Contribution to Sector Inquiry into the consumer Internet of Things

Foreword

We would like to thank the Directorate-General for Competition of the European Commission for the opportunity to contribute to the competition Sector Inquiry into the consumer Internet of Things (IoT). As a small company operating in an emerging ecosystem, we welcome to opportunity to influence futures rules designed to keep the European IoT market open to all.

A- Contributor Overview

Cybronics was founded in 2010 to design software and services for smart home devices. Over the years we have developed several services targeting consumer IoT devices; in 2010 LifeShow, which enabled users to automatically stream personal photos to their connected screens –Internet enabled Pictured frames, tablets, or Smart TVs – and in 2013 Watsh, which allowed users to remotely watch and comment videos in real-time on connected screens. Since 2017 we have shifted our focus to voice applications for smart speakers and smart displays.

In parallel, we offer professional services to large companies to support their software development projects around new IoT devices; this currently represents our main activity. We provide outsourced design, development, project management and/or maintenance for applications running on IoT devices such as Smart TVs, internet-enabled dongles, STBs, smart speakers, and smart displays. We also provide technical consulting services to support in-house application development. Our customers are mainly large French TMT companies such as France Télévisions, Orange or FDJ.

Over the years we have worked on projects involving all major consumer IoT platforms, from Apple to Google, Amazon and Samsung.

Lastly, we have been granted a European patent (EP2612467B1) related to the processing and sharing of data within a home network, connecting smart home appliances and lighting systems to smart home entertainment devices. We envision a system where smart home devices from different manufacturers are able to locally share data that can then be used to provide targeted advertisements or announcements, while protecting user privacy through on-device processing. We plan to develop a new IoT service based on this patented system and/or to license it in the near future; implementing such as system would require that access to smart home data is not limited by consumer IoT platforms; as such we have a vested interest in assuring the openness of the consumer IoT ecosystem.

B- Contribution to the Sector inquiry

Our contribution should be viewed as complementary to the "Data" chapter of the preliminary report, especially chapter 7.3.5 on Data monetisation, digital advertising, and consumer profiling. We fully share the data related concerns listed in chapter 8.4 of the preliminary report, in particular §(425) regarding data monetisation.

One of the clear benefits for consumers to invest in smart home devices is the ability to simplify their daily lives by creating "routines" that can trigger actions (such as: turning on the lights) on multiple devices from a single command (such as a voice request: "turn on all the lights in the bedroom") or event (such as sunset or sunrise).

Until the launch of smart speakers and multiple purpose voice assistants, the "connected home" ecosystem was still fragmented, with a variety of device manufacturers providing appliances that could only be controlled through dedicated mobile applications. This prevented sharing of data and control between smart devices and implementation of multi-device routines if they involved multiple manufacturers.

A few independent providers of hardware or software IoT Gateways tried to enable control of a variety of devices from a single interface or application, thus allowing the creation of routines spanning different devices; however, these providers found it difficult to maintain interoperability work in the long run, and most were ultimately acquired by large manufacturers (ex: SmartThings by Samsung) or disappeared completely.

With the launch of voice assistants (Siri, Alexa, Google Assistant) and smart speakers, followed by development kits to simplify their integration with smart home devices (Apple HomeKit, Amazon Alexa Smart Home Skill API, Google Smart Home Actions) along with official interoperability certification programs ("Works with Apple HomeKit", "Works with Alexa", "Works with Google Assistant"), the smart home consumer IoT ecosystem has become less fragmented and easier to apprehend for end-users. Multiple smart home devices can now be controlled by a single voice assistant, thus enabling multi-device control scenarios.

As underlined in the preliminary report, if this trend guarantees interoperability with smart home devices and benefits end-users in the short term, it may eventually lead to the emergence of "gatekeepers" to all data generated by the smart home devices, slowing down or preventing future innovations that require access to this data. These gatekeepers will likely be the main consumer IoT technology platforms which are also the main voice assistant providers: Google, Amazon and Apple.

Furthermore, both Google and Amazon have been requesting as part of their certification programs that all certified smart devices continuously expose their state to the Google Assistant or Alexa cloud services; for example a smart light switch must constantly expose its on/off status, or a smart thermostat must provide its currently set temperature. This improves the functionality of voice assistants which are always "aware" of the status of any smart home device and can better interpret commands from end-users, allowing them to offer proactive suggestions or trigger automated routines.

However, this approach also enables the consumer IoT technology platforms to centralize all data generated from smart home devices in real-time, and as they explore new ways to monetize the smart home business, to leverage the position they currently enjoy on adjacent digital markets (advertising or e-commerce) and replicate it on the new consumer IoT sector.

Other consumer IoT technology platforms may also be tempted to "lock-up" the data generated by certified devices to prevent competitive usage by 3rd parties. For example, with iOS 14 Apple has added a new "network privacy control" that blocks 3rd party apps from finding and communicating with local smart home devices, in the name of privacy protection. This has the side effect of restricting functionalities, for example "content casting" from a mobile app to a TV device using a 3rd party protocol, while similar functionalities offered by Apple are not affected, such as the AirPlay protocol. In the future Apple could extend such "privacy controls" to all HomeKit certified devices, preventing manufacturers from sharing any data or functionality with 3rd parties unless they have received explicit confirmation from end-users using an Apple operated consent management framework. This would be similar to the approach Apple implemented with the App Tracking Transparency framework on iOS 14.5.

Whether all smart home data is centralized by gatekeepers, or its access to third parties is severely restricted and controlled by consumer IoT technology platforms, the end result will be the same: a few companies will become gatekeepers for accessing smart home data and only they will be able to monetize it directly or indirectly, at the expense of 3rd party services.

In our view manufacturers and service providers should be able to freely share smart home device data with 3rd parties, only being limited by the GDPR requirements. As such they should not be required to go through a gatekeeper to request data access authorization from end-users, nor be forced to expose all data generated by their devices to a single party to obtain certification. We think that 3 measures should be implemented to guarantee the openness of smart home data:

1. Prevent consumer IoT technology platforms or voice assistant providers from requiring exclusive access to all smart device data for their own usage as part of their interoperability certification programs; smart devices manufacturers should be able to share specific data to 3rd parties, after obtaining user consent;
2. Prevent consumer IoT technology platforms or voice assistant providers from limiting access to real-time smart device data as part of their interoperability certification programs; smart device manufacturers should be able to broadcast real-time smart device data to multiple 3rd parties, after obtaining user consent;
3. Prevent consumer IoT technology platforms or voice assistant providers from requiring that access to smart device data can only be shared with 3rd parties after getting user consent through a platform operated consent management framework; smart device manufacturers and 3rd parties should be able to use any own consent management framework, being bound only by RGPD requirements.

We think these measures will ensure a level playing field for both existing and future actors in the consumer IoT ecosystem and allow future innovations in IoT services and products.
We look forward to the final report on the Consumer IoT Sector Inquiry and remain at the disposal of the Directorate-General for Competition of the European Commission.