants. As they are hardware-based, they typically cannot be reconfigured by users.

(469) Prominence-related provisions are typically part of contractual agreements. Respondents indicate that some of these agreements involve direct monetary payments or other revenue-sharing arrangements.

8.6 EXCLUSIVITY, TYING AND CONCURRENCY CONCERNS

8.6.1 Exclusivity requirements

(470) As mentioned in Chapter 2, the findings of the sector inquiry reveal that most smart devices have a single voice assistant built-in, and that this is true both for voice assistant providers' own smart devices and for third-party devices. Some manufacturers of smart devices seem content with offering users devices with only one built-in voice assistant. Others explain that they would prefer that their devices could carry more than one general-purpose voice assistant, and that there is customer demand for such dual assistant devices. In addition, they would like to be able to compete on equal terms with the handful of manufacturers of smart devices that have been able to negotiate deals to have two general-purpose voice assistants built-in on their devices.

(471) The results of the sector inquiry indicate that attempts to secure exclusivity of voice assistant presence on smart devices could potentially raise competition concerns if they prevent other competing voice assistants from being built-in simultaneously on the devices. In order to meet user demand for smart devices with the leading voice assistants built-in, some device manufacturers have chosen to develop separate product lines, each supporting a different voice assistant.

8.6.2 Concurrent use of voice assistants

(472) As explained in Chapter 2, concurrent use of voice assistants, namely switching between voice assistants by using a specific activation word to activate one of the voice assistants, is possible only on a limited number of smart devices manufactured by the respondents. Certain concerns about the inability to allow for concurrent use of voice assistants on smart devices were raised during the sector inquiry[83].

8.6.3 Tying

(473) Smart device manufacturers raise concerns about voice assistant providers bundling different types of software, technology and applications, including voice assistants.

8.7 DISINTERMEDIATION

(474) As explained in Chapter 5, the majority of respondents offer their consumer IoT services and enable control of their smart devices through third-party general-purpose

[83] Similar concerns have also been raised in the US. See, for example, Written Testimony of Patrick Spence, Chief Executive Officer of Sonos, to the U.S. House Judiciary Committee, Antitrust, Commercial and Administrative Law Subcommittee, 17 January 2020, retrievable from https://docs.house.gov/meetings/JU/JU05/20200117/110386/HHRG-116-JU05-Wstate-SpenceP-20200117.pdf ; United States of America U.S. Department of Justice v Google LLC, Case 1:20-cv-03010, Filed 20 October 2020, points 141 and 163-164.

voice assistants and/or smart device operating systems, provided by a few leading providers of consumer IoT technology platforms.

(475) Consequently, some respondents indicate that they depend largely on these leading providers of voice assistants and smart device operating systems when featuring as intermediaries between the smart device manufacturer or consumer IoT service provider and the user. Respondents to the sector inquiry raise the following concerns with respect to intermediation.

8.7.1 Controlling the user relationship and user experience

(476) Overall, some respondents express fear of losing their brand recognition and their direct relationship with the user, since the voice assistant and smart device operating system providers usually have the most direct relationship with users. For instance, a few respondents express concerns that the increasing use of general-purpose voice assistants to control smart home devices might lead to the loss of brand visibility, since users activate consumer IoT services and smart device functionalities using the voice assistant's activation word, sometimes even without referring to the brand of the appliance that executes the voice command. In practice, this reportedly reduces visibility of smart device manufacturers' brands while enhancing users' perception of voice assistants as the centre of the smart home.

(477) Several submissions to the public consultation on the preliminary report by consumer IoT service providers, in particular radio broadcasters, put forward similar concerns regarding voice assistants controlling the user's experience, resulting in the loss of brand attribution or recognition, as well as the direct relationship with the user.

(478) Furthermore, many respondents indicate that some of the leading providers of consumer IoT technology platforms impose their own set-up and user on-boarding processes on third parties, for when users connect smart devices or access consumer IoT services through their voice assistants and smart device operating systems for the first time.

(479) Concerning the set-up process, some respondents explain that in order to make their consumer IoT products and services interoperable with, and accessible via, third-party voice assistants, users are forced to set up their smart devices through the voice assistant provider's application. Furthermore, according to some replies, it is common practice to require that the user have an account or ID supplied by the voice assistant provider to authenticate and access third-party consumer IoT services and smart devices.

(480) As a result, smart device manufacturers and consumer IoT service providers are reportedly prevented from controlling the user's on-boarding experience, that is, the user experience from the moment when the user accesses their products for the first time, if this is done through a third-party user interface or smart device operating system. This could prevent smart device manufacturers and consumer IoT service providers from collecting relevant data from users, such as contact details and personal information, which might be valuable to ensure proper after sales communication and to

require consent from users to send relevant marketing content and offers. Additionally, smart device manufacturers and consumer IoT service providers report that they sometimes face authentication issues that they cannot solve without the intervention of the platform provider (since the ID used to access the service or device functionality is provided by a third party). In contrast, the leading providers of consumer IoT technology platforms fully control the experience relating to their first-party products from the very beginning of the user interaction, collect relevant user data and in most cases do not depend on a third party to solve technical accessibility issues.

8.7.2 Controlling the access to consumer IoT services and related data

(481) Some respondents, and in particular consumer IoT service providers, explain that the visibility of their services on smart devices and voice assistants depends to a great extent on discoverability rules set up by providers of consumer IoT technology platforms, as already discussed in Section 8.5. In this regard, many consumer IoT service providers indicate that the discoverability of voice applications is controlled by the leading general-purpose voice assistant providers, who do not disclose such rules to third parties. One creative content service provider explains that *"Integrated service providers have the short-term advantage of being easily retrievable via the integration on the voice assistant. However, in the long run, such integration makes these services dependent from the intermediation power of the voice assistant. Also, this intermediation happens with no algorithmic transparency, eventually forcing service providers to pay if they want their content to be visible to consumers."*

(482) Moreover, many consumer IoT service providers seem to be unable to negotiate discoverability conditions with providers of consumer IoT technology platforms, which only make exceptions to their general contractual terms and conditions for large counterparties with significant leverage to negotiate. Some stakeholders fear that voice assistant providers would – going forward - agree to carry only those consumer IoT services in exchange for payment, thus affecting the profitability of consumer IoT service providers.

(483) Furthermore, some responses to the questionnaires and submissions to the public consultation on the preliminary report claim that, due to the intermediation of the leading providers of consumer IoT technology platforms, they do not have consistent and immediate access to relevant data on the use of their services and smart devices on third-party voice assistants and smart device operating systems (see also Section 8.4). As indicated by one respondent, voice assistant providers "*have full consumer data access while third-party developers need to deal with a really complicated setup procedure before the user can give us their data e.g. their location to receive more relevant information*". This lack of automatic data gathering prevents third-party consumer IoT service providers from customising the user experience in real time and reportedly puts them at a competitive disadvantage with respect to the first-party services offered by leading general-purpose voice assistant providers.

8.7.3 Controlling technical performance and related processes

(484) In general, respondents, regardless of their background or size, are dependent on the technical support provided by voice assistants and smart device operating system providers. As a consequence, unresponsiveness regarding technical issues concerning accessibility or functioning of third-party consumer IoT products and services reportedly affects the quality and the brand image of third parties operating via voice assistants and smart device operating systems. For instance, respondents explain that they rely on the voice assistant providers to sort out problems with the activation word and voice command for accessing a consumer IoT service or starting a smart device's function. In this regard, some smart device manufacturers indicate that technical support from voice assistant providers is insufficient and that communication with technical teams when issues arise is not timely enough. However, the majority of players reportedly lack sufficient leverage to negotiate the inclusion of contractual obligations concerning timely technical support in their largely standardised agreements with the voice assistant providers.

(485) With respect to technical support, a number of smart device manufacturers and consumer IoT service providers indicate that they are dependent on the timely advance notice of software updates by smart device operating system and voice assistant providers, in order to adapt their consumer IoT products and services in time for the upcoming changes to the underlying system. Nevertheless, some express the concern that they suffer delays that affect their business planning (that is on the launching of new products not yet adapted to new operating system versions) and even the continuity of their service on third-party voice assistants and operating systems.

(486) Some wearable device manufacturers raise concerns about not receiving full information from smart mobile device operating system providers regarding new devices, operating system updates or privacy policies, which sometimes results in technical problems on the side of the wearable device manufacturers. In this respect, it is reported that unresponsiveness or delayed notifications of updates to smart mobile device operating systems (for example iOS and Android) create difficulties for wearable manufacturers. For instance, some features might be disabled following an operating system update, which creates consumer confusion. In other cases, the update might cause bugs and connectivity problems.

(487) Several respondents raise concerns in particular in relation to one leading operating system and the fact that new operating system updates sometimes require expensive engineering work to make all the wearable device functionalities compatible with the system. Concerns are also raised in relation to operating system providers for being unresponsive and delaying approval of new applications or updates. This is said to harm both consumers, which have limited functionalities on their wearable devices, and the wearable device manufacturers, which see their reputation suffer as a result.

(488) Lastly, some wearable manufacturers have also experienced difficulties with app store providers that block, remove or delay the approval of their companion apps. These

respondents complain that communication with the app store providers during the application review process is difficult and when a certain application or update is not approved, the feedback is very limited.

8.8 CONTRACTUAL ISSUES

(489) Respondents to the Commission's questionnaires, as well as some submissions to the public consultation on the preliminary report, have drawn attention to the fact that some companies' agreements contain clauses that amplify commercial imbalances between them and the weaker contractual party.

(490) For example, some agreements reportedly include clauses enabling one of the parties to terminate an agreement with its contractual parties at its sole discretion or without informing the contractual party beforehand. Other agreements reportedly to contain clauses allowing one of the parties to terminate an agreement should the counter-party introduce infringement proceedings against it concerning intellectual property rights.

(491) Another example is that the scope of the agreements can be very large and apply to a "company" at group level, including all affiliates of the company. This, combined with certain other provisions of the agreement, can give some companies broad rights with respect to, for example, data access and usage, which extend beyond the business division concerned by the agreement.

8.9 KEY FINDINGS

(492) As set out above, the replies to questionnaires, the submitted agreements, as well as the submissions to the public consultation, reveal a certain number of potential concerns.

8.9.1 Pre-installation, default-setting and prominence

(493) The responses to the questionnaires and the submissions to the public consultation reveal the existence of practices regarding pre-installation, default-setting and prominent placement of consumer IoT services on smart devices or in relation to voice assistants. These practices can be decisive for the discoverability, visibility and findability of a consumer IoT service, and can give competitive advantages to the provider of a service that is pre-installed or set as default or is otherwise given a prominent placement. The services allegedly favoured in this way are often the proprietary services of the leading providers of consumer IoT technology platforms, or those of large international creative content service providers, to the detriment of smaller and/or local players.

8.9.2 Exclusivity, concurrency and tying concerns in relation to voice assistants

(494) Attempts by leading voice assistant providers to secure exclusivity of voice assistant presence on certain smart devices or, where dual assistant support is allowed, to prevent the concurrent use of the voice assistants, have been reported. Smart device

manufacturers also raise concerns about voice assistant providers bundling different types of software, technology and applications, including voice assistants.

8.9.3 Data

(495) The sector inquiry findings indicate that voice assistants are at the centre of data collection in the consumer IoT sector and that this allows the leading voice assistant providers to accumulate large amounts of data, enabling them not only to control the data flows and user relationships but also to leverage into adjacent markets that is the provision of IoT services and products. The results of the sector inquiry indicate that not having access to data can raise barriers to new entrants on the voice assistant market and hinder the development of smaller competitors on that market. Moreover, because of the privileged access to volumes of data the leading voice assistant providers can reportedly more easily improve the quality of their voice assistant/voice recognition technology via algorithmic training and machine learning. Finally, some respondents claim that due to the intermediation of the leading ecosystem providers they do not have consistent and immediate access to relevant data on the use of their services and smart devices on third-party voice assistants and smart device operating systems.

8.9.4 Standardisation and interoperability

(496) The majority of respondents observe a lack of interoperability in the consumer IoT sector due to technology fragmentation, lack of common standards and the prevalence of proprietary technology (becoming “de facto” standards in the sector). This situation reportedly hinders compatibility and interoperability between products, services and technology of different brands, which could lock users into the products and services of the same provider and limit consumer choice. Open standardised solutions are reported to develop slowly and to lack the necessary user base to catch up with proprietary innovation.

(497) However, the development of proprietary technologies is at the same time largely welcomed by some respondents, as long as they are well documented, with effective access terms, and allow for broad and full interoperability. It is reported that the current fragmented landscape, in terms of access to the different standards and proprietary technologies, could lead to significant practical difficulties for stakeholders to identify the precise licensing obligations and licensing costs their devices and applications may generate.

(498) Interoperability requires technical and business engagement among companies active in the consumer IoT sector in order to achieve meaningful integration between the different parts of an IoT ecosystem. In practice, however, such integration processes are largely determined by the presence of a few providers of leading proprietary voice assistants and operating systems relevant for the consumer IoT sector. These companies are able to determine independently the requirements to achieve interoperability with their proprietary technology through unilaterally governed terms and conditions, technical requirements and certification processes. By unilaterally governing the

interoperability and integration processes, some respondents to the sector inquiry indicate that the leading voice assistant providers may also be able to limit the functionalities of third-party smart devices and consumer IoT services, compared to their own, by imposing technical constraints, such as limited APIs.

8.9.5 Disintermediation

(499) Respondents raise several concerns regarding the role of the leading providers of voice assistants and smart device operating systems as intermediaries between the user and the smart devices or consumer IoT services that are controllable and accessible through the voice assistant and/or operating system. Respondents fear that they will lose their brand recognition and their direct relationship with the user, as it is voice assistants and smart device operating system providers that usually have the most direct relationship with users through their user interfaces. Also, some of the leading ecosystem providers require that their set-up and user on-boarding processes are followed when the user connects to smart devices or accesses consumer IoT services via their voice assistants and smart device operating systems. Finally, several smart device manufacturers and consumer IoT service providers report difficulties with app store providers who block, remove or delay updates of their apps, and add that there is little or no communication about the reasons for such blockages or delays.