

Oscar Borgogno

TOELI Research Fellow, University of Turin, Turin, Italy

Giuseppe Colangelo

Jean Monnet Professor of EU Innovation Policy and Associate Professor of Law and Economics, University of Basilicata, Potenza, Italy; TTLF Fellow, Stanford University, Stanford, USA; <https://orcid.org/0000-0002-0089-3545>; giuseppe.colangelo@unibas.it

Shaping interoperability for the IoT: the case for ecosystem-tailored standardisation

Abstract: No matter how good a smart device may be, it remains useless outside the context of a digital ecosystem. Internet of Things (IoT) environments are possible as long as services and products can interconnect smoothly and exchange data in real time. Therefore, interoperability ranks high in global policy agendas, with the promise of bringing an end to network effects slanted in favour of ecosystem orchestrators. However, recent regulatory initiatives introducing interoperability obligations risk falling short, or even generating unintended consequences, in the absence of a coherent approach to standardisation. Against this backdrop, relying on the UK Open Banking experience, the article makes a proposal for workable interoperability in IoT ecosystems aimed at ensuring market contestability without undermining incentives to innovate.

Keywords: Internet of Things; ecosystems; platforms; data sharing; interoperability; standards; API; Open Banking; antitrust; regulation.

I. Introduction

The Internet of Things (IoT) is positioned at the interplay between physical and digital worlds in a manner that is set to have a profound influence on the world economy.¹ Global IoT revenue is projected to increase by EUR 301.5 billion over the next eight years, peaking at EUR 408.7 billion in 2030, with almost 8 billion devices interconnected.² This new wave goes beyond smart consumer devices as it involves the systemic use of sensors for industrial applications, spanning from remote monitoring of equipment to factory automation and healthcare services.³ In fact, business-to-business solutions are expected to account for nearly 62 per cent of overall IoT revenue by 2030.⁴

¹ United Nations Conference on Trade and Development - UNCTAD, 'Digital Economy Report – Cross-border data flows and development: For whom the data flow', (2021) 32-35 <https://unctad.org/system/files/official-document/der2021_en.pdf> (all the links were last visited on 8 February 2023).

² Statista, "Transforma Insights: Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by use case (in millions)" (2020) <<https://www.statista.com/statistics/1194701/iot-connected-devices-use-case/>>.

³ N Fildes, "Battle intensifies to unlock value in the Internet of Things" (2019) Financial Times, 18 June <<https://www.ft.com/content/a10a52a4-789f-11e9-b0ec-7dff87b9a4a2>>.

⁴ McKinsey & Company, "The Internet of Things: Catching up to an accelerating opportunity" (2021) 13 <<https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it>>.

However, the economic features at the basis of the rapid adoption of IoT may be a double-edged sword if not properly addressed by policy makers. No matter how good a smart device may be, it remains useless outside the context of a digital ecosystem. Since the IoT is a network made up of physical and virtual things which are seamlessly connected, in the absence of smooth interoperability with the rest of the network, any device is likely to lose much of its utility.⁵ Furthermore, IoT environments are possible as long as all sorts of devices can be interconnected and can exchange data in real time. Therefore, the ability to gather and access different data sources is crucial in order for IoT innovation to thrive. As a result, access to data and data sharing practices have attracted attention among policy makers and enforcers as key factors for unlocking competition and incentivising innovation.⁶

The European Union has been a forerunner in promoting the free flows of data to enable inter-platform competition with a broad array of heterogeneous legislative initiatives.⁷ While the General Data Protection Regulation (GDPR) enshrined a general data portability right for individuals⁸, the Second Payment Service Directive (PSD2) introduced a rule on sector-specific access to account data in favour of specific players;⁹ meanwhile, the Regulation on the free-flow of non-personal data has facilitated data sharing practices in the commercial arena (business-to-business).¹⁰ In the same vein, the Commission introduced the Open Data Directive with the goal of putting government data to good use for private players¹¹ and launched the Data Governance Act to promote the voluntary sharing of data by individuals and businesses and to harmonise conditions for the use of certain public sector data.¹²

Nevertheless, the exponential growth of mobile ecosystems and large technology platforms within IoT environments has demonstrated that the competitive landscape has

⁵ There are indications that consumers are wary of the risks posed by the lack of interoperability: see Eurostat, “Data browser: Internet of Things – barriers to use” (2020) <https://ec.europa.eu/eurostat/databrowser/view/isoc_iiot_bx/default/table?lang=en>, reporting that 5% of individuals in the EU cited a lack of compatibility with other devices or systems as their reason for not using IoT.

⁶ See, for example, Bundeskartellamt, “Sector inquiry smart TVs - Conclusion and recommendations for action” (2020) <https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Others/Sector_inquiry_smart_TV_s_conclusion.pdf?__blob=publicationFile&v=2>; Hadopi and CSA, “Assistants vocaux et enceintes connectées - l’impact de la voix sur l’offre et les usages culturels et médias” (2019) <<https://www.hadopi.fr/ressources/etudes/etude-hadopi-csa-assistants-vocaux-et-enceintes-connectees-limpact-de-la-voix-sur>>.

⁷ O Borgogno and G Colangelo, “Data sharing and interoperability: Fostering innovation and competition through APIs” (2019) 35 Computer Law & Security Review 105314.

⁸ 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 [2016] OJ L 119/1, Article 20.

⁹ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, [2015] OJ L 337/35, Article 67.

¹⁰ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, [2018] OJ L 303/59.

¹¹ Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, [2019] OJ L 172/56.

¹² Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), [2022] OJ L 152/1.

not evolved according to the policy makers' expectations.¹³ Digital ecosystems, built on the combination of an operating system running on a mobile phone, have emerged as digital infrastructures within which a huge number of IoT interactions take place. Therefore, the digital economy seems to be moving away from being a market for information where consumers move their data backlog from one provider to another. Indeed, major concerns regarding data lock-in have been raised in recent European data strategy initiatives.¹⁴

As a consequence, policy makers have gradually moved towards a different approach intended to nurture competitive dynamics within and between platform-based ecosystems. With this aim, interoperability requirements are taking centre stage.¹⁵ Indeed, any lack of interoperability between providers may act as a technical barrier making it harder for users to switch and multi-home.

Notably, in its data strategy, the European Commission announced the establishment of EU-wide common, interoperable data spaces in strategic sectors to overcome legal and technical barriers to data sharing.¹⁶ Further, the Commission has identified the lack of interoperability as a crucial element for the exploitation of data value, especially in the context of artificial intelligence deployment.¹⁷ Furthermore, as of November 2022 the Digital Markets Act (DMA) has entered into force, introducing, amongst its other provisions, interoperability obligations for online platforms having a gatekeeping position.¹⁸ Notably, the DMA envisages horizontal interoperability for basic functionalities of number-independent interpersonal communications services and vertical interoperability obligations to install third-party app stores and sideload apps, and to ensure access to essential functionalities of operating systems or hardware capabilities of a given device.¹⁹

With specific regard to IoT environments, the relevance of platform ecosystems and interoperability were underlined by the European Commission in a recent sector inquiry²⁰ and in the proposal for a Data Act.²¹

¹³ European Commission, Commission Staff Working Document accompanying the "Final Report - Sector inquiry into consumer Internet of Things" COM(2022) 10 final, 41, acknowledging that Amazon, Google, and Apple "have become the leading technology companies and built their own ecosystems within and beyond the consumer IoT sector."

¹⁴ See European Commission, "A European strategy for data" COM(2020) 66 final, 10; and European Commission, "Towards a common European data space" COM(2018) 232 final, 10.

¹⁵ See European Commission, Commission Staff Working Document accompanying the Communication on the Digitising European Industry Reaping the full benefits of a Digital Single Market, SWD(2016) 110 final, 9, targeting the lack of common standards and interoperable solutions throughout the products and services life cycles as one of the main hurdles to IoT innovation.

¹⁶ European Commission, "A European strategy for data", supra note 14.

¹⁷ Ibid., 8. See also European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM(2021) 206 final, Recital 81, referring to the possibility of developing further measures aimed at "lowering technical barriers hindering cross-border exchange of data for AI development, including on data access infrastructure, semantic and technical interoperability of different types of data."

¹⁸ Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), (2022) OJ L 265/1.

¹⁹ Ibid., Articles 6(4), 6(7), and 7.

²⁰ European Commission, "Final Report - Sector inquiry into consumer Internet of Things" COM(2022) 19 final.

²¹ European Commission, Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act) COM (2022) 68 final.

In the former, on the premise that the market viability of IoT service providers and smart device manufacturers depends on the smooth access to dominant technology platforms, the Commission argued that both horizontal and vertical interoperability among consumer services, smart devices, and technology platforms play a pivotal role in unlocking the full potential of IoT ecosystems and preventing any lock-in to a certain provider's products.²² In the latter, by pursuing the overarching goal to end *de facto* exclusivity control over personal and non-personal information enjoyed by manufacturers of data collecting devices, the Commission acknowledged that the right to data portability enshrined in the GDPR is inherently unfit to deliver on the pro-competitive expectations voiced by academics and policy makers.²³ Further, according to the Commission, the absence of an obligation to create technical interfaces for automated and continuous data flows in the context of IoT "can make it hard to offer certain services that require real time data flows, leading to lock-in situations for data subjects and hampering the development of innovative services based on access to such data."²⁴ However, the proposal supports the adoption of open interoperability specifications and standards only to facilitate switching between data processing services.²⁵

The role of interoperability has been finally confirmed in the launch of the proposal for a European Health Data Space (EHDS), the first common data space in a specific area to emerge from the EU strategy for data.²⁶ Indeed, the Commission pointed to the absence of binding or compulsory standards across the EU and consequently limited interoperability.²⁷ More recently, EU institutions committed to promoting interoperability and open standards in the European Declaration on Digital Rights and Principles for the Digital Decade.²⁸

As far as any type of interoperability is concerned, standards are decisive to enable the broad complementarity of products and services. The reliance of IoT applications on seamless interoperability and continuous access to different data sources requires efforts to be made in the field of standardisation. Indeed, IoT devices are integrated by means of

²² European Commission, *supra* note 20, 5.

²³ European Commission, Commission Staff Working Document, Impact Assessment Report accompanying the Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act) SWD(2022) 34 final, 10. On the inherent pro-competitive rationale underpinning the right to data portability and the risk of inconsistencies with the GDPR overall framework, see B Koops, "The trouble with European data protection law" (2014) 4 International Data Privacy Law 4, 44, arguing that "[b]y its nature, data portability would be more at home in the regulation of unfair business practices or electronic commerce, or perhaps competition law—all domains that regulate abuse of power by commercial providers to lock-in consumers."

²⁴ European Commission, Data Act (including the review of the Directive 96/9/EC on the legal protection of databases) – Inception Impact Assessment (2021) 3 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en>.

²⁵ See, e.g., W Kerber "Governance of IoT Data: Why the EU Data Act will not Fulfill its Objectives" (forthcoming) GRUR International, arguing that the proposal does not solve the problem of data interoperability with respect to sharing IoT data and noting that the data is also not required to be made available in standardised formats and by using standardised and open technical interfaces.

²⁶ European Commission, Proposal for a Regulation on the European Health Data Space COM(2022) 197 final.

²⁷ *Ibid.*, Explanatory memorandum, 9-10.

²⁸ European Council, "Declaration on digital rights and principles: EU values and citizens at the centre of digital transformation" (2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/11/14/declaration-on-digital-rights-and-principles-eu-values-and-citizens-at-the-centre-of-digital-transformation/>.

intelligent interfaces to develop smart environments in which each item is able to exchange data in order to improve the customer experience.

To this end, analysing limits and potentials of interoperability obligations in fostering competition and innovation across the IoT economy, this article aims to assess whether and to what extent the experience of consumer financial data sharing regulatory framework may provide useful insights. In particular, noting that Open Banking shows similar competitive dynamics and interoperability features, we argue that the experience developed in the UK could serve as a best practice to implement workable interoperability in the IoT.²⁹

The paper is structured as follows. Section II summarizes the recent literature on interoperability. Section III analyses the role of standards in ensuring the effectiveness of interoperability initiatives and the significant trade-offs faced by policy makers. Section IV illustrates the Open Banking experience and the different approaches taken towards Application Programming Interfaces (APIs) standardisation in the retail payment market. Section V puts forward a proposal for delivering workable interoperability in the IoT landscape to ensure market contestability without threatening incentives to innovate. Section VI concludes.

II. Interoperability: definitions and related literature

Since the concepts of interoperability and portability have been widely used in different contexts and are not necessarily always well distinguished, it is worth providing a clarification about their respective features and implications.³⁰

Interoperability can be broadly defined as the ability of two or more products or services to work together despite differences in interface, execution, or coding language.³¹ More specifically, full interoperability involves interchangeability, compatibility and usability of services and products offered by different companies.³² Indeed, as noted by Crémer, de Montjoye, and Schweitzer, three sub-categories of interoperability can be identified in addition to the concept of data portability.³³ First, protocol interoperability (or partial

²⁹ UK Competition and Markets Authority, “Retail banking market investigation: Final report” (2016) <<https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk>>.

³⁰ See D Schnurr, “Switching and Interoperability Between Data Processing Services in the Proposed Data Act” (2022) CERRE Report, 11, <<https://cerre.eu/publications/switching-and-interoperability-between-data-processing-services-in-the-proposed-data-act/>>, arguing that the proposal for a Data Act includes rules referring to both data portability and interoperability in the context of data processing services, without however neither distinguish between them nor making sufficiently clear as to which rules are intended to achieve each of them.

³¹ P Wegner, “Interoperability” (1996) 28 ACM Computing Surveys 285.

³² C Thanos, “Mediation: the technological foundation of modern science” (2014) 13 Data Science Journal 88, 93.

³³ J Crémer, Y-A de Montjoye, and H Schweitzer, “Competition policy for the digital era” (2019) 58-59 <<https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>>. See also C Busch, N Fourberg, J Kramer, P Kroon, N Steffen, S Taş, P Thoste, and L Wiewiorra, “Interoperability regulations for digital services. Study for the German Federal Network Agency” (2022) <https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Onlinekomm/Study_1_interoperabilityregulationsDigiServices.pdf?__blob=publicationFile&v=1>, distinguishing between compatibility and interoperability by building on the concept of digital environment: while the first refers to the unimpeded operation and consistent interchangeability of components, applications and systems (especially within an environment), the second is based on the prerequisite of a common standard as it

interoperability) refers to the ability of different products and services to work together in a complementary fashion. This form of interoperability allows smooth interaction between different and potentially complementary services or products provided by different manufactures. Second, full protocol interoperability ensures that two or more substitute services can interoperate through a more fundamental interconnection and alignment of features (such as messaging systems or mobile ecosystems). Partial and full protocol interoperability should be understood as a continuum.³⁴ While the former requires that only some or a subset of all features are shared with other players, the latter involves a deeper level of integration and standardisation between operators. Third, data interoperability refers to the ability of sharing and accessing data on a continuous, often reciprocal, real-time basis (usually through APIs).³⁵

Conversely, data portability is the ability to port from data holder A to data holder B a bulk of data created during the use of a service by an individual. As clarified by Schnurr, data portability differs from data interoperability because it comes with a one-off transfer at a specified point in time.³⁶ In order to be effective and enable consumer switching, data portability requires that the information is available in a structured, commonly used, and machine-readable format, but not a systemic use of APIs.

An additional clarification regards the distinction between vertical and horizontal interoperability.³⁷ While the former (i.e. interoperability within a platform/ecosystem) enables downstream integration across the value chain between complementary products as well as within a digital infrastructure provided upstream, the latter (i.e. interoperability between platforms/ecosystems) requires that similar services and products can smoothly interoperate between each other so to share direct network effects. As such, horizontal interoperability can be conflated with full protocol interoperability, whereas vertical interoperability relies to a large extent on protocol interoperability.

The case for horizontal and/or vertical interoperability has become a much-debated issue for competition policy in digital markets. Indeed, whether horizontal interoperability represents the proper regulatory solution to ensure an effective data sharing and promote technological innovation is controversial.

Notably, on the premises that interoperability increases network effects for all players, Crémer, Rey and Tirole argue that interoperability can level the playing field between small and large players, hence increasing contestability and competition.³⁸ More recently, Crawford et al. maintain that such obligations are necessary to avoid the economic risks

focuses on the cooperation and combinability of components, applications and systems that may be located in different environments.

³⁴ Busch, Fourberg, Kramer, Kroon, Steffen, Taş, Thoste, and Wiewiorra, *supra* note 33, 7.

³⁵ See also OECD, “Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies” (2019) OECD Publishing, 32, considering APIs as promising mechanisms through which data access can be controlled through time.

³⁶ Schnurr, *supra* note 30, 11.

³⁷ See, e.g., M Bourreau, J Krämer, and M Buiten, “Interoperability in Digital Markets” (2022) <https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf>; J Mancini, “Data Portability, Interoperability and Digital Platform Competition” (2021) OECD Background Paper <<https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf>>; C Riley, “Unpacking interoperability in competition” (2020) 5 *Journal of Cyber Policy* 94; W Kerber and H Schweitzer, “Interoperability in the digital economy” (2017) 8 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 39.

³⁸ J Crémer, P Rey, and J Tirole, “Connectivity in the Commercial Internet” (2000) 48 *Journal of Industrial Economics* 433.

arising from firm-specific network effects (e.g. lock-in dynamics and market tipping).³⁹ However, Bourreau points out that interoperability and multi-homing may represent two substitute means to enhance competition and improve contestability in digital markets.⁴⁰ More specifically, mandating horizontal interoperability can have ambivalent impacts on competition.⁴¹ Bourreau and Krämer show that, as homogenization restricts differentiation and innovation opportunities, mandating horizontal interoperability could reduce existing incentives for multi-homing and ultimately hinder competition.⁴² By analyzing the consolidation process of U.S. securities clearinghouses and depositories, Awrey and Macey argue that horizontal interoperability requirements could help dominant firms to take advantage of a frictionless environment with low barriers to entry, ultimately entrenching their monopoly power.⁴³

Further, if multi-homing is possible without significant costs, the potential welfare gains from horizontal interoperability obligations are limited in digital markets where innovation is occurring at a fast pace.⁴⁴ Moreover, forcing market players who already developed their own services to implement new horizontal interoperability obligations would be highly costly, complex, and time-consuming, especially for regulatory monitoring and enforcement.⁴⁵ Finally, as interconnected networks should use the same encryption method, horizontal interoperability may affect security and privacy.

In light of these considerations, concerns have been raised by the European Commission itself on the DMA proposal to make number-independent interpersonal communication services and social network services offered by gatekeepers horizontally interoperable.⁴⁶ Alongside several technical issues, it is argued that the measure would be doomed to hinder innovation, incentives to invest, and service differentiation, ultimately damaging consumer welfare.

III. The role of standards

A second layer of complexity involves the relationship between interoperability and standards.

³⁹ GS Crawford, D Dinielli, A Fletcher, P Heidhues, M Schnitzer, FM Scott Morton, and K Seim, “Equitable Interoperability: the “Super Tool” of Digital Platform Governance” (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3923602>.

⁴⁰ M Bourreau, “DMA: Horizontal and Vertical Interoperability Obligations” (2022) CERRE Issue Paper, <https://cerre.eu/wp-content/uploads/2022/11/DMA_HorizontalandVerticalInteroperability.pdf>.

⁴¹ Busch, Fourberg, Kramer, Kroon, Steffen, Taş, Thoste, and Wiewiorra, *supra* note 33, 58.

⁴² M Bourreau and J Krämer, “Interoperability in Digital Markets: Boon or Bane for Market Contestability?” (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4172255>.

⁴³ D Awrey and J Macey, “Open Access, Interoperability, and DTCC’s Unexpected Path to Monopoly” (2022) 132 *Yale Law Journal* 1.

⁴⁴ Bourreau, Krämer, and Buiten, *supra* note 37, 24.

⁴⁵ Bourreau, *supra* note 40, 10; and Schnurr, *supra* note 30, 9.

⁴⁶ European Commission, “Non-paper from the Commission services on interoperability for messenger services and online social networks in the DMA” (2022) <<https://www.iccl.ie/wp-content/uploads/2022/03/wk03135.en22.pdf>>. See also Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, “Interoperability between messaging services – an overview of potential and challenges” (2021) 18, <https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2021/20211209_Messenger.html>, pointing out that “an increasing depth of technical implementation of interoperability (for example, due to increased standardisation) may restrict options for expanding the scope of functions and innovation.”

Interoperability relies on standardisation in order to be effective. Different manufacturers and application developers can benefit from open access and interoperability requirements as long as technical protocols and APIs are designed in a homogeneous way, guaranteeing effective data access and smooth interconnection with the underpinning digital infrastructure. Standards serve exactly this purpose by providing a set of technical rules and characteristics which allow devices not only to connect and integrate, but also to ensure the quality and security of IoT interactions. Moreover, from the perspective of competition policy, well-designed standards prevent the risk of third-party providers being surreptitiously undermined in comparison to proprietary services through lower levels of interoperability.

When it comes to the design and implementation of standards, two main distinctions arise.

With regard to the implementation aspect, standards can be open or closed, depending on whether developers retain control over access and implementation of the underlying technologies. While the former are open source and freely available to manufacturers and services providers willing to enter the market with interoperable products, proprietary standards often require a licence for the intellectual property owned by developers and may also come with proprietary enhancements for administering access to specific market niches.

Depending on how they are developed, standards can be industry-led or formal. The former are designed by market players which (independently or collectively) voluntarily agree to define common procedures and characteristics for products and services in a timely fashion. When these solutions are broadly adopted by the market participants, they are considered *de facto* standards as their implementation is substantially unavoidable for manufacturers. Conversely, formal standards are developed with a top-down approach by standard development organisations (SDOs) officially appointed by policy makers and regulators.⁴⁷ They are usually developed via processes that are transparent and open to broad participation by the industry and by stakeholders under the coordination and rules set by the competent SDOs. While formal standardisation prioritizes consensus and social welfare implications over efficiency, industry-led standards focus on agility, speed, and the need for a positive reaction by the market participants in order to succeed.

The policy choice between voluntary and mandatory standardisation initiatives involves relevant trade-offs. Technical expertise and flexibility considerations support bottom-up spontaneous standardisation processes. Moreover, there is a risk that mandating specific solutions in markets at an early stage of development may undermine innovation and lower incentives to invest.⁴⁸ On the other side, technology fragmentation or the lack of open standards available on the market, as well as the need to ensure a prompt and effective data sharing, may justify top-down interventions and mandatory standards.⁴⁹ Indeed, standardisation may be a complex and time-consuming process because of the difficulties in reaching an agreement when several players are involved with different and potentially conflicting incentives.

⁴⁷ Under EU law, formal SDOs are those recognised by Regulation (EU) No 1025/2012 on European standardisation [2012] OJ L 316/12.

⁴⁸ Kerber and Schweitzer, *supra* note 37, 58, stressing that uncertainty about the appropriate standards and other interoperability solutions calls for caution in imposing top-down public policy solutions.

⁴⁹ J Kramer, “Personal Data Portability in the Platform Economy: Economic Implications and Policy Recommendations” (2020) 17 *Journal of Competition Law & Economics* 2, arguing for a more widespread obligation to offer standardised APIs to enable consumers to continuously port their data according to Article 20 GDPR.

These trade-offs also emerge from the recent EU Commission's IoT sector inquiry, where the majority of participants expressed the need to prioritise standardisation over proprietary solutions in order to guarantee higher levels of interoperability.⁵⁰ The Commission noted that the IoT standardisation environment is strongly heterogeneous, as smart devices and services rely on a mix of protocols, open standards, open sources, and proprietary technologies, depending on the different technology layers implemented in smart devices.⁵¹ While formal standards prevail only at the level of basic connectivity technologies (e.g. Bluetooth and WiFi), *de facto* standards have emerged in the field of operating systems, wearable devices and user interfaces.⁵² Technology fragmentation and *de facto* standards can exacerbate the costs and complexity of interoperability. As things stand, manufacturers risk having to make redundant investments in order to comply with heterogeneous APIs and certification processes, ultimately leading to the poor reusability of technical solutions and imposing major hurdles to product innovation.⁵³ Further, recent competition inquiries into payment and financial services outlined the risk that API standard fragmentation could translate into higher barriers to entry for new entrants.⁵⁴

Therefore, the Commission, on one hand, has praised open standardisation and encouraged dialogue and interaction between IoT players in order to develop industry-wide standards⁵⁵, and, on the other hand, has recognised that intense standardisation activities by a high number of competing SDOs and private partnerships/industry organisations in the IoT sector might also lead to a lack of transparency and ultimately undermine interoperability.⁵⁶

In this scenario, European policy makers did not take a clear stance towards standardisation. Notably, while acknowledging the importance of interconnection for the flourishing of competition in IoT and data-enabled environments, there is no clear indication as to how standards should be developed and implemented in order to ensure workable interoperability across digital markets. Indeed, the DMA merely states that, "where appropriate and necessary", the Commission may mandate European standardisation bodies to develop appropriate standards.⁵⁷ With regards to number-independent interpersonal communications service, gatekeepers are obliged to provide the necessary technical interfaces or similar solutions that facilitate interoperability, upon request, and free of charge.⁵⁸ Similarly, the Data Act proposal rules out the possibility of mandating the adoption of technical standards or interfaces. However, it provides the Commission with the power to delegate the adoption of European harmonised standards for the interoperability of data processing services.⁵⁹ Further, the Commission pledges to

⁵⁰ European Commission, *supra* note 20, 71.

⁵¹ *Ibid.*, 6.

⁵² European Commission, *supra* note 13.

⁵³ *Ibid.*, 98-99.

⁵⁴ See Hellenic Competition Commission, "Final Report on the Sector Inquiry into Financial Technologies" (2022) <<https://epant.gr/en/enimerosi/press-releases/item/2460-press-release-publication-of-the-final-report-of-the-fintech-sector-inquiry.html>>; Autorité de la Concurrence, "Opinion on the sector of new technologies applied to payment activities" (2021) <<https://www.autoritedelaconcurrence.fr/en/opinion/sector-new-technologies-applied-payment-activities>>.

⁵⁵ European Commission, *supra* note 20, 58.

⁵⁶ *Ibid.*, 71 and 101-102.

⁵⁷ DMA, *supra* note 18, Article 48.

⁵⁸ *Ibid.*, Article 7.

⁵⁹ Data Act, *supra* note 21, Article 28(4).

adopt common specifications by way of implementing acts in case harmonised standards are missing or existing standards are insufficient.⁶⁰

On a related note, the UK Open Banking initiative stands out as one of the most advanced cases of mandated interoperability in the digital economy instead.⁶¹ Open Banking is commonly seen as a secure environment that allows consumers to share bank transaction data with trusted third parties who can analyse such information to offer them new services or make payments on their behalf. Therefore, it has the potential to strengthen the consumer bargaining position in relation to financial service providers by facilitating choice and improving the quality of data-enabled products.⁶²

The global attention gained by the Open Banking project convinced the UK Government to expand third-party data access and API standardisation to a broader range of financial services and products, thereby launching the Open Finance project.⁶³ This initiative is part of the broader Smart Data strategy under which the UK Government is looking to expand data access tools in all regulated markets.⁶⁴

Against this background, this paper aims at contributing to the literature on interoperability and standards assessing whether the Open Banking standardisation approach may serve as a valuable blueprint for tackling some of the competitive issues underpinning IoT business environments.

IV. The Open Banking experience

Following a review of retail banking, in 2017 the UK Competition and Markets Authority (CMA) found that incumbent banks, which had consistently retained an 80 per cent market share of the retail banking market over the years, were exploiting consumer stickiness and barriers to entry in order to enjoy monopolistic rents, jeopardising data-enabled innovation.⁶⁵ In order to tackle these competitive weaknesses, the CMA made full use of its market investigation powers to ease the functioning of the access-to-account rule enshrined in the PSD2.

This piece of legislation mandated banks to allow customers to share their account transaction data with trusted third parties but left them free to do so while adopting the method they preferred.⁶⁶ As a result, access seekers would have to face major transaction costs as they would either have to develop applications working with many different API standards or rely on technical service providers to interoperate with different banks. Moreover, the incumbents had a clear incentive not to cooperate in the implementation

⁶⁰ Ibid., Article 28(5).

⁶¹ UK Competition and Markets Authority, *supra* note 29.

⁶² O Borgogno and G Colangelo, “Consumer Inertia and Competition-sensitive Data Governance: The Case of Open Banking” (2020) 9 *Journal of European Consumer and Market Law* 4.

⁶³ Financial Conduct Authority, “Open finance – Feedback Statement” (2021) <<https://www.fca.org.uk/publication/feedback/fs21-7.pdf>>.

⁶⁴ Department for Business, Energy and Industrial Strategy, “Smart Data Working Group” (2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/99336/5/smart-data-working-group-report-2021.pdf>.

⁶⁵ UK Competition and Markets Authority, *supra* note 29.

⁶⁶ O Borgogno and G Colangelo, “Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule” (2020) 31 *European Business Law Review* 4.

of the access-to-account rule and to keep their own infrastructure as closed as possible to potential rivals.⁶⁷

To address these concerns, the CMA required the nine major banks in Britain and Northern Ireland to agree on common and open API standards, data formats and security protocols that would allow new entrants to calibrate their applications according to a single set of specifications.⁶⁸ The CMA entrusted a special purpose organisation (the Open Banking Implementation Entity) with the task of reaching an agreement between the banks, consumer representatives and fintech third-party providers on the appropriate standards for implementing financial data access. The CMA also appointed an Implementation Trustee, having the power to impose binding decisions on all nine major banks subject to the order in the case of no deal.⁶⁹ As such, this remedy imposed full protocol interoperability with reference to the payment data infrastructure of banks and other account providers.

The common standard approach allowed the UK to gain a leading position in the worldwide adoption of financial data sharing.⁷⁰ The CMA order significantly secured the adoption of Open Banking by preventing incumbents from delaying and frustrating the implementation of the access-to-account rule. Furthermore, account providers that were not subject to the remedy also decided to comply with PSD2 by adopting free API standards rather than develop their own. As of August 2021, there were 119 firms with live to market open banking-enabled products and services while the Open Banking ecosystem accrued around 3 million users in Great Britain and Northern Ireland.⁷¹

By taking stock of the UK experience, Australia introduced an even more ambitious economy-wide data sharing framework (i.e. the Consumer Data Right - CDR), which gives consumers the right to share their data between any kinds of service providers of their choosing.⁷² In 2019, this regime was initially implemented within the banking sector. The Australian Competition and Consumer Commission required the four major banks to share product reference data with accredited data recipients and mandated the adoption of a single set of API standards for data sharing.⁷³ Further, the Australian Government established the Data Standards Body to deliver open standards supporting

⁶⁷ Portuguese Competition Authority, “Sector inquiry on FinTech” (2021) <<https://www.concorrenca.pt/en/articles/adcs-sector-inquiry-fintech-74-companies-operating-portugal-consider-there-are-barriers#:~:text=The%20findings%20of%20the%20sector,a%20closed%20ecosystem%20as%20barriers>>

⁶⁸ UK Competition and Markets Authority, “The Retail Banking Market Investigation Order 2017” (2017) <<https://www.gov.uk/government/publications/retail-banking-market-investigation-order-2017>>.

⁶⁹ UK Competition and Markets Authority, “Agreed Timetable and Project Plan” (2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885537/Notice_of_proposed_changes_to_the_open_banking_roadmap_-_web_publication_-_cma_gov_uk_-_May_2020_-_pdf>.

⁷⁰ Payments Cards & Mobile and Mastercard, “The future of open banking in Europe” (2021) <<https://openbanking.mastercard.com/readiness-index/open-banking-readiness-index/>>.

⁷¹ Open Banking Implementation Entity, “Open Banking Impact Report” (2021) <<https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-october-2021-ug/home/>>.

⁷² Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth).

⁷³ Australian Competition and Consumer Commission, “Competition and Consumer (Consumer Data Right) Rules 2020” (2020) <<https://www.accc.gov.au/media-release/consumer-data-right-rules-made-by-accc>>.

the CDR. Within this entity, various working groups open to participation by any stakeholders are now designing and testing open standards.

Given the UK and Australian experiences, many other jurisdictions developed a considerable interest in following suit. Conversely, the EU has refrained from publicly mandating API standardisation and has left banks free to come up with their own data sharing interfaces or to take part in privately-led standardisation initiatives.⁷⁴ The underpinning rationale of such choice was hinged on the concern that a common API standard could jeopardise innovation and dynamic competition between standards. However, when launching the Digital Finance and the Retail Payments Strategies in 2020, the European Commission recognised that the lack of APIs interoperability hindered newcomers and committed to establish an Open Finance framework by the end of 2024 as well as to review the PSD2.⁷⁵

V. Open Banking as a blueprint for IoT interoperability regulation?

Some elements suggest that the Open Banking approach could serve as a best practice to implement workable interoperability in the IoT universe.

In particular, Open Banking resembles the IoT in terms of its competitive dynamics and interoperability features as it builds on smooth data sharing mechanisms and connection between different service providers in the context of vertically integrated platforms. Indeed, similar to the retail payment market, the IoT sector encompasses various service providers connected between each other and the role of intermediaries (either banks or leading technology platforms) enabling machine and user interaction is of the utmost importance for the network to thrive.

Further, information is a key input not only to compete in financial services, but also to design and produce smart products that can meaningfully interoperate within leading digital ecosystems. Therefore, the type of information that leading technology platforms and financial institutions hold and the way they use it is pivotal for the potential flourishing of IoT and financial technology. Given the gateway role that such incumbents

⁷⁴ Some late and light-touch attempts to ensure API interoperability were taken by the European Payment Council (“Terms of reference of the SEPA Payment Account Access Multi-Stakeholder Group” (2021) <<https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2021-08/EPC166-21v1.0%20-%20ToR%20SEPA%20Payment%20Account%20Access%20MSG.pdf>>) and the European Banking Authority (establishing an industry working group on APIs and publishing seven sets of clarifications in response to its requests, <<https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/eba-working-group-on-apis-under-psd2>>). In January 2019 the Euro Retail Payments Board (ERPB) established a new Working Group tasked with defining key elements of a potential Single Euro Payments Area API Access Scheme (Euro Retail Payments Board, “Report on a Single Euro Payments Area (SEPA) Application Programming Interface (API) Access Scheme” (2019) <https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/11th-ERPBM-meeting/Report_from_the_ERPB_WG_on_a_SEPA_API_Access_Scheme.pdf>). Its mandate was renewed in June 2021 and a Work Block, consisting of experts and representatives of interested European standardisation initiatives in the field of PSD2 APIs, was established with the goal of developing “minimum requirements that ensure pan-European harmonisation and interoperability as well as the integrity of the scheme” (European Payment Council, “Call for European standardisation initiatives in the field of PSD2 API’s to participate in the API Work Block of the SEPA Payment Account Access Multi-Stakeholder Group” (2022) <<https://www.europeanpaymentscouncil.eu/news-insights/news/call-european-standardisation-initiatives-field-psd2-apis-participate-api-work>>).

⁷⁵ European Commission, “Digital Finance Strategy for the EU” COM (2020) 591 final, 14; European Commission, “Retail Payments Strategy for the EU” COM (2020) 592 final, 15.

may play for the viability of data-enabled products and services, a data bottleneck problem may affect both IoT environments and retail financial markets. In this respect, users' data may sometimes constitute a significant barrier for newcomers willing to enter either the retail financial or the IoT markets.

Moreover, both the financial retail and the IoT sectors feature fragile market dynamics closely dependent on users' trust. Therefore, the ability of infrastructure orchestrators to maintain high levels of cybersecurity, personal data protection, and users' engagement is particularly relevant.⁷⁶ Ultimately, the financial and IoT universes are multi-sided markets where technical failures and unexpected changes can trigger crisis of confidence leading to death spirals for platform-based business models. Thus, both environments share a common need to avoid degradation of network quality due to poorly secured interoperability mechanisms.

The suggestion of looking at the Open Banking as a useful case study for IoT interoperability and standardisation is supported by a recent market study conducted by the CMA, which explicitly referred to the Open Banking as a model to ensure the successful rollout of electric vehicles (EVs) and related charging infrastructure.⁷⁷ Indeed, since vehicles are physical products that obtain, generate or collect data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service, they are explicitly included in the Data Act scope. EV smart charging requires effective data sharing among several stakeholders. The lack of interoperability due to differing standards limits consumer choice about where to charge and how to pay. Therefore, similar to what happens in IoT environments, the main regulatory challenges relate to the policy choices involving interoperability and standardisation. In particular, policy makers are called to gauge the option for a mandated rather than a spontaneous API adoption by providers in order to deliver effective interoperability.⁷⁸

However, since interoperability is context dependent, some important differences between retail financial markets and the IoT should not be overlooked. The banking industry is indeed much more mature than the IoT and mandated interoperability was justified by the empirical identification of a market failure. Further, the banking industry is characterized by a relative high number of legacy incumbents. Hence, if each bank were allowed to adopt different data sharing interfaces, newcomers would face extremely high transaction costs.⁷⁹ Conversely, the IoT has witnessed a much quicker world-wide consolidation process and the market viability of IoT service providers and smart device

⁷⁶ D Evans, "Governing Bad Behavior by Users of Multi-sided Platforms" (2012) 27 Berkeley Technology Law Journal 1201.

⁷⁷ UK Competition and Markets Authority, "Electric Vehicle Charging market study" (2021) <<https://www.gov.uk/cma-cases/electric-vehicle-charging-market-study>>. See G Colangelo and S Ennis, "Energy Data Sharing and the Case of EV Smart Charging" (2022) CERRE Report <<https://cerre.eu/publications/energy-data-sharing-and-the-case-of-ev-smart-charging/>>.

⁷⁸ For a different proposal drawing on the Open Banking experience, see D Awrey and J Macey, "The Promise and Perils of Open Finance" (2023) 40 Yale Journal on Regulation 1, arguing for a universal access requirement in the context of the US data aggregation market to ensure that firms offering financial products and services enjoy non-discriminatory access to Open Finance platforms.

⁷⁹ R Berner and K Judge, "The Data Standardization Challenge" in (DW Arner, E Avgouleas, D Busch, and SL Schwarcz, eds) *Systemic Risk in the Financial Sector: Ten Years After the Great Crash* (Montreal, McGill-Queen's University Press, 2019, 135).

manufacturers currently depends on smooth access to a small number of dominant technology platforms (i.e. Alphabet, Amazon, and Apple).⁸⁰

For these reasons, we advance a proposal for ecosystem-tailored standardisation that relies on the Open Banking approach, but introducing adaptations to the specific features of the sector at issue.

Moving from the premises that common certification procedures, APIs, and open standards are needed to ensure smooth data access and interoperability, we suggest that IoT ecosystem orchestrators should be asked to engage in standardisation processes that are transparent and open to broad participation by the industry and by stakeholders. Nonetheless, such regulatory initiative should aim at ensuring interoperability within each ecosystem (rather than among ecosystems) in order to preserve differentiation and incentives to innovate. Therefore, leading IoT ecosystems should be required to implement vertical interoperability.

As orchestrators of key bottlenecks within the IoT economy, they can restrain other firms' ability to benefit from network effects and obtain unchallenged access to users' data. Further, they are in a position to determine requirements and certification processes by which access and interoperability with their ecosystems take place. Moreover, as they usually are vertically integrated and compete with third-party providers over their own platforms, such a dual role may incentivise them to give preferential treatment to their own products and services (so called self-preferencing) by restricting interoperability for third-party services and devices. In this scenario, vertical interoperability would promote complementary innovation and modular combination of services across the value chain.

Conversely, horizontal interoperability should be rejected as it could cause unintended consequences in terms of inter-ecosystem competition and dynamic innovation.⁸¹ Indeed, it would force firms to provide substitutable services and products, preventing differentiation between ecosystems for the sake of delivering a level playing field among providers. In addition, horizontal interoperability could raise data security issues.

Moreover, digital ecosystem orchestrators should be required to design open interoperability standards together with third-party providers and manufacturers under the strict oversight of a publicly appointed supervisor. In the event of a failure to reach a compromise between the different stakeholders, the competent supervisory body would have the power to impose a solution on all parties. Similarly, the competent supervisor should be entrusted with the task of overseeing compliance over time both from the sides of leading technology platforms as well as from third-party manufacturers and service providers. As already happened with the UK Open Banking, there is a serious risk that incumbents could try to surreptitiously undermine data transfers with the final goal of watering down the competitive potential of interoperability.⁸²

⁸⁰ European Commission, *supra* note 20, 44-47; UK Competition and Markets Authority, "Mobile ecosystems market study" (2022) 50 <<https://www.gov.uk/government/publications/mobile-ecosystems-market-study-final-report>>.

⁸¹ See Borreau, Krämer, and Buiten, *supra* note 37, noting that, in the dynamic context of digital markets, services compete and differentiate themselves by innovating concerning new features, which runs counter to attempts to standardise services, hence mandated horizontal interoperability is likely a harmful remedy in digital markets, as it tends to enshrine existing incumbency, limits the firms' innovation and differentiation capabilities, and requires enduring regulation.

⁸² The importance of enforcement and policing against surreptitious forms of non-compliance was recently highlighted by Barclays and Lloyds's breaches of the CMA Open Banking Remedy in relation to open APIs for data access. See UK Competition and Markets Authority, "Lloyds Banking Group's Breaches of The

As long as public supervision and transparency are ensured, ecosystem-tailored standardisation could harness the skills and best-practices developed by existing technical bodies. For instance, formal SDOs already opened several work streams for the development of IoT standards both in the EU and at international level. The European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) actively cooperate with the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) to develop standards facilitating interoperability and communication between voice assistants, wearable devices, and consumer IoT services as well as smart home devices.⁸³ At the same time, several industry-led standardisation initiatives which emerged over the last decade could offer useful technical guidance. In 2019, Apple, Google, and Amazon established a working group (now named Matter) within the Connectivity Standards Alliance to launch a new, royalty-free connectivity standard enabling compatibility among a large range of smart home devices.⁸⁴ Moreover, since 2014 the Thread Group alliance has been operating to provide network protocols to connect and control products for home automation.⁸⁵ Finally, in 2019 both Amazon and the Linux Foundation launched initiatives (the Voice Interoperability Initiative and the Open Voice Network respectively) to facilitate multi-homing and interconnection between voice-assistants.⁸⁶

Nevertheless, the proposal at stake would be time-consuming and resource-intensive for both market supervisors and leading platform orchestrators. Engaging with the implementation of vertical interoperability requirements and ex post standardisation of existing digital ecosystems is an extremely complex, cumbersome, and costly task which could face strong resistance from the firms involved. A potential way to deal with this issue would be to require technology platforms to contribute with their finances to ecosystem-tailored supervisory costs. As showed by the UK Open Banking experience, adequate implementation, team's resources and skills are crucial to achieve the pro-competitive goal of ecosystem-tailored standardisation.

Further, conceiving a workable governance and enforcement of vertical interoperability obligations requires regulators to strike a delicate balance between the interests of incumbents and newcomers while dealing with limited public resources. The UK Open Banking experience allows us once again to better understand this issue since it was originally funded by incumbent banks. As the implementation roadmap set out by the CMA was substantially completed by the end of 2022, the UK Government started considering how to ensure the necessary supervision for enforcing the continuing obligations under the CMA's Retail Banking Order to allow customers to access their

Retail Banking Market Investigation Order 2017 in Relation to Open APIs under the Open Banking Remedy” (2022)

<www.assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/106195/6/LBG_Article_12_draft_public_letter_public_version_.pdf>; UK Competition and Markets Authority, “Barclays Bank’s breaches of The Retail Banking Market Investigation Order 2017 in relation to Open APIs under the Open Banking Remedy” (2022) <<https://www.gov.uk/government/publications/cma-letter-to-barclays-about-13-breaches-of-the-retail-banking-order>>.

⁸³ See, e.g., CEN/TC 294 ‘Communication systems for meters’ <<https://standards.iteh.ai/catalog/tc/cen/8ae0124c-2738-411c-a5f8-2f7b4d5721bc/cen-tc-294>>; IEC/TC 124 ‘Wearable electronic devices and technologies’ <<https://standards.iteh.ai/catalog/tc/clc/ce8f2886-a516-44a2-a821-5f203e0add69/iec-tc-124>>; CLC/TC 79 ‘Alarm Systems’ <<https://standards.iteh.ai/catalog/tc/clc/fcccb4a0-46bd-4afd-8962-74b1acffe19b/clc-tc-79>>.

⁸⁴ <<https://csa-iot.org/all-solutions/matter/>>.

⁸⁵ <<https://www.threadgroup.org/thread-group#OurMembers>>.

⁸⁶ <<https://developer.amazon.com/en-US/alexa/voice-interoperability>>.

data securely and benefit from financial data sharing.⁸⁷ For instance, the leading industry body for financial services (i.e., UK Finance) proposed to let the nine largest banks free to withdraw from membership (and funding duties) after three years.⁸⁸ This spurred a discussion as, according to several fintech firms, such proposal would turn into an unfair leverage to manipulate the new supervisor's activity, especially when it comes to oversight of interoperability requirements and standardisation initiatives.⁸⁹

However, a substantial element differentiates our model from the UK Open Banking. Our proposal would not lead to a one-size fits all solution as the standards would be tailored to the specific features of each ecosystem. Indeed, as the IoT encompasses a wide range of heterogeneous products and services interconnected together within diverse digital ecosystems, it would not be appropriate to impose a single set of interoperability standards on the whole sector. Rather, the Open Banking paradigm could serve as a reference for delivering vertical interoperability tailored around the features of major digital ecosystems in the IoT universe. Adopting an ecosystem-based approach to standardisation would foster dynamic innovation and ecosystem diversification as platform-operators would not be bound to level their offer between each other. Moreover, interoperability could work smoothly in a vertical fashion thereby facilitating ecosystem entry by newcomers and lowering down the risk of technological self-preferencing.

Overall, our proposal is set to complement the existent EU regulatory framework filling the gaps left open by the proposed Data Act, which only addressed interoperability for cloud service providers. Further, by adopting a straightforward approach towards mandated standardization to deliver on vertical interoperability, the solution at stake also complements the DMA, which already introduced some vertical obligations for app store gatekeepers. Indeed, the DMA only provides the Commission with the ability to force SDOs to facilitate the adoption by digital gatekeepers of appropriate standards as long as this is necessary to implement vertical interoperability requirements to install third-party app stores and side load apps, and to ensure access to essential functionalities of operating systems or hardware capabilities of a specific device. Moreover, our proposal would draw on the technical toolbox recently established by the Data Governance Act. As the European Data Innovation Board (EDIB) is entrusted with the fundamental task of identifying the relevant standards and interoperability requirements for cross-sector data sharing, it could serve as a foothold for launching the implementation of ecosystem-tailored standardisation.⁹⁰

VI. Concluding remarks

The IoT is likely to bring substantial changes across a large part of worldwide economies. An increasingly high number of products require interconnection within larger networks of smart devices, therefore smooth access and interoperability with digital ecosystems are

⁸⁷ UK Competition and Markets Authority, 'Millions of customers benefit as Open Banking reaches milestone' (2023) <<https://www.gov.uk/government/news/millions-of-customers-benefit-as-open-banking-reaches-milestone>>; UK Competition and Markets Authority, 'The Future Oversight of the CMA's Open Banking Remedies' (2021) <www.gov.uk/government/consultations/future-oversight-of-the-cmas-open-banking-remedies/the-future-oversight-of-the-cmas-open-banking-remedies>.

⁸⁸ UK Finance, 'Open Banking Futures: Blueprint and Transition Plan' (2021) <www.ukfinance.org.uk/system/files/Open-Banking-Phase-II-report-FINAL.pdf>.

⁸⁹ Financial Times, 'Watchdog Criticised over Plans to Combat Dominance of Big Banks' (2021) <www.ft.com/content/c7cba98a-b8fe-415b-9cc9-bfd765b4f7d5>.

⁹⁰ Data Governance Act, *supra* note 12, Recitals 53 and 54.

essential for third parties to engage within the IoT universe. At the same time, by exerting control over the interface between final users and application developers, as well as device manufacturers, the orchestrators of these ecosystems may engage in anticompetitive behaviours and undermine the economic potential of the IoT.

To address these concerns, a wave of regulatory initiatives has progressively emerged in recent years to address the strategic role played by large platform-based digital ecosystems. In such scenario interoperability obligations are taking centre stage, promising to put an end to network effects which work only in favour of the most prominent digital ecosystem owners. However, given that interoperability is context dependent, interventions should build on a careful assessment about whether it is more desirable aiming to vertical rather than horizontal interoperability as well as relying on mandatory rather than voluntary standardisation.

Against this background, we put forward a twofold proposal. Firstly, we argue that competition-oriented reforms in the IoT should aim to deliver vertical (within ecosystem) interoperability. Horizontal (between ecosystems) interoperability would, indeed, threaten platform design and governance, thus jeopardising their business models, preventing their differentiation, and ultimately reducing incentives to innovate. Secondly, we sound a note of caution against poorly designed legislative measures that fail to address the role of standardisation for delivering interoperability. In this regard, by taking stock of the Open Banking experience, we argue that industry-led standardisation under the oversight of independent public bodies is the correct solution for tackling interoperability challenges in the IoT world. Under our proposal, leading IoT technology platform orchestrators would be expected to design open interoperability standards together with third-party providers and manufacturers. In this way, the hurdles of formal standardisation processes could be overcome while countering the risks of *de facto* standards conveniently developed under the control of large technology platforms.

By implementing ecosystem-tailored standardisation, policy makers could strike a reasonable balance between the need to ensure contestability in digital markets and the overarching goal of preserving consumer welfare and innovation.