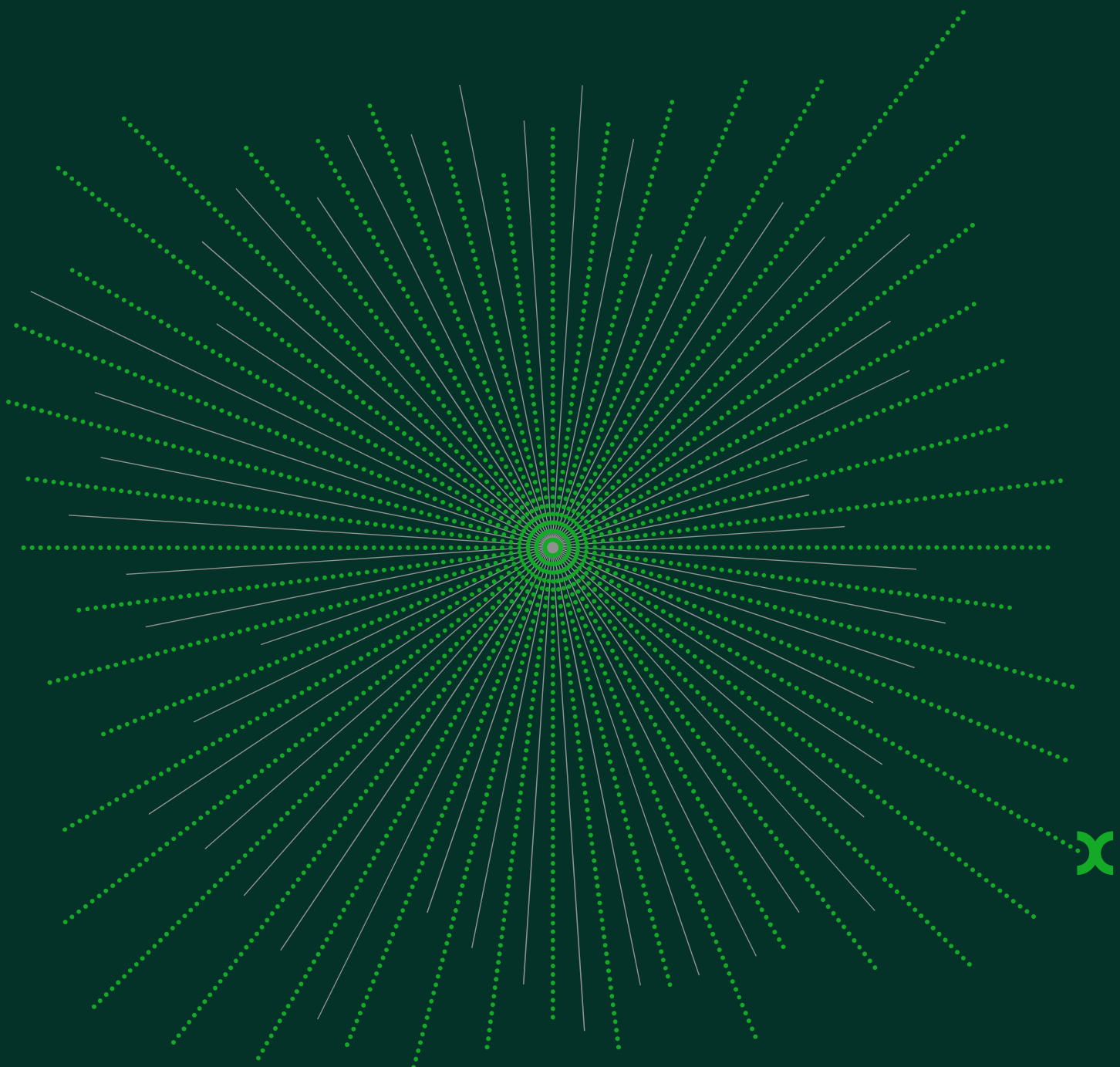
The benefits of hardware interoperability

—

In the context of Article 6(7) of the Digital Markets Act

Prepared for CODE

3 February 2025



Contents

Figures and Tables

About Oxera Consulting LLP (Oxera)

Oxera is an international economics consultancy with over 40 years of experience across sectors, geographies and jurisdictions. We build relationships with policymakers—assessing, shaping, and advising regulatory and government policy.

We have a deep understanding of the digital sectors, having been actively engaged in the debate around the future of digital regulation. We regularly publish on this topic, contribute to public consultations, and advise policymakers, regulators and businesses on issues in digital markets.

This study was commissioned and paid for by the members of CODE.

About Coalition for Open Digital Ecosystems (CODE)

CODE is a coalition of companies that believe open digital ecosystems are better for businesses, consumers and society. They aim to foster collaboration among academics, consumers, companies, policymakers and startups in a collective effort to exchange ideas that encourage and embed the principles of openness. This will, in turn, help drive a thriving European digital economy, in which consumers have more choice, technological lock-in belongs to the past, and businesses can innovate.

CODE members include: Flywallet, Garmin, Google, Honor, Lenovo, Lynx, Meta, Motorola, Nothing, Opera, Qualcomm, Vodafone and Wire.

Executive summary

Interoperability plays an important role in the digital economy and can be a key driver of innovation, competition, choice and economic growth. Hardware interoperability, in particular, enables users to seamlessly connect devices from various providers, creating benefits for consumers. However, effective interoperability can be hindered by certain barriers, and is often not implemented to its full potential, including in mobile ecosystems.

In this context, the European Union (EU) included Article 6(7) in the Digital Markets Act (DMA) to promote contestability by mandating interoperability for features controlled by designated gatekeepers' operating systems (OSs) and voice assistants (hereafter, Article 6(7)). At present, there are ongoing discussions on how specifically to achieve effective hardware interoperability under Article 6(7) of this Regulation. In particular, the EC is in the process of providing guidance to Apple on how to fulfil the interoperability obligations through two specification proceedings. These proceedings focus on several iOS connectivity features and functionalities as well as the process Apple has set up to address interoperability requests submitted by developers and third parties for iOS and iPadOS.[1]

CODE asked Oxera to analyse the benefits, barriers and potential solutions related to hardware interoperability, alongside examining how this works in practice both inside and outside the tech industry. This report develops a general framework to promote the adoption of hardware interoperability and makes specific recommendations for the effective implementation of Article 6(7). The framework recognises that hardware interoperability in many cases will be market-driven, but in particular circumstances regulatory intervention is justified, specifically where there are existing or potential market failures. Article 6(7) can be seen as such an intervention, aiming to address market failures and to make markets more contestable through mandating interoperability.

What is interoperability?

This report starts by defining hardware interoperability as the ability of different systems, products or services to work together seamlessly, reducing friction and enabling greater interaction across markets. Devices typically operate within a layered technology stack, ranging from foundational hardware to the OS, application software and connectivity features. Interoperability can occur both horizontally, within the same layer (e.g. between two devices or applications), and vertically, between different layers (e.g. between hardware and the OS). Access to certain functionalities is often provided through software interfaces, such as application programming interfaces (APIs), rather than direct access to underlying hardware components. For example, APIs can enable secure identity

[1] European Commission (2024), 'Commission starts first proceedings to specify Apple's interoperability obligations under the Digital Markets Act', 19 September, accessed 9 December 2024.

verification by interacting with a device's fingerprint scanner without granting direct access to the underlying hardware.

Success stories, benefits and barriers for hardware interoperability

We explore the benefits, challenges and ways of interacting between devices through six case studies. These case studies cover well-established applications, such as the role of interoperability in internet infrastructure, the status of interoperability in personal computers (PCs)/laptops and the mobile ecosystem, and an overview of the Internet of Things (IoT) and emerging technologies space, which currently has in place nascent initiatives for interoperability.

Hardware interoperability can offer numerous advantages, often benefitting multiple stakeholder groups simultaneously. Consumers can benefit from greater choice and competition by being able to mix and match devices from different manufacturers without compatibility issues (and therefore choose to use the devices they prefer), saving both time and money while avoiding being locked into a single ecosystem. New providers of complementary devices or services that require access to hardware find market entry more accessible with interoperability, as they do not need to build their own ecosystems from scratch. The firms providing access can use interoperability to their advantage to broaden their user bases by enabling connections with third-party devices or ecosystems, making their products appeal to a wider user base as they work seamlessly with other providers. At the same time, hardware interoperability can contribute to economic growth through efficiency, innovation and technological advancement, and sustainable development for society as a whole.

Alongside the many benefits of interoperability, our report identifies several barriers that can arise, particularly from technical, regulatory or business considerations. Technical barriers often involve challenges relating to the design, compatibility or lack of standardisation of systems, while regulatory barriers can arise from legal frameworks that limit data sharing or impose particular compliance requirements. Business barriers, conversely, are driven by firms' incentives, where companies may not choose (or resist) interoperability in order to keep certain competitive advantages, to focus on product differentiation or to exercise control over their platforms.

While these barriers need to be considered seriously, they are sometimes strategically leveraged by incumbent firms to avoid interoperability. As such, these barriers can be overstated, particularly when gatekeepers use them as justification to delay or resist interoperability. While such a strategy might benefit the individual firm, it neglects the broader benefits of interoperability, which can generate greater overall benefits than any single firm can achieve alone. This broader impact underpins the rationale for regulatory interventions such as the DMA.

A framework for promoting hardware interoperability

We have developed a set of five general principles that aim to support interoperability by balancing regulatory interventions and market-driven incentives. These five principles are as follows.

1 **Market-driven decisions**: as a general rule, in markets without substantial market failures interoperability decisions should be left to the market. In a functioning market economy, firms act in their self-interest, which generally promotes competition.
2 **Targeted policy intervention**: where vertically integrated firms control access to essential components, and the benefits of intervention outweigh the costs, public policy intervention may be justified. However, interoperability should not be mandated in cases where there is clear evidence of insurmountable security, privacy or integrity risks.
3 **From collaborative approach to regulatory intervention**: in many cases, effective interoperability may be achieved through collaboration between access providers and third parties to agree on the form and terms of access. However, where good-faith negotiations stall, or where deemed insufficient, regulators may need to intervene to determine the form and terms of access.
4 **Balanced pricing conditions**: regulators should weigh trade-offs when setting pricing for interoperability access, ensuring that gains in innovation by smaller rivals are not offset by potential reductions in innovation due to ex ante regulation.
5 **Transparent implementation**: any mandated interoperability should involve clear descriptions of the features and functionalities for which interoperability is available, including non-discriminatory access conditions as well as a fast, quick and transparent resolution process in the case of a lack of clarity or disputes.

Policy recommendations for the effective implementation of Article 6(7)

While the five-step approach outlined above is intended as a universal framework for promoting interoperability, and is flexible in application, we note that Article 6(7) represents a regulatory intervention that is broadly aligned with these principles. Specifically, principles 1 to 4 are embedded in the wording of Article 6(7), where (in short) the process of core platform services (CPS) designation has triggered the obligation to be interoperable, free of charge, and principle 5—its implementation—is now the focus of the European Commission (EC) in compliance discussions.

Drawing from the lessons on hardware interoperability across various sectors and products discussed throughout this report, we present a set of targeted recommendations for the effective implementation of Article 6(7). These recommendations focus on three critical areas, as described below.

1 **Non-discriminatory access**. By mandating effective interoperability with the same hardware and software features that are available to services or hardware provided by the gatekeeper, Article 6(7) clearly establishes the foundation for non-

discriminatory access although, in some cases, a defined approach may have to be discussed and specified before any practical implementation. There is a risk that gatekeepers offer some interoperability (by providing similar functionalities), but in a manner that still favours their own devices. To avoid this, there is a need for comprehensive, transparent API documentation, and the sharing of proprietary standards or the adoption of industry standards.

2 **Accountability and collaboration on security and integrity**. Article 6(7) acknowledges that the security and integrity of the OS being opened should not be compromised, and that gatekeepers may take strictly necessary and proportionate measures to resist interoperability, provided these are duly justified. We recommend that it be made expressly clear that the burden of proof should lie with the gatekeeper to identify security and integrity challenges and to collaborate with stakeholders to address these issues. Drawing on lessons from other industries, we consider that, in cases where there is a disagreement between parties or where these issues are not resolved in a timely manner, regulatory review of the relevant concerns may be required. There is precedent for solutions to be found including robust procedures for screening access seekers, alongside certification and verification mechanisms. However, these verification programmes should not impose undue burdens on access seekers. The gatekeeper should be obliged to provide timely decisions, offer clear reasoning, and work constructively to ensure that the process is completed efficiently.

3 **Empowering user choice**. The way that interoperability is implemented can sometimes require users to take certain actions to grant permissions. To align with the contestability objectives of Article 6(7), the way that third-party devices are presented to consumers must be carefully considered. This requires the design of clear, non-discriminatory and user-friendly choice architecture that offers equal treatment to third-party and gatekeeper devices.

The above recommendations are in line with the measures proposed by the EC in December as part of the preliminary findings of its proceedings for Apple.[2] An in-depth comparative analysis is beyond the scope of this report.

[2] European Commission (2024), 'Commission seeks feedback on the measures Apple should take to ensure interoperability under the Digital Markets Act', 19 December, accessed 10 January 2025.

1 Introduction

Interoperability is a critical component of a thriving digital economy and can be a driver of innovation, choice, competition and economic growth. [3] In particular, hardware interoperability plays a crucial role in enabling users to seamlessly access and integrate a growing number of devices from multiple providers that assist in day-to-day tasks. From connecting smartwatches to smartphones, to allowing third-party services to utilise functionalities like cameras, audio systems or Bluetooth, interoperability underpins much of the convenience and innovation that users now take for granted.

In recent years, policymakers and regulators have turned their attention to the different barriers in digital markets and the use of unfair business practices that could favour some firms over others. For example, a firm might restrict or limit access to essential platform functionalities, such as near-field-communication (NFC) technology, thereby preventing potential competitors from offering an alternative.

The EU has recently adopted new legislation to address such practices, in particular with the DMA, Article 6(7) of which includes obligations that aim to increase contestability in digital markets by mandating hardware interoperability. [4] These obligations came into effect in March 2024 and the EC is currently undertaking two specification proceedings to assist Apple in complying with its obligations under Article 6(7).[5] These proceedings are focused on ensuring that Apple provides free and effective interoperability with its hardware and software features, addressing both technical aspects, including connectivity functionalities, and procedural elements, such as transparency and fairness in responding to interoperability requests.

In this context, CODE asked Oxera to analyse the benefits of hardware interoperability and how these could be achieved through effective implementation of Article 6(7).

1.1 Scope of this report

Interoperability is a cornerstone of the EU's digital strategy. This report aims to bring an economic perspective to the subject in order to support effective policy and enforcement decision making.

[3] Hodapp, D. and Hanelt, A. (2022), 'Interoperability in the era of digital innovation: An information systems research agenda', *Journal of Information Technology*, **37**:4, pp. 407–427; EU (2024), 'Shaping Europe's digital future: Interoperability and open data', News and highlights, 13 May.
[4] EU (2022), 'Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector' (hereafter, referred to as 'DMA, Article 6(7)'.
[5] European Commission (2024), 'Commission starts first proceedings to specify Apple's interoperability obligations under the Digital Markets Act', Press release.

We focus on two main aspects. First, the ability of third-party products to access hardware features and functionalities of devices made by another company, such as the NFC chip or wireless capabilities of a smart home device. Second, the integration of hardware within another company's digital ecosystem, for example, a smartwatch functioning as part of a different firm's broader digital platform. Throughout the report, we draw on lessons from successful interoperability stories in both digital and non-digital markets and products.

In the remainder of this section, we explore the definition of interoperability. In section 2, we provide an overview of the current status of interoperability in different sectors and product types before highlighting the associated economic benefits (section 3), associated barriers and potential solutions (section 4). Section 5 introduces a framework to promote interoperability that recognises the market-driven approach and the need for intervention, while section 6 provides recommendations for how the hardware interoperability obligation in the DMA can be implemented effectively.

1.2 What is interoperability?

1.2.1 Definition

In order to discuss the nuances of interoperability, it is essential to first establish a clear definition. Interoperability has been described in various ways across reports and publications, but they all revolve around a common idea: the ability of different systems, products or services to work together.

According to the DMA, interoperability refers to 'the ability to exchange information and mutually use the information which has been exchanged through interfaces or other solutions, so that all elements of hardware or software work with other hardware and software and with users in all the ways in which they are intended to function'.[6]

The Centre on Regulation in Europe (CERRE), a leading European think tank, defines interoperability as 'the ability of different products or services to "work together," meaning that some common functionalities can be used indifferently across them, typically via appropriate information exchange'.[7] Similarly, Kerber and Schweitzer (2017) describe interoperability as 'the ability of a system, product or service to communicate and function with other (technically different) systems, products or services'.[8]

Despite the different definitions, the common link between these is the idea that interoperability allows systems to work together, ensuring they can communicate and function in coordination. This is a crucial part of the digital economy, where many systems must talk to each other. Frictions between these systems will reduce the volume and

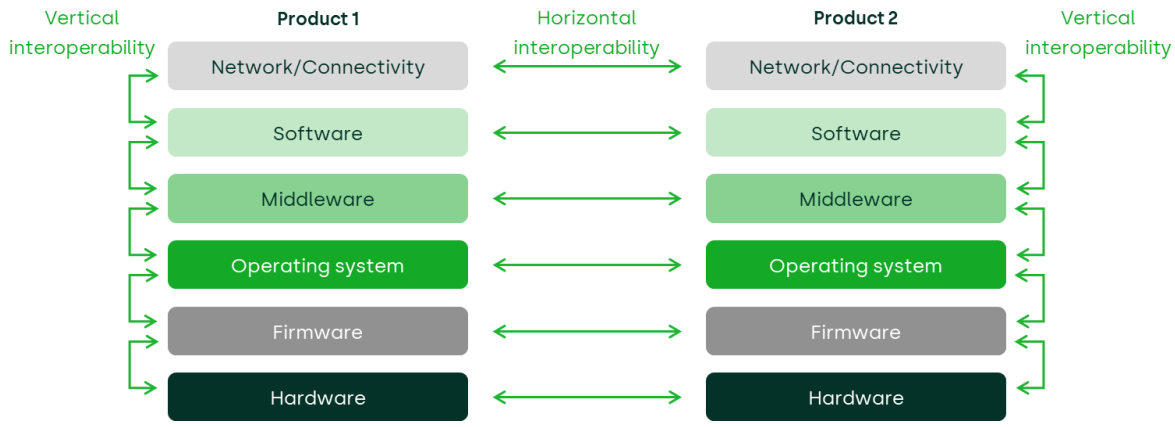
[6] DMA, Article 2(29).
[7] CERRE (2022), 'Interoperability in digital markets', March, p. 10.
[8] Kerber, W. and Schweitzer, H. (2017), 'Interoperability in the Digital Economy', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 31 January.

velocity of transactions that can take place. Interoperability connects different systems and lowers transaction costs between systems, allowing more interactions to happen.

In the context of digital interoperability, devices typically operate across a layered technology stack, as illustrated in Figure 1.1 below. Each layer serves a distinct purpose, contributing to the overall performance and interoperability of digital systems. These layers, from foundational hardware to network connectivity, are interconnected yet distinct in their roles.

- **Hardware** forms the physical foundation of the stack. It includes the tangible components of a device, such as processors, sensors and storage, and provides the infrastructure for the higher layers. Unlike other layers, hardware is fixed and requires compatibility with software and connectivity to function effectively in a broader ecosystem.
- **Firmware** is embedded software programmed into hardware to control its basic functions. It acts as a bridge between hardware and the OS, ensuring that hardware components can communicate and execute specific commands.
- **OSs** provide a platform for managing hardware and software resources. They enable user interaction and support application software by offering standardised interfaces for developers.
- **Middleware** facilitates communication and data exchange between applications and the OS or hardware. It acts as an intermediary layer that simplifies software development by managing functions such as messaging, authentication and data management. Middleware focuses on interoperability between software applications rather than direct user interaction.
- **Software** encompasses applications and programs that perform specific tasks for users. It is the most user-facing layer of the stack, ranging from productivity tools to entertainment platforms. Unlike middleware or OSs, software directly interfaces with users, relying on the underlying layers for functionality and compatibility.
- Potentially dependent on different tiers of the stack, the **connectivity functionality** ensures that devices can communicate with external systems, networks and other devices. This includes Wi-Fi, Bluetooth, NFC and other protocols that enable data transfer and remote interactions. Unlike the other layers, connectivity enables a device to interact with external networks, allowing integration within a larger digital ecosystem of devices.

Figure 1.1 Illustration of interoperability in a digital 'tech stack'



Source: Oxera, adapted from CERRE (2022), 'Interoperability in digital markets', March, p. 10.

Together, these layers enable interoperability, which can be horizontal—across devices—or vertical—within a single device's technology stack.

Horizontal interoperability occurs when competing products at the same level of the value chain can work with one another. These products are usually substitutes and compete in the same market—for instance, smart lightbulbs made by two competing manufacturers but operating within the smart home system. Horizontal interoperability can enable platforms to share direct network effects, increasing the overall network size and reducing barriers to entry for smaller competitors.

On the other hand, vertical interoperability involves complementary systems at different levels of the value chain. This can be either:

- within-platform vertical interoperability, where a platform allows third-party developers to create complementary services within their platform (e.g. video game consoles allowing developers to build games for the platform); or
- cross-platform vertical interoperability, where third-party developers can also supply their complementary services on other platforms (e.g. if video games developed for one console could also work on another console).

The concept of horizontal and vertical interoperability is illustrated in Figure 1.1. Each stack represents a digital product; for example, two stacks could represent two smartphones, or one stack could represent a smartphone while the other represents a VR headset.

These stacks are considered horizontally interoperable if they can interoperate at the same level in the stack (e.g. in the hardware layer through a physical connecting cable). In contrast, vertical interoperability occurs between the layers of the same stack. For instance, interoperability may exist between the hardware and firmware levels of a

smartphone stack, where specific firmware is designed to optimise the performance of the hardware components. Effective hardware interoperability often relies on compatible APIs at other levels, such as software or OSs, to enable smooth functionality across devices. It is important to note that interoperability can span multiple layers, extending from hardware all the way up to software.

1.2.2 Levels of interoperability

Interoperability can be understood on a spectrum, with four key levels ranging from the most basic level of interoperability to the most advanced, as seen in Figure 1.2 below. Each level of interoperability builds on the one before it.

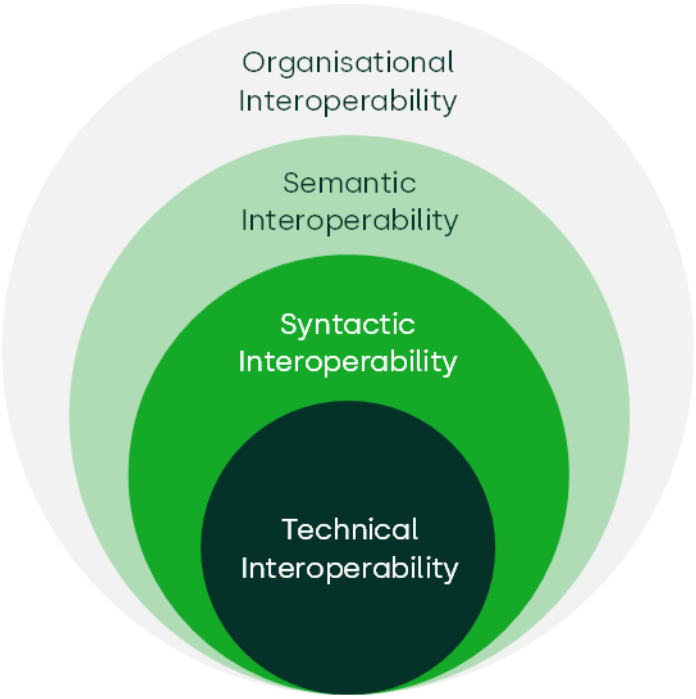
The first, and most basic level, is **technical interoperability**, which refers to the ability of systems to connect and communicate using standard communication protocols and supporting infrastructure. Universal Serial Bus (USB) standards are a prime example of technical interoperability, as they provide a universal protocol enabling a wide range of devices—such as keyboards, external drives and printers—to connect to computers and transfer data seamlessly. It ensures basic communication without requiring further alignment on data format or meaning.

The second level, **syntactic interoperability**, goes beyond mere connection and addresses the format and structure of the data being exchanged. Bluetooth pairing illustrates this level, as it enables devices like wireless headphones and smartphones to exchange structured data such as audio signals or command instructions in a pre-defined format. This represents syntactic interoperability because it ensures that the devices can process and interpret the structured data correctly to provide the intended functionality.

At the third level, **semantic interoperability** ensures that systems not only understand the data format but also the meaning of the information being exchanged. Smart home ecosystems are a good example, as devices like smart speakers, thermostats and lighting systems must share a common understanding of commands and concepts—such as 'turn off the lights' or 'set the temperature to 22 degrees'—to function seamlessly. This fits the category because it demonstrates how a shared interpretation of terms and commands enables meaningful interaction across devices.

Finally, the highest level of interoperability is **organisational interoperability**. This involves different organisations being able to effectively exchange information, even if they are using distinct systems or infrastructures, or operating in different geographic or cultural contexts. For example, in disaster response, multiple agencies (e.g. local governments, international NGOs) collaborate and share data across different systems to achieve a common goal. While this level is highly relevant in contexts requiring cross-organisation coordination, it is less relevant to hardware interoperability.

Figure 1.2 The four levels of interoperability



Source: Oxera, adapted from Serrano, M., Barnaghi, P., Carrez, F., Cousin, P., Vermesan, O. and Friess, P. (2015), 'IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps', March.

A related, but distinct, concept is data portability, which is also referred to in the DMA.[9] This refers to users' ability to transfer their data from one service or platform to another.

We note that data portability and interoperability are distinct, but related concepts. Data portability is user-driven, meaning it empowers individuals to move their data freely between services, promoting user control and competition. Interoperability, on the other hand, is more market-driven, focusing on the seamless integration of systems and services to enable them to work together. However, these concepts are interrelated in that data portability requires some degree of interoperability between different data formats. In this case, at least syntactic and semantic interoperability are needed. Systems must understand and process exported data in a meaningful way. However, data portability does not require full interoperability for data-porting obligations to be met.

[9] In particular, in Article 6(9), which we discuss further in footnote 99.

1.3 The relationship between hardware and software interoperability

Effective hardware interoperability often relies on complementary interoperability at other levels, such as software or OS interoperability, to ensure that hardware functionalities can operate smoothly. Hardware interoperability requires an interface to enable information exchange, which can occur at different levels of the technology stack.

For example, in smartphones, the OS plays a crucial role in enabling interoperability by managing the interaction between hardware and software resources. Access to certain functionalities can often be provided through software interfaces, such as APIs, rather than direct access to hardware components. For instance, APIs can facilitate secure identity verification by interfacing with the device's fingerprint scanner without granting direct access to the underlying hardware.

In this report, we take a comprehensive view of interoperability, recognising the interdependence of hardware and software layers and the importance of addressing barriers to interoperability beyond the hardware layer alone.

2 Success stories and ongoing developments in hardware interoperability

Interoperability can act as a driver of innovation and economic growth across a variety of industries. From telecoms, consumer electronics and the IoT, the ability of products, services and systems to interconnect and work together seamlessly has been a key enabler of thriving ecosystems. Examples such as the internet, the USB, Wi-Fi and Bluetooth demonstrate how hardware interoperability can lead to significant economic benefits, stimulate growth, encourage vibrant competition and expand consumer choice.

In this section, we present six case studies across different industries to highlight how interoperability can shape industries, facilitate collaboration and unlock innovation. We highlight instances where interoperability has succeeded in delivering these benefits, offering lessons for future applications, as well as cases where interoperability has so far been less successful. These include an overview of the role of hardware interoperability in: (i) the emergence of the internet infrastructure; (ii) PCs/laptops; (iii) IoT for smart homes; (iv) IoT for industry devices; (v) mobile ecosystems; and (iv) emerging technologies. Across these case studies, common themes emerge to characterise the state of interoperability.

First, hardware interoperability often fosters collaborative growth models, where interconnected systems allow different stakeholders to benefit from a shared ecosystem. Through common standards, markets can grow and become more inclusive, enabling participants to access a broader range of customers, partners and opportunities. This collaborative approach allows for organic growth, as participants contribute to and benefit from a larger, interconnected system. These benefits are also discussed in sections 3.2 and 3.3.

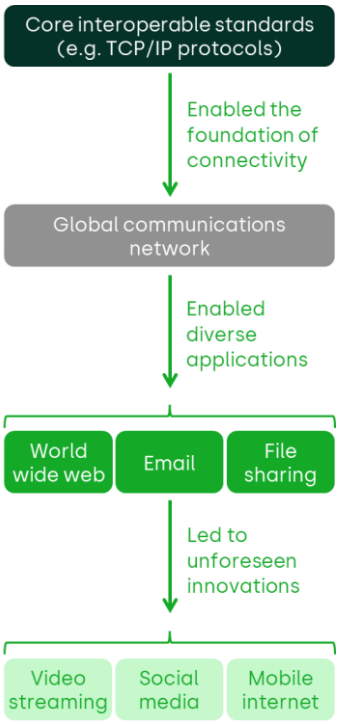
Second, interoperability has positive spillover effects, creating benefits and enabling innovations far beyond its original purpose. For instance, the internet's basic protocols and the wide adoption of PCs and laptops paved the way for applications such as e-commerce, video streaming and social media, which were not part of its initial design. This highlights how interoperability can act as a platform for unforeseen advancements, generating economic and social value over time.

Third, hardware interoperability can take time to develop and requires buy-in from multiple stakeholders. When incentives are aligned, interoperability can be established quickly as multiple parties join an initiative. However, there are also cases where interoperability is currently underdelivered—for example, in mobile ecosystems, smart homes, industrial IoT or emerging technologies—due to a variety of barriers. In the case of technologies where there is no incumbent technology or firm through which access is required in order to reach consumers or enable functionality, market forces are already in play to address these, but in other cases, where progress has been slow, there may be a role for regulators to intervene to help overcome the barriers (see sections 4 and 6).

2.1 Role of interoperability in the internet infrastructure

Box 2.1 Case study: the growth of the internet and the role of interoperability

The origins of the internet can be traced back to the late 1960s when two US universities, funded by the Advanced Research Projects Agency (ARPA, later DARPA), successfully connected their computers. This was the beginning of a larger vision to create a network of computers that could communicate across different institutions. By the 1970s, this network, known as ARPANET, was driven by the needs of academic institutions and the US government and military organisations to share data more efficiently, expanding as more universities joined. It was also largely funded by the US government and the military, with initial purposes focusing on academic and secure communications.



As ARPANET grew, it became clear that future needs would involve more than just connecting US institutions. When other countries and institutions joined the network, there was a realisation that a 'network of networks'—the 'internet'—was necessary. This led to the development of the transmission control protocol (TCP), which allowed data to be split into packets and reassembled at its destination, and the internet protocol (IP), a system of unique addresses to identify where information should be sent. These technologies were crucial in making the internet scalable and globally accessible, as packets could travel via any available route, making it easy to expand across geographic boundaries.

Unlike the telephone networks, which were centrally planned and controlled from the outset, the internet grew organically, driven by the needs of its users. Protocols like TCP/IP were developed as and when needed. The network expanded slowly throughout the 1970s and 1980s, eventually gaining momentum with the introduction of the PC in the early 1980s and Tim Berners-Lee's World Wide Web in 1989. By 1993, the internet had around a million users. However, because the internet's growth was piecemeal, its early designers did not fully anticipate the scale it would reach. For example, the limit set for IP addresses (originally very few and then expanded to 4bn—an inconceivable amount at the time) was thought to be sufficient, but that assumption has since been proven wrong, necessitating the introduction of IPv6 to address future demands.

By the late 1990s, control of the internet had transitioned from government oversight to the private sector, with organisations like the Internet Engineering Task Force and the Internet Society guiding its standards. Around this time, there were approximately 10,000 internet service providers, portals like AOL and Yahoo! thrived on advertising revenue, e-commerce and email started to expand and search engines started to emerge. The introduction of smartphones, notably the iPhone in 2007, significantly accelerated global internet usage, with a new focus on services such as social networks or video streaming.

The expansion of wireless and mobile internet enabled unforeseen innovations and wearable devices that function seamlessly while connecting users to the wider internet. And this expansion continues as the structure of the internet develops further.

Source: Oxera based on Ball, J. (2020), *The system: who owns the internet, and how it owns us*, Bloomsbury Publishing; Britannica (2024), 'Foundation of the Internet', accessed 8 November 2024.

2.2 PCs/laptops

Box 2.2 Case study: the PCs and laptops industry

PCs and laptops are essential for both private and professional activities, requiring seamless compatibility with a wide range of peripheral devices. This interoperability enables users to connect and operate various external devices with ease, significantly enhancing the user experience. Historically, the interoperability of PCs and laptops with peripherals has relied on the adoption of universal standards. Key technologies include the following.

- USB: introduced in the mid-1990s, USB quickly became a universal standard for connecting peripherals. Its evolution from USB 1.0 to USB-C significantly improved speed, power delivery and device compatibility, enabling integration with external drives, docking stations and advanced audio-visual equipment.
- High-Definition Multimedia Interface (HDMI): a standard for high-definition video and audio, HDMI enabled laptops to connect seamlessly with external displays, projectors and sound systems, facilitating both personal entertainment and professional presentations.
- Bluetooth: the development of Bluetooth enabled wireless connectivity with devices such as keyboards, headphones and even musical instruments, eliminating the need for physical cables and expanding user flexibility.

Thus, laptops have adapted to a growing hardware ecosystem, with widespread compatibility that benefits both consumers and new entrants in the market. Consumers can upgrade or replace components easily, and manufacturers face competitive pressure to innovate.

However, in recent years, there has been an increase in the number of instances where non-physical connections—such as wireless technologies—have led to a lower degree of interoperability. Wi-Fi-based functionalities such as screen mirroring or file sharing often encounter limitations when attempting to connect devices across ecosystems. For instance, Apple's AirDrop offers peer-to-peer file sharing within the Apple ecosystem, but does not support cross-brand compatibility at the same level. Furthermore, major OS updates can bring stricter driver requirements, which enable data transmission between peripheral devices and the PC or laptop. These restrictions may arise from outdated firmware, leading to the failed recognition of certain mouses, headphones, keyboards or other hardware accessories. These limitations stem from proprietary components layered on top of standardised protocols, designed to create competitive differentiation while restricting full interoperability. Despite these challenges, the PC and laptop market continues to maintain a high level of interoperability across hardware, largely due to widespread adoption of open standards.

Source: Oxera based on Passingham, M. (2024), 'USB, HDMI and more: the ultimate guide to computer ports', *Which?*, 25 September, accessed 9 December 2024.

2.3 Smart homes

Box 2.3 Case study: the smart homes industry

Smart homes integrate various devices, such as speakers, cameras, thermostats and security systems, requiring interoperability to function within a unified system, often managed through a smartphone or in-home network. Unlike traditional appliances, smart home technologies depend on cross-functional compatibility, which must span across brands and platforms.

However, achieving this can be challenging, as many devices remain incompatible with competing ecosystems, which have a diversity of technical interfaces. Consumers are often forced to commit to a single platform or incur additional costs to manage multiple systems. There are other concerns about network limitations and security vulnerabilities, which may need improvements in Wi-Fi infrastructures with more advanced routers or extenders to hubs that centralise and verify communication in a secure way.

This lack of universal compatibility creates barriers for both consumers and manufacturers. Consumers face restricted choices and higher costs to maintain devices across ecosystems, while manufacturers must either specialise in a single platform or develop multiple versions of their products to meet different connectivity standards, security requirements and customer support expectations. These challenges increase risks for the parties that seek smart home interoperability, limiting innovation and adoption of smart home technologies.

To address these issues, industry participants have started to introduce some initiatives to improve IoT interoperability. For example, Matter is a vendor-neutral standard designed to unify smart home ecosystems. Matter creates a local wireless network that enables direct device-to-device communication, enhancing the responsiveness and reliability of connected devices. Its robust certification programme ensures interoperability between devices from different manufacturers, providing a clear pathway towards seamless smart home integration.

At the same time, users have a significant role to play in managing their devices. They can enhance and ensure secure interoperability through strong mechanisms for passwords and active management of network permissions.

Source: Oxera based on Neidig, S. (2022), 'How Matter Addresses Interoperability Issues in Smart Home Devices', *All About Circuits*, accessed 9 December 2024.

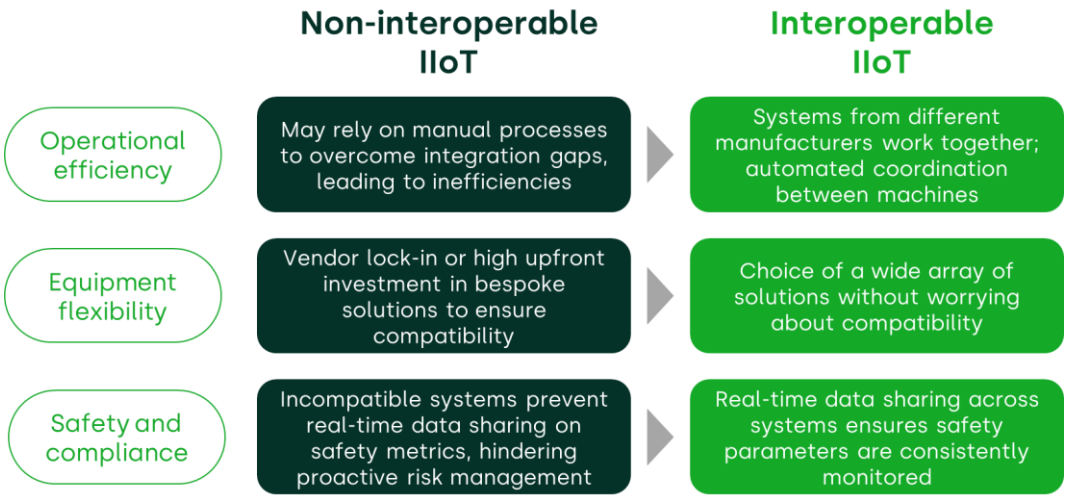
2.4 Industry IoT devices

Box 2.4 Case study: industrial applications of IoT devices

The Industrial Internet of Things (IIoT) is transforming manufacturing and industrial sectors, with the market for IIoT devices and technologies projected to grow from USD 77.3bn in 2020 to USD 110.6bn by 2025. This growth is driven by the adoption of advanced technologies that connect machines, devices and systems across industries such as aerospace, automotive, photovoltaic engineering and warehouse robotics. However, achieving interoperability within IIoT ecosystems remains a critical challenge.

The industrial sector currently lacks widespread universal interoperability frameworks. Manufacturing processes vary significantly across industries, and there are no unified standards for smart industrial sensors or data sharing between machines from different vendors. For example, transferring operational data between machines in one ecosystem may not align with processes in another, creating inefficiencies and integration barriers.

Emerging standards, such as the MassRobotics AMR Interoperability Standard, offer promising solutions. This standard enables autonomous mobile robots (AMRs) from different manufacturers to share basic operational information, such as locations and tasks, allowing them to work together on the same factory floor. This interoperability could enable benefits such as improved efficiency, reduced downtime, enhanced scalability and greater flexibility in adopting cutting-edge technologies across industries.



Source: Oxera based on Choi, K. (2023), 'What Is the MassRobotics AMR Interoperability Standard?', *Mass Robotics*, 19 June, accessed 9 December 2024; Volansys (2020), 'How Industrial IoT (IIoT) is transforming the Manufacturing Industry', 29 October, accessed 9 December 2024.

2.5 Mobile ecosystems

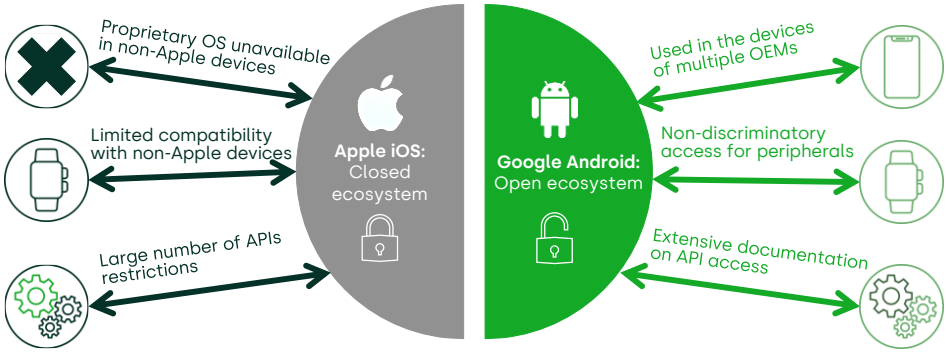
Box 2.5 Case study: the mobile ecosystems and the role of smartphones

Smartphones have become central to users' lives, serving as the gateway for activities, from managing personal data and communication to engaging with a variety of applications such as health, payments and entertainment. Users expect their devices to pair smoothly with their smartphone, using appropriate channels and functionality and to seamlessly coordinate in the background to allow peripheral control. To deliver these functionalities, smartphones must interoperate with networks, peripherals and auxiliary devices. However, interoperability issues persist, limiting connectivity and functionality across platforms and devices. The EC has taken steps to address these challenges through Article 6(7), which aims to promote greater openness and competition in the digital market by endorsing interoperability in OSs that the EC has designated as CPSs under the DMA.

A key aspect of the interoperability debate lies in the contrasting approaches taken by the two largest mobile ecosystems: Android and iOS. Android, with its open-source model, fosters a more flexible and interoperable ecosystem, allowing a broad range of devices, peripherals and applications to connect and operate across platforms. In contrast, Apple's closed ecosystem restricts the integration of third-party devices and services, often limiting interoperability to Apple's proprietary devices and apps through the technological interface (e.g. AirPlay) or through restricting the APIs available to third parties. This model reinforces Apple's control over its user experience, but also creates barriers to seamless cross-platform compatibility, degrading the user experience.

Additionally, Apple only opened NFC capabilities to third-party developers through iOS 18.1 as of October 2024. This move provides essential APIs for the evolution of business-to-consumer interaction in systems for digital identification, payments and ticket management. The removal of the traditional wired headphone jack posed another problem for smartphone interoperability. The users who still preferred wired connections faced increased costs due to the need for adaptors, whereas those seeking wireless headphones often found issues arising from different latencies and Bluetooth bandwidth limitations. Looking forward, enabling innovative use cases in the mobile ecosystem depends on first ensuring that key functionality and information currently available to the OS owner's own peripheral devices are also accessible to third-party developers. Following this, more exciting and innovative use cases can be contemplated by a wider number of providers.

Therefore, the central role of smartphones not only shapes how consumers engage with the digital world, but also places smartphone manufacturers in a position of influence and power as other devices depend on them for functionality and connectivity.



Source: Oxera based on Competition and Markets Authority (2022), 'Mobile ecosystems: Market study final report', 10 June.

2.6 Emerging technologies

Box 2.6 Case study: emerging technologies

Several technologies are still in their formative stages, but offer significant potential for the future of hardware interoperability. Among these are Augmented/Virtual/Extended Reality (AR/VR/XR), AI-specialised chips and 5G network slicing. Interoperable approaches in their development can potentially deliver important benefits for users and providers in the future.

The AR/VR/XR industry has progressed towards wired connectivity with third-party devices and platforms, enabling interoperable solutions for gaming and entertainment purposes. Despite some royalty-free standards introduced by the OpenXR initiative, wireless connections remain an area to be addressed since current methods lead to high latency and the need for various adaptors. The XREAL Air headset is noteworthy due to its accessible HDMI and USB-C connections to PCs and gaming consoles. However, its wireless capabilities are more limited and current software solutions are not equally functional across OS.

AI-specialised chips and processors could represent the next significant stage of hardware innovation. Providers such as NVIDIA and BrainChip are currently developing proprietary architectures tailored to different applications such as AI training and low-power processing. While this approach is optimising short-term performance, long-term prospects would considerably benefit from interoperability. As the industry matures, implementing standards and promoting collaboration could enable broader compatibility to drive AI-oriented innovation with reduced reliance on vendor-specific approaches.

5G network slicing could potentially offer another transformative approach to connectivity through multiple virtual networks sharing the same physical infrastructure. 'Slices' of these networks would be allocated dynamically to specific applications or services to improve efficiency and performance, while maintaining consistency with non-discrimination and other open internet principles. Providing clear regulatory guidelines at an EU level on how network slicing can be deployed and used consistently with the Open Internet Regulation will help foster innovation for consumers, whilst ensuring open internet principles. In particular, Ofcom has proposed approaches compatible with these principles to support these developments (compatible with UK law) and CERRE has also advised how to facilitate this in the EU.

Overall, hardware interoperability could be crucial in the development of these emerging technologies. By embracing openness and standardisation, these industries can improve accessibility, enhance functionality, ensure long-term sustainability and achieve broader market adoption across diverse sectors.

Source: Oxera based on The Khronos Group (2016), 'OpenXR Overview', accessed 29 November 2024; XREAL (2023), 'Building Augmented Reality for Everyone', accessed 27 November 2024; Hollister, S. (2024), 'Nvidia reveals Blackwell B200 GPU, the 'world's most powerful chip' for AI', The Verge, accessed 25 November 2024; BrainChip (2024), 'BrainChip Introduces Lowest-Power AI Acceleration Co-Processor', accessed 25 November 2024; SDxCentral (2020), 'What Is 5G Network Slicing?', accessed 26 November 2024; CERRE (2024), 'Ideas for the Future of European Telecommunications Regulations', September; Ofcom (2022), 'Statement: Net Neutrality Review', October.

3 The economic benefits of hardware interoperability

This section explores the diverse, significant benefits from hardware interoperability across multiple stakeholder groups—including end-users, producers of complementary devices, main access providers and the wider economy. As Gasser (2015) notes, the goal is not just to maximise compatible connections, but to create societal value through innovation, competition, choice and accessibility.[10]

There can be many advantages from hardware interoperability, often overlapping across different stakeholder groups. For instance, firms could broaden their user bases by enabling connections with third-party ecosystems, making their products more appealing as they work seamlessly with others.[11] Users benefit by being able to mix and match devices from different manufacturers without compatibility issues, saving time and money while avoiding being locked into a single ecosystem.[12] New providers of complementary devices find market entry more accessible, since they do not need to build their own ecosystems from scratch and increase competition in the downstream markets.[13]

These positive outcomes can lead to faster adoption of new technologies and greater digitalisation, opening avenues for advancements and business innovations in the wider economy.[14] Various case studies demonstrate these benefits through the creation of new product lines, the widespread adoption of standards, and the formation of long-lasting partnerships. We expand on the benefits for each group of stakeholders below.

3.1 For users

Users are the owners or operators of hardware for a variety of purposes, such as communication, leisure, work or administration. For them, three key benefits of hardware interoperability are improved experience, reduced transaction costs and increased choice.

3.1.1 Improved user experience

An improved user experience consists of the ability to seamlessly connect and use different devices without significantly exerting effort or facing compatibility issues. Interoperable

[10] Gasser, U. (2015), 'Interoperability in the Digital Ecosystem', *The Berkman Center for Internet & Society at Harvard Law School*, 6 July.
[11] Hey, F. (2024). 'Data interoperability and portability in the DMA: Competition booster or lame duck?', *Institute of Economics of the Ilmenau University of Technology*, **29**:192.
[12] Chen, P. and Hitt, L. (2006), 'Information technology and switching costs'. *Handbook on economics and Information Systems*, December, pp. 437–470.
[13] Morton, F., Crawford, G., Crémer, J., Dinielli, D., Fletcher, A., Heidhues, P. and Schnitzer, M. (2023), 'Equitable Interoperability: The "Supertool" of Digital Platform Governance', *Yale Journal on Regulation*, **40**:1013.
[14] Gasser, U. and Palfrey, J. (2007), 'Breaking down digital barriers: When and how ICT interoperability drives innovation', *The Berkman Center for Internet & Society at Harvard Law School*, November.

solutions aim to make technology more convenient and functional by reducing the obstacles that users often face.[15]

These frictions are the setbacks that occur when devices lack compatibility.[16] For example, when a user is operating multiple devices, straightforward mechanisms to complete tasks can be vital to support their experience. Whether the goal is transferring data, printing documents or connecting peripherals, hardware interoperability can enable users to save time and increase the ease of using devices, which is likely to improve their productivity.[17]

Economically, interoperable devices help users spend less effort troubleshooting and more time actually using the technology. Likewise, they can more easily replace incompatible devices and customise their personal home or work ecosystems for various needs without additional set-up complications. This flexibility is also valuable in shared environments, such as families or workplaces with a mix of devices, where borrowing cables may become necessary due to unexpected failures. The overall satisfaction of users is increased, and they can get the most out of their technology investments.

3.1.2 Reduced search and transaction costs

Interoperable hardware interfaces allow users to seamlessly integrate new components and workflows into their working practices. This helps to avoid the often time-consuming and costly process of searching for components compatible with manufacturer-specific ecosystems.[18] For example, as described in section 2.2, USB proved to be a major advance in impactful hardware standards by providing universal charging ports, helping users avoid the need for specialised adaptors or cables for different devices.[19] Moreover, by choosing interoperable devices, users do not suffer inefficiencies from an excess of cables when organising their physical workplace, and they can also move or travel more easily.[20]

Interoperability ensures that when users wish to modify their setups, they only incur the direct cost of replacing the specific component they want to change. For instance, if a user wants to replace their headphones, they can choose any brand that supports the same universal standards, such as Bluetooth connectivity.[21] Without such solutions, users might

[15] Elmi, Y. (2023), 'Interoperable IoT Devices and Systems for Smart Homes: A Data Analytics Approach to Enhance User Experience and Energy Efficiency', *Journal of Digitainability, Realism & Mastery*, **2**:10, pp. 51–66.
[16] Yang, Y. (2024), 'Technical Challenges Affecting the Popularization of Virtual Reality Technology', *International Conference on Mechanics, Electronics Engineering and Automation*, September, pp. 261–272.
[17] Zhu, F. (2024), 'Dedicated Product Integration in the Era of AI: The Case of the AI Copilot Key', Harvard Business School, September; A clearer example regarding wireless data transfer is presented in Box 3.1.
[18] Capgemini Research Institute (2024), 'Connected products: Enhancing consumers' lives with technology', accessed 22 November 2024.
[19] Intel (2015), 'Two decades of "plug and play" How USB became the most successful interface in the history of computing', accessed 8 November 2024.
[20] Smirniotis, M. (2019), 'Why You Should Switch to USB-C Fast Charging Now', *The New York Times*, accessed 22 November 2024.
[21] Falco, J. (2017), 'BaseRock Bluetooth: Bi-directional Bluetooth and 3.5 mm Headphone Jack Compatibility Device', *Electrical Engineering Department of the California Polytechnic State University*, Spring.

need to purchase additional adaptors or replace their devices to ensure compatibility. Given that these investments are supplementary to the device itself, the increased costs could become a burden.[22] However, interoperable hardware facilitates straightforward decision-making for users by eliminating the need to make these additional purchases.[23]

3.1.3 Increased choice

Users may prefer to mix and match devices from different manufacturers without being locked into a single ecosystem.[24] To illustrate, a particular user may prefer a smartphone from one manufacturer for its excellent camera, a smartwatch from another manufacturer for its fitness tracking features, and headphones from yet another manufacturer for their superior sound quality. Interoperability between these devices could allow the user to seamlessly integrate them, enhancing their choice prospects to seek the best options from various vendors to suit their individual needs. One example of this benefit is seen in the Ring and Lorex smart home security systems, which are compatible with different systems, such as Alexa, Google Home and smartphones. Due to their widespread interoperability, users are able to choose the devices they prefer without worrying about compatibility.[25]

When compatibility is limited to a single provider's products, users may face long-term difficulties in modifying their setups. In the example above, if the smartphone user had already invested in a non-interoperable alternative, their choice of compatible smartwatches and headphones would be reduced. The need to replace functional devices to ensure compatibility would incur additional expenses. Even if the long-term benefits of migrating to an interoperable ecosystem outweigh the immediate monetary costs of switching, such an investment may fall outside the budget of many users. They may be reluctant to switch, effectively reducing their choices and keeping them locked in to one ecosystem.[26]

Hence, interoperability offers greater flexibility by allowing users to choose from a wide array of devices from multiple vendors. Purchasing barriers are effectively reduced, fostering more dynamic markets where manufacturers strive to offer the best possible value and users choose according to their individual needs.[27]

[22] Kerber, W. and Schweitzer, H. (2017), 'Interoperability in the Digital Economy', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 31 January.
[23] Choi, S. and Whinston, B. (2000), 'Benefits and requirements for interoperability in the electronic marketplace', *Technology in Society*, **22**:1, January, pp. 33–44.
[24] Chen, P. and Hitt, L. (2006). 'Information technology and switching costs', *Handbook on Economics and Information Systems*, December, pp. 437–470.
[25] Oxera based on Ring (2014), 'Ring: Home Security Systems – Cameras, Alarms, Doorbells', accessed 7 November 2024; Lorex (2024), 'Lorex: Security Cameras - Home Security Camera Systems', accessed 14 November 2024.
[26] Kerber, W. and Schweitzer, H. (2017), 'Interoperability in the Digital Economy', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 31 January.
[27] Choi, S. and Whinston, B. (2000), 'Benefits and requirements for interoperability in the electronic marketplace', *Technology in Society*, **22**:1, January, pp. 33–44.

Box 3.1 Case study: user benefits from Quick Share as a data-transfer method

Nowadays, users are demanding faster, more reliable methods to share files between wider device ecosystems. Fewer clicks, greater reach and independence of internet connectivity are the envisioned features, especially when users are in physical proximity. Exclusively using Bluetooth is problematic due to its insufficient bandwidth for faster, larger transfers. Similarly, transferring data through the internet using Wi-Fi alone is dependent on strong internet connectivity that might not always be available to a user.

To address users' need to be able to transfer data between devices, Apple introduced AirDrop, initially for macOS in 2011 and then for the entire iOS ecosystem in 2013. Without requiring internet access, it uses Bluetooth connections and low latency wireless links to create a high-speed Wi-Fi peer-to-peer network between Apple devices. It provides security through a firewall and Transport Layer Security (TLS) encryption. However, this seamless file transfer mechanism does not support connections with devices from other manufacturers.

Pursuing a similar yet more interoperable solution, Android released Nearby Share in 2020, with full compatibility between Android devices of version 6.0 or greater. Samsung recently took the initiative to collaborate with Google to rebrand Nearby Share as Quick Share, expanding the compatibility of this seamless file transfer utility to Chrome OS (version 91 onwards) and Windows computers (64-bit-based version 10 onwards).

Facilitating these powerful, user-friendly solutions for users led to significant time savings and operational efficiencies from which both Android and Windows users benefit. In contrast to Apple's closed solution, Quick Share opens this feature for seamless functionality for users of devices from multiple manufacturers.

Source: Oxera based on Itani, M. (2023), 'AirDrop ultimate guide: Everything you need to know about Apple's file transfer solution', XDA, accessed 22 November 2024; Taylor, C. (2020), 'Apple Wireless Direct Link (AWLD)', CyberHoot, accessed 29 November 2024; Banerjee, A. (2024), 'What is Nearby Share and how to get started with it', Android Authority, accessed 4 November 2024; Samat, S. (2024), 'What we announced at CES 2024', The Keyword, accessed 4 November 2024.

3.2 For complementary-device providers

Complementary-device providers could find substantial advantages from the existence and promotion of hardware interoperability channels. Specifically, they benefit from an increased market reach, savings in production costs, flexibility in supply chains, quicker market entry and greater focus on product differentiation unrelated to compatibility.

3.2.1 Faster time to market and increased market reach

Interoperability can allow new companies to enter markets more easily by leveraging a hardware standard to make their products compatible with more devices. This helps them reach a broader audience from the start, without requiring users to possess devices from a specific ecosystem.[28]

In addition to accelerating market growth, interoperability could help entrants form strategic partnerships with larger firms, producing the devices they wish to complement. The complementor can benefit from the latter, promoting not only their compatibility but also unique features in which their existing user base may be interested.[29] For instance, the smart lighting products from Kasa Smart and Geeni integrate seamlessly into leading voice assistant ecosystems such as Alexa and Google Home, as well as iOS and Android smartphones. Without needing to develop proprietary technology for controlling the smart appliances, these young firms market directly to voice assistant and smartphone users, who in turn gain trust through their existing association with the latter, more established brands. [30] This mutually beneficial relationship enables entrants to thrive while strengthening the ecosystem of the access provider.

Markets embracing interoperability could attract faster innovators in the downstream market due to reduced barriers to entry. Complementors could then focus more on enhancing product features and quality instead of dedicating additional expenditures to matching or creating compatibility with proprietary systems that have different rules. Common industry standards could make entry more straightforward and quicker, fostering a more competitive environment for complementors.[31]

3.2.2 Production cost savings encourage device differentiation

Adjusting product designs for different hardware ecosystems can be a significant source of operational costs and inefficiencies for providers of complementary devices. They would often need to create various hardware specifications, employ teams with different skill sets and set up multiple procurement processes to cover a wider range of products.[32] When enabled through standardisation, interoperability eliminates this need and facilitates access to hardware features and data for these manufacturers. In turn, they can achieve economies of scale and scope by streamlining production into a more unified process.[33]

[28] Hey, F. (2024), 'Data interoperability and portability in the DMA: Competition booster or lame duck?', *Institute of Economics of the Ilmenau University of Technology*, **29**:192.
[29] Axiado (2023), 'Axiado Launches AI Security Platform Featuring OCP Compliant Modules, Strategic Software Alliances, and Premier System Partners', accessed 28 November 2024.
[30] Oxera based on Kasa Smart (2020), 'Kasa Smart', accessed 8 November 2024; Geeni (2017), 'Geeni', accessed 8 November 2024.
[31] Morton, F., Crawford, G., Crémer, J., Dinielli, D., Fletcher, A., Heidhues, P. and Schnitzer, M. (2023), 'Equitable Interoperability: The "Supertool" of Digital Platform Governance'. *Yale Journal on Regulation*, **40**:1013.
[32] Box 3.2 exemplifies how interoperability can mitigate this problem.
[33] Elmi, Y. (2023), 'Interoperable IoT Devices and Systems for Smart Homes: A Data Analytics Approach to Enhance User Experience and Energy Efficiency', *Journal of Digitainability, Realism & Mastery*, **2**:10, pp. 51–66.

With interoperability, adopting new technologies becomes easier, potentially enabling manufacturers to develop one-size-fits-all (or at least many) solutions. Complementary-device providers can confidently advertise broader compatibility ranges for their products, reducing the necessity to specialise production lines for different ecosystems from external manufacturers. This means that they can boost their productivity and focus resources on enhancing product features, quality and purposes rather than dealing with compatibility issues.[34]

By reducing the complexity associated with multiple connector specifications and compatibility decisions, interoperability can incentivise providers to innovate and diversify their product offerings. They can cater to consumers with different needs and preferences, adding value without the limitations imposed by closed ecosystems. This could encourage device differentiation, as firms dedicate their efforts to creating unique and higher-quality products. Furthermore, this environment could foster broader competition, benefitting consumers through improved choices and driving the market toward greater innovation.[35]

[34] Zhu, F. (2024), 'Dedicated Product Integration in the Era of AI: The Case of the AI Copilot Key', Harvard Business School, September.
[35] Poliak, A. (2013), 'Open Standards and Product Differentiation', QNX Software Systems, accessed 25 November 2024.

Box 3.2 Case study: the Android Compatibility Commitment (ACC)

As an OS with an integrated ecosystem, Android offers a substantial interoperable foundation through 12m lines of open source code. The ACC states standards that guarantee interoperability with the vast majority of Android devices. Consequently, hundreds of device manufacturers focus their production on one OS to cater to more users. Likewise, app developers no longer need to incur testing and modification costs to ensure compatibility with hundreds of different devices.

This reduction in hardware fragmentation increases the productivity among device manufacturers and developers of Android apps while decreasing production costs. A single process serves a broad range of Android devices, freeing more time and resources for enhancing quality rather than ensuring compatibility. Furthermore, they are incentivised to compete by differentiating their offerings to consumers once they have ensured the baseline of Android compatibility.

So long as these processes prevent fragmentation without unduly restricting manufacturers' ability to innovate or differentiate their products, such provisions can enable a healthy competitive environment while delivering interoperability benefits to users.

Source: Oxera (2018), 'Android in Europe', accessed 26 November 2024.

3.2.3 Supply-chain flexibility

Interoperable hardware components could enhance supply-chain flexibility for complementary-device producers. With openness in such specifications, these manufacturers can have increased choices when purchasing production inputs. Instead of relying on a single supplier for specialised parts, they can source components from multiple vendors who adhere to the same standards. Such a wider selection would allow producers to streamline their supply operations, reduce costs through competitive pricing, and avoid being tied to any one supplier.[36] As an example, the emergence of Open Radio

[36] Kerber, W. and Schweitzer, H. (2017), 'Interoperability in the Digital Economy', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 31 January.

Access Network (Open-RAN) technology helped manufacturers of telecoms hardware components sell their components to more Mobile Network Operators (MNOs).[37]

This flexibility could also build resilience in the face of unexpected events. For instance, if a primary supplier experiences disruptions due to natural disasters or political instability, device producers can quickly switch to alternative suppliers without significant delays. Since the components are standardised, transitioning between suppliers is smoother and less costly, minimising impacts on production and sales. This ease of switching could reduce risks and help maintain steady operations even during unforeseen circumstances.[38]

Ultimately, having multiple sourcing options and the ability to adapt swiftly to disruptions could empower complementary-device providers to worry less about supply-chain uncertainties. They could invest confidently in other areas of product development due to the reassurance of having a flexible and resilient supply chain.

3.3 For the access provider

Access providers are firms that allow third parties to interoperate with their own devices. They serve as a bridge between their user base and the rest of the digital ecosystem. By promoting hardware interoperability, access providers could expand their ecosystem to include more devices, which in turn can lead to an increase in the user base, the ability to generate new revenue streams through collaborations and partnerships, and achievement of cost efficiencies by sharing research and development (R&D) costs.

3.3.1 Increase the user base

Hardware interoperability could boost an access provider's user base. When they enable more devices from complementary external manufacturers to be compatible with their ecosystem, the latter becomes more attractive to potential users. Such an expanded compatibility gives users more choices and flexibility, making the platform appealing to a wider audience that seeks the special features offered by the access provider's devices.[39]

As more people start using the platform due to its broad compatibility, developers and manufacturers could be motivated to create even more products that work with it. This creates a positive feedback loop—i.e. a growing number of users attracting more developers, and more compatible products attracting even more users.[40] This positive cycle not only expands the user base further but also encourages complementary-device

[37] Oxera based on Cisco (2021), 'What is Open RAN (ORAN)?', accessed 8 November 2024; RCRWirelessNews (2020), 'Open RAN 101–A timeline of Open RAN journey in the industry: Why, what, when, how? (Reader Forum)', accessed 8 November 2024.
[38] Fadojutimi, B., Israel, A., Arowosegbe, O. and Ashi, T. (2024), 'Future-proofing supply chains: leveraging ERP platforms for advanced automation and interoperability', International Research Journal of Modernization in Engineering Technology and Science, **6**:9.
[39] Hey, F. (2024), 'Data interoperability and portability in the DMA: Competition booster or lame duck?', *Institute of Economics of the Ilmenau University of Technology*, **29**:192.
[40] IBM's introduction of open architecture in PCs describes this positive feedback loop in Box 3.3.

providers to join in, enhancing the platform's ability to generate revenue.[41] Likewise, a growing number of users generates additional data, which developers can use to make technical enhancements and improvements that subsequently attract more users, also strengthening this loop.[42]

By offering increased choice and flexibility to consumers, access providers can strengthen their market position and drive sustainable growth. The enriched ecosystem and larger user base may lead to greater customer loyalty, as users are more likely to remain with a platform that offers them superior value. This strategy helps access providers stay competitive and succeed in the long term.

[41] Kerber, W. and Schweitzer, H. (2017), 'Interoperability in the Digital Economy', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 31 January.
[42] Zhu, F. (2024), 'Dedicated Product Integration in the Era of AI: The Case of the AI Copilot Key', Harvard Business School, September.

Box 3.3 Case study: IBM's open architecture for PCs

Before IBM introduced openness in PC architecture, the industry was highly fragmented as most companies produced proprietary systems. While innovative at the time, these computers were incompatible with one another, effectively limiting options for software and hardware upgrades. The lack of standardisation deterred developers and manufacturers from investing heavily in any single platform, slowing the pace of growth and innovation in the broader PC market.

IBM's decision to embrace an open architecture in 1981 marked a shift in the industry. In contrast to its competitors, it allowed external manufacturers to freely access technical specifications to produce compatible components for the IBM PC. These third-party developers contributed to its ecosystem in specialised ways, from word processing to data analysis. Consequently, the adoption of the IBM PC grew exponentially, as users found value in different applications, from hobbies to workplace productivity, made possible through interoperability.

The IBM PC rapidly set an industry standard, creating a positive feedback loop of adoption: as more users embraced the platform, developers and manufacturers eagerly joined, creating compatible products and further expanding the ecosystem. IBM's strategy turned its PC into a cornerstone of the personal computing revolution, boosting accessibility and reshaping the global computing landscape.

Source: Oxera based on IBM (2024), 'The IBM PC', accessed 26 November 2024; Schleicher, D. and Tolev, A. (2023), 'Learning From the IBM PC: How an open hardware platform for automotive applications can help transform the industry', Amazon Web Services for Industries, accessed 26 November 2024.

3.3.2 Reduced R&D costs

Access providers might find key collaboration avenues to innovate collectively and pool resources in the development of common device ecosystems. When companies collaborate on interoperable technologies, they can combine their expertise and financial resources to advance technological developments more rapidly. This collaborative effort

reduces the need for each provider to invest heavily in developing proprietary systems, thereby minimising the duplication of efforts.[43]

Thus, access providers could optimise their R&D expenditures. To illustrate, instead of multiple companies separately creating similar technologies, they can work together on unified solutions that benefit all parties involved. This allows them to allocate funds more strategically, focusing on unique innovations or enhancements that offer the greatest potential for market success and return on investment.[44]

This shared approach to innovation may enable access providers to streamline their costs and enhance profitability, promoting a more sustainable business model. This not only benefits the providers themselves, but may also accelerate the availability of advanced technologies to consumers, cultivating a more dynamic and competitive market.

[43] Contestabile, J. (2011), 'Concepts on information sharing and interoperability', *IEEE Conference on Homeland Security Technology*, January, pp. 1–16.
[44] Such collaborative efforts are reflected in Box 3.4.

Box 3.4 Case study: the Open Process Automation Forum (OPAF)

Process automation initiatives used to be dominated by proprietary systems and manufacturer-specific architectures. Integrating new hardware required costly reconfigurations, which posed a significant constraint for innovation prospects, especially for smaller firms. For instance, adding a sensor often needed replacing or retrofitting other components to maintain compatibility. This lack of interoperability created inefficiencies and fragmentation, slowing collaboration due to the considerable R&D investments required to drive valuable changes.

To provide a platform aiming to combat these challenges, the OPAF was established in 2017, with large access providers such as ExxonMobil among the founding members. Its mission was to create O-PAS™, a standards-based framework enabling interoperability across hardware and software components. Following OPAF's principles, COPA QuickStart was launched in 2021 to accelerate the adoption of Industrial Control Systems with components from multiple vendors. This initiative boosted development cycles and improved system flexibility, enabling firms to focus on core innovations rather than adapting to proprietary systems. Phoenix Contact, a key manufacturer of industrial automation solutions, supported the launch of COPA QuickStart by sharing hardware and engineering resources.

By pooling expertise from access providers and system integrators, OPAF facilitated avenues for collaboration in R&D. Firms find valuable opportunities to upscale process automation systems and integrate highly efficient technologies without being locked in to a single vendor.

Source: Oxera based on the Open Group (2018), 'Open Process Automation™ Forum', accessed 19 November 2024; Canadian Process Equipment & Control News (2021), 'COPA QuickStart touted as the "standards of standards"', accessed 19 November 2024.

3.3.3 Increased monetisation opportunities

Interoperable hardware solutions could also open up new avenues to generate revenue. For example, revenue-sharing agreements through licensing allow access providers to charge other companies for using the former's devices to promote the latter's products or services. The former benefit from the sales made by the latter. Diversifying these monetisation channels prevents access providers from relying on only the sales of their

own products, since they can also capitalise on the broader market activity generated by interoperability.[45]

Collaborating with external firms helps access providers expand their market reach and enhance their profitability. As part of a larger ecosystem of compatible devices, they may directly target new, specific, customer bases that might have been inaccessible otherwise. For example, smart TV remote controllers may distinctly offer buttons that correspond to specific platforms under a licensing contract.[46] They can attract users who are keen on interoperable solutions for streaming content through these platforms. Aside from increasing sales opportunities, these contracts may improve their brand recognition and customer loyalty, leading to a more sustainable business model with diversified income streams and more competition.

3.4 For the wider economy

The wider economy refers to the collective economic system that includes all industries, markets and societal stakeholders beyond individual organisations or sectors. It can gain substantial benefits from hardware interoperability, particularly in increased innovation prospects, incentives to collectively solve societal problems, and environmental conservation. These advantages can contribute to economic growth, technological advancement and sustainable development for society as a whole.

3.4.1 Increased innovation prospects leading to spillover effects

Hardware interoperability could create an environment where standards support B2B transparency, potentially leading to spillover effects for the wider economy through accelerated digitalisation and technological progress. The Open Industry 4.0 Alliance illustrates these developments, as several manufacturers have benefitted from improved throughput and production transparency with standardised data storage processes and equipment.[47] Furthermore, as described in Box 2.1, a prime example is the role that interoperability played in the growth of the internet. Core interoperable standards enabled foundational connectivity that led to a global communications network. This facilitated diverse applications in the form of the World Wide Web, email and file sharing. In turn, these spurred unforeseen innovations such as video streaming, social media and mobile internet.

Once interoperability is established, unexpected advances in technology and business models may arise, generating value beyond the original purpose. These are spillover effects from which society as a whole benefits. Just as the internet's interoperable framework

[45] Walls, J. (2020), 'New revenue streams abound as connected homes accelerate', TechTarget, accessed 25 November 2024.
[46] Oxera based on PR Newswire (2011), 'Streaming From Netflix Will Soon be Even More Convenient With Netflix One-Click Remotes Introduced by Major Consumer Electronics Makers', accessed 20 November 2024; Gartenberg, C. (2020), 'The Netflix button is an advertisement masquerading as a product', accessed 20 November 2024.
[47] Oxera based on Open Industry 4.0 Alliance (2019), 'About us – Open Industry 4.0 Aliiance', accessed 1 November 2024; Open Industry 4.0 Alliance (2022), 'Projects & Success Stories', accessed 1 November 2024.

paved the way for innovations that revolutionised communication and commerce, hardware interoperability can optimise existing systems and open doors to novel opportunities across industries. Hardware interoperability acts as a catalyst for innovation, driving economic growth and competition, as industries can build upon common platforms to innovate more rapidly and efficiently.[48]

3.4.2 Incentives to collectively solve societal problems

Pursuing interoperable hardware standards can help technological innovators to join forces and address pressing societal issues. The lack of interoperability can lead to functional gaps between machines that are at the core of daily life. For instance, vehicles with unreliable communication systems could create traffic disruptions. To mitigate this problem, car manufacturers have aligned their efforts to develop faster, more accurate non-cellular technology for recognising other entities and infrastructure on the road.[49] When working together, manufacturers can mitigate incompatibility through the definition of key standards that directly aim to solve problems faced by society.[50]

This kind of collaboration may help them avoid duplicating efforts and use resources more efficiently. Similarly, they may find more effective ways to implement compatible specifications in their devices to ensure that consumers are not exposed to significant risks. Interoperability sets the stage for developing standards as companies cooperate during production and technical planning. This makes it easier for different technologies to work together seamlessly, speeding up progress in tackling societal challenges. Especially within particular sectors, this encourages diverse stakeholders to unite in reducing the risks of functional failures, for the benefit of society.[51]

3.4.3 Environmental conservations

Interoperable standards lay the foundation for extending device lifespans through compatibility with other interfaces. Likewise, eliminating the need for multiple hardware specifications that achieve the same function may help to decrease electronic waste. For instance, the EC's 'common charging' solution mandated the universal adoption of USB-C as a standard charging port in the EU for electronic devices by December 2024 for handheld devices, and by April 2026 for laptops. This allows consumers to charge their devices with any USB-C charger, regardless of the device brand, and to purchase new devices without

[48] Gasser, U. and Palfrey, J. (2007). 'Breaking down digital barriers: When and how ICT interoperability drives innovation', *The Berkman Center for Internet & Society at Harvard Law School*, November.
[49] Oxera based on Koon, J. (2023), 'Competing V2V Technologies Emerge, Create Confusion', Semiconductor Engineering, accessed 7 November 2024; Toyota Newsroom (2018), 'Toyota and Lexus to Launch Technology to Connect Vehicles and Infrastructure in the U.S. un 2021', accessed 7 November 2024.
[50] Nan, J. and Xu, L. (2023), 'Designing interoperable health care services based on fast healthcare interoperability resources: Literature review', *JMIR Medical Informatics*, **11**:1.
[51] Iyengar, R. (2018), 'Blockchain in Healthcare: A Data-Centric Perspective', Medium, accessed 26 November 2024.

needing a new charger. As a result, the number of chargers produced and discarded is significantly reduced, cutting annual electronic waste by an estimated 980 tonnes.[52]

Several additional opportunities are created for recycling and repurposing devices, supporting circular economy models and lowering waste disposal costs.[53] The development of secondary markets for used devices and components can lead to lower consumer prices and new business ventures. Additionally, firms may benefit by complying with waste reduction regulations and strengthening their sustainability credentials to attract environmentally conscious investors. Resource conservation can become more attainable and effective to stimulate economic activity in sustainability-focused sectors.[54]

Box 3.5 Case study: the Open Charge Point Protocol (OCPP)

The OCPP proposes a standardised communication framework that enables interoperability among EV charging stations and management systems, regardless of manufacturer. By supporting compatibility across networks, it facilitates accessibility to EV infrastructure, enabling users to charge vehicles seamlessly and providers to scale efficiently. OCPP promotes smart charging practices with real-time data to optimise renewable energy distribution during off-peak periods. This contributes to lower carbon emissions and a more sustainable energy grid, helping cities and companies deploy EV infrastructure more effectively.

Adopted by European manufacturers such as Allego and Alfen, OCPP enhances user experience while advancing environmental goals. It has the potential to create business opportunities, reduce waste and support circular economy models, benefitting economies through lower consumer costs and compliance with sustainability regulations. By attracting environmentally conscious investors, OCPP fosters progress toward societal and environmental objectives.

Source: Oxera based on EVBox (2020), 'Understanding OCPP: Why Interoperability Matters', accessed 1 November 2024; Kuman, R. (2024), 'What is the Open Charge Point Protocol (OCPP) in EV charging?', EV Engineering & Infrastructure, accessed 1 November 2024.

[52] European Commission (2022), 'The EU common charger', accessed 25 November 2024.
[53] Box 3.5, although with a higher emphasis on efficient energy distribution, exemplifies this benefit.
[54] Udeh, E., Amajuoyi, P., Adeusi, K. and Scott, A. (2024), 'The role of Blockchain technology in enhancing transparency and trust in green finance markets', *Finance & Accounting Research Journal*, **6**:6, pp. 825–850.

4 Potential barriers to achieving hardware interoperability

This section outlines the various barriers to interoperability, which can stem from technical, regulatory or business considerations. Technical barriers often involve challenges relating to the design, compatibility or standardisation of systems, while regulatory barriers can arise from legal frameworks that limit data sharing or impose compliance requirements. Business barriers, conversely, are driven by firms' incentives, where companies may resist interoperability to maintain competitive advantages, product differentiation or control over their platforms.

Despite the potential benefits of interoperability, businesses may strategically use these barriers—particularly business barriers—as a means to delay or avoid meeting interoperability obligations, even when such obligations exist. Business barriers, in particular, remain one of the primary reasons why interoperability is often not achieved, as firms use them to protect entrenched positions. With that in mind, this section proposes solutions to address these issues, discussing when and how interventions may be justified and identifying practical steps to promote interoperability effectively.

4.1 Technical barriers

4.1.1 Technical, security and integrity risks

Technical incompatibilities between systems can create barriers to interoperability, arising from differences in physical design, language protocols or proprietary interfaces.

Physical compatibility refers to connection issues that arise when different systems attempt to integrate with one another. For example, if two pieces of hardware have physically different connection protocols (e.g. connectors, ports). While adaptors can mitigate these compatibility issues, they often come at an extra cost.

Language protocol barriers emerge when systems have incompatible data formats or definitions. Effective data exchange requires a common understanding of both the data structure and its meaning. If two systems have incompatible data formats or definitions, they may struggle to integrate seamlessly.

Proprietary interfaces are often designed to prioritise integration with authorised products within the same ecosystem, ensuring that the connected hardware and software meet specific standards. For instance, a device may display an 'accessory not supported' message when attempting to connect to unauthorised software or hardware.[55]

[55] For example, proprietary interfaces in wearables increase the difficulty to access relevant health data by physicians. Canali S., Schiaffonati V. and Aliverti A. (2022), 'Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness', PLOS Digit Health, **1**:10, October.

Furthermore, security and integrity concerns can also constitute a technical barrier to interoperability, which is heightened in an increasingly interconnected digital economy.[56,57] In this context, the adage 'the network is only as strong as its weakest link' holds true.

In essence, each interoperating connected device represents a potential entry point for cyber threats, and if one device or system lacks adequate security measures, it may jeopardise the integrity of the entire network. IoT networks are thought to be particularly prone to cyber threats, as some of the smaller IoT devices have low computational power and less storage capacity and hence security mechanisms are difficult to implement.[58]

However, it is worth considering that there may be a trade-off between the security of a device and it's utility. A device that cannot interoperate with other devices—such as one incapable of accessing the internet—may offer high security but would have very limited utility. Therefore, it is necessary to balance security and interoperability to achieve both functionality and protection.

Moreover, interoperability can, in some cases, strengthen security. When two systems lack interoperability, consumers often resort to workarounds to bridge the gap, which can introduce security risks. For example, there are a number of non-official third-party platforms that enable file sharing between non-Apple and Apple devices, effectively bypassing the lack of native interoperability.[59] In addition, user workarounds often involve relying on making suboptimal choices from a security perspective, such as jailbreaking a phone or using uncertified cables. These practices can compromise device security and consumer safety. Allowing interoperability with trusted and approved third parties can mitigate these risks by providing secure, reliable options for users while maintaining control over safety standards.

In addition, it may be the case that third-party complementors have more stringent security and privacy standards than the access provider.[60] In this scenario, the presence of third parties can increase security and privacy standards for consumers.

4.1.2 Are these risks valid?

There are two important points to consider when assessing the validity of the risks associated with interoperability.

First, while it is important to consider whether interoperability will lead to security risks, firms might sometimes leverage these technical barriers strategically to avoid pursuing interoperability.[61] For instance, businesses may choose to retain proprietary standards or

[56] Kerber, W. and Schweitzer, H. (2017), 'Interoperability in the Digital Economy', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 31 January, p. 42.
[57] Gasser, U. (2015), 'Interoperability in the Digital Ecosystem', *The Berkman Center for Internet & Society at Harvard Law School*, 6 July.
[58] Kumari, P. and Jain, A. (2023), 'A comprehensive study of DDoS attacks over IoT network and their countermeasures', *Computers & Security*, **127**.
[59] See, for example, Snapdrop (2015), 'About', accessed 8 November 2024
[60] CERRE (2022), 'Interoperability in Digital Markets', March, p. 31.
[61] See Box 4.1 for a discussion of misconceptions of risk between open and closed systems.

interfaces to ensure that their products work only within their own ecosystem. While this approach might limit security risks, proprietary standards could also be less secure than open alternatives, although this cannot be assessed due to their closed nature. Such decisions may also reflect a strategic choice to safeguard profits. As such, these barriers can be overstated, particularly when gatekeepers use them as justification to delay or resist interoperability (see Box 4.1 for a discussion of misconceptions of risk between open and closed systems).

Second, in other cases, businesses might delay making decisions in favour of interoperability, citing concerns about security, even when interoperability is technically feasible. For example, when launching a new feature, platforms may limit interoperability by initially keeping the system closed to themselves or a select group of trusted third parties. This restricted access allows for testing and refinement of the feature in a controlled environment, ensuring that any bugs or design flaws are addressed before wider release. Furthermore, failures in the system could result in significant brand reputation risks. Thus, firms may not automatically pursue interoperability in the short term, as platforms prioritise security and brand protection during the feature's early rollout stages.

Box 4.1 The open systems risk myth

Openness and interoperability in technical ecosystems are sometimes believed inherently to compromise security and integrity, favouring closed systems as safer alternatives. However, this view oversimplifies a more complex issue, and there are many examples of open systems being more secure than closed ones. Open systems, such as OpenTitan and Open-RAN, provide robust security frameworks by enabling transparency, third-party auditing and modularity.

For instance, OpenTitan's hardware root-of-trust ensures the function of trusted operations. This is achieved through cryptographic isolation and resistance mechanisms to external interferences. Similarly, Open-RAN allows MNOs to verify their interfaces against open standards. They can reduce risks linked to delayed vulnerability detection, weaker safeguards and over-reliance on secrecy. Especially prevalent in closed systems, these concerns would leave MNOs vulnerable to exploitation once their hidden flaws are exposed.

Closed systems are not immune to security flaws as well. Their opaque nature can delay vulnerability detection and remediation. In contrast, open systems can effectively mitigate such risks through rigorous public scrutiny and adherence to stringent protocols. Security is not a simple trade-off between open and closed systems, it is largely case-dependent. With robust hardware frameworks and transparent protocols, open systems can often exceed the security benchmarks of their closed counterparts.

Source: Oxera based on National Telecommunications and Information Administration (2023), 'Open RAN Security Report', accessed 29 November 2024; Parisi, E., Musa, A., Ciani, M., Barchi, F., Rossi, D., Bartolini, A. and Acquaviva, A. (2024), 'Assessing the performance of opentitan as cryptographic accelerator in secure open-hardware system-on-chips', *Proceedings of the 21st ACM International Conference on Computing Frontiers*, May, pp. 172–179, accessed 29 November 2024; NCC Group (2024), 'Security Risks of AI Hardware for Personal and Edge Computing Devices', accessed 13 December 2024.

4.1.3 Solutions

While there are technical challenges when it comes to hardware interoperability, these are often far from insurmountable, although timing and coordination play an important role in minimising the costs and risks involved. Compatibility issues, for example, are more easily addressed if considered at the design stage and there is appropriate documentation that accompanies them (see section 6.2 for further details).

Standards can also help to align design requirements across sectors alongside reducing fragmentation, ensuring that systems remain compatible over time.[62] By establishing interoperability standards from the outset, firms can avoid costly transitions later on. That said, striking the right balance in the timing of interventions is critical. Taking action too early risks locking the market into immature, suboptimal standards before a consensus is reached.[63] Conversely, waiting too long may exacerbate fragmentation, making interoperability more costly and complex.

In some cases firms may choose to overcome compatibility issues themselves, for example by developing industry standards. This is the case in smart homes and industry IoT as presented in sections 2.3 and 2.4, and also demonstrated in Box 4.2 below, which outlines how the adoption of standards in the telecommunications industry has helped operators to achieve interoperability on a global scale.[64] On the regulatory side, laws such as the DMA may mandate certain standards to ensure contestability, as further discussed in section 6, while competition law rulings may enforce interoperability through standardised information sharing or interface access.[65]

The presence of proprietary interfaces and security or privacy concerns can be more challenging to address, as these issues go beyond technical compatibility and rely heavily on the willingness of firms to open their systems, particularly if technical barriers, such as trade-offs between system integrity and interoperability, are overstated to delay or deny standardisation. However, as set out in section 4.1.2, it is important to recognise that interoperability and security need not be conflicting goals. It is possible to realise the benefits of interoperability while managing potential vulnerabilities that could arise when integrating third-party systems.[66]

The risks often associated with security and privacy are not inherent to interoperability itself, but rather depend on its implementation. The way in which the technology stack is designed and delivered can determine whether the addition of third-party devices into a network increases risk. For example, the more transparent the code and security processes, and the greater the number of experts or agents with oversight and visibility of the system, the more secure it can be, as vulnerabilities can be identified and addressed promptly. Moreover, effective solutions can be implemented to safeguard user privacy and security by ensuring that issues arising in one layer of the technology stack do not propagate to others. For instance, features such as a 'private compute core' can isolate sensitive processes, mitigating risks and maintaining the integrity of the broader system.[67]

[62] See the example of global system for mobile communications (GSM) in Box 4.2.
[63] For example, had USB been regulated too early, it might have prevented companies from arriving at USB-C as a modern industry standard.
[64] Box 4.1 outlines how the adoption of standards in the telecommunications industry has helped operators to achieve interoperability on a global scale.
[65] A notable example is the 2007 case against Microsoft, where the company was mandated to provide information about its interfaces to facilitate interoperability between its OS and competitor servers. CFI, Judgment of 17.9.2001, *Case T-201/04 – Microsoft Corp.*
[66] Kerber, W. and Schweitzer, H. (2017), 'Interoperability in the Digital Economy', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 31 January, p. 5.
[67] Android Magazine (2023), 'What is Private Compute Core? How can you use your smartphone with peace of mind?', accessed 11 December 2024.

Furthermore, verification programmes can provide a practical solution to address security risks associated with interoperability by ensuring that devices and systems meet established standards for safety and functionality (see the case study outlined in Box 6.1 on how this was balanced in the case of messaging interoperability). These programmes, often developed through industry collaboration, certify that hardware and software are compatible and secure, reducing the risk of vulnerabilities. These examples provide a pathway for moving beyond recognising the risks to discussing practical solutions for achieving secure interoperability.

For policymakers, this requires careful consideration of how to balance the demand for greater user flexibility with the imperative to safeguard system integrity. Interoperability regulations that overlook the importance of security and quality controls may unintentionally expose users to harm, ultimately reducing the very benefits that they aim to deliver. However, in most cases, concerns around security and integrity can be addressed through collaboration and thoughtful design, and should not be used as an excuse to impede progress or avoid finding workable solutions.

Box 4.2 Case study: global system for mobile communications (GSM)

The GSM Association (GSMA) was established to support the development and deployment of GSM technology across Europe and beyond. Its primary objectives were to facilitate cooperation, uphold technical standards and promote interoperability. In 1987, representatives from 13 countries signed a memorandum of understanding committed to creating a mobile phone system that could work across national borders. By the end of the 20th century, the initiative had 250m users globally, far exceeding the initial hope of 20m.

GSM quickly became the global standard for mobile communications, securing over 90% of the global market share. This standardisation provided mobile users with a seamless experience, allowing them to communicate across networks in different countries. Today, the GSMA continues to support interoperability and innovation through protocols and standards for 4G, 5G and upcoming technologies such as 6G. It also fosters collaboration across the mobile ecosystem through events such as the Mobile World Congress (MWC), which brings together operators, suppliers and related industries.

Source: Oxera based on GSMA (2024), 'Our history', accessed 9 December 2024; ZDNET (2007), 'Happy 20th birthday, GSM', accessed 9 December 2024.

4.2 Regulatory barriers

4.2.1 Potential concerns

One example of a regulatory barrier to interoperability could be the General Data Protection Regulation (GDPR). Designed to protect individual privacy and empower consumers with control over their personal data, the GDPR aims to enhance data security and trust. Under this regulation, firms must obtain explicit consent from consumers before processing their personal data. Particularly when involving data-sharing initiatives, these requirements can complicate interoperability. While the regulation allows for data sharing under specific conditions—such as obtaining informed consent or ensuring legitimate interests[68]—companies may hesitate to promote interoperability due to concerns about compliance and potential penalties for violations.

This is particularly important in the healthcare sector, where data is particularly sensitive. Many wearable devices store data in local storage without encryption or adequate data protection, resulting in a risk of losing confidential and personal data.[69] That said, there are significant payoffs to achieving interoperability in this sector if it leads to improved patient outcomes through more accurate diagnoses and timely treatments.[70]

Security law can also affect interoperability. The network and Information Security (NIS) Directive, originally NIS 1 and more recently NIS 2, was brought in to enhance cybersecurity across the EU.[71] Under NIS 2, companies designated as 'essential' (e.g. energy, transport, health) and 'important' (e.g. digital services, manufacturing) face differing requirements. Essential entities are mandated to implement a higher level of security measures, whereas important entities may have slightly less-stringent obligations, but still encounter significant compliance demands. This divergence may lead to a fragmented regulatory landscape where hardware is tailored to meet sector-specific requirements rather than promote interoperability.

Firms may also cite competition law as a reason for resisting interoperability. Interoperability requires coordination between two or more firms. This collaboration, if not approached with caution, could lead to significant competition law concerns. For instance, when discussing standard setting, the EC notes that: 'standard development can, however, in specific circumstances where competitors are involved, give rise to restrictive effects on competition by potentially restricting price competition and limiting or controlling production, markets, innovation or technical development'.[72] One way this could arise is if firms exchange information during the standard development process. Such exchanges

[68] Data Protection Commission (2019), 'Guidance note: legal bases for processing personal data', December, accessed 9 December 2024.
[69] Vijayan, V., Connolly, J., Condell, J., McKelvey, N. and Gardiner, P. (2021), 'Review of Wearable Devices and Data Collection Considerations for Connected Health', *Sensors*, **21**:16, August.
[70] The Institute of Electrical and Electronics Engineers Standards Association (2018), 'Wearables and Medical IoT Interoperability and Intelligence (WAMIII)', accessed 9 December 2024.
[71] EU (2022), 'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union'.
[72] European Commission (2023), 'Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements', 21 July, para. 441.

could reduce or eliminate price competition, if it allows firms to align their pricing strategies or control production levels, leading to collusive outcomes that harm the competitive landscape.

4.2.2 Solutions

Regulatory barriers such as data protection laws, cybersecurity mandates and intellectual property rights might require a variety of solutions, but these can often be overcome.

For privacy and data protection, compliance can often be achieved by obtaining user consent for data sharing, particularly under regulations like GDPR. For example, to address the challenge of data protection in the health industry, the Institute of Electrical and Electronics Engineers Standards Association has developed the Wearables and Medical IoT Interoperability and Intelligence (WAMIII) programme to foster a global community of stakeholders who collaborate to build consensus and develop solutions for secure medical device interoperability. This programme aims to establish standard frameworks for a secure data portability mechanism. Additionally, WAMIII seeks to build a global certification system to ensure patient privacy and establish trust in data outputs.

Competition law concerns around standard setting and coordination between competitors can be addressed through mechanisms designed to foster transparency and minimise anticompetitive risks. For example, adopting clear governance structures for standard-setting organisations (SSOs) can help to mitigate the risks of information exchanges leading to collusive outcomes; SSOs can implement confidentiality rules and independent oversight during discussions to ensure that competitive dynamics are preserved. Such measures build confidence among firms participating in interoperability initiatives while safeguarding compliance with competition law.

4.3 Business barriers

4.3.1 Potential concerns

Business incentives often represent the primary obstacle to achieving interoperability.[73] Firms may view interoperability as misaligned with their strategic goals, particularly when they believe it may undermine profitability and market control.

One example of this is the tension between interoperability and product differentiation. When firms adopt interoperable standards, it may lead to greater homogeneity, as they must align products to comply with common interfaces or protocols. This alignment may, in theory, limit a firm's ability to develop distinct features from its competitors, reducing its scope to differentiate and cater to specific consumer preferences.[74] In particular, if

[73] Scott Morton, F., Crawford, G., Crémer, J., Dinielli, D., Fletcher, A., Heidhues, P. and Schnitzer, M. (2023), 'Equitable interoperability: The "Super Tool" of Digital Platform Governance', *Yale Journal on Regulation*, **40**:3, p. 1018.
[74] Kerber, W. and Schweitzer, H. (2017), 'Interoperability in the Digital Economy', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 31 January, pp. 5–6.

interoperability is built around setting standards, this may result in an upper limit of what is achievable technically. For example, as set out in Box 2.1, the internet has developed around certain interoperable protocols (such as TCP/IP) that may limit certain types of innovation if they require features to be layered on top of the established protocols.[75] The inability to distinguish itself from its competitors may therefore reduce a firm's willingness to pursue interoperability. That said, this barrier is more relevant to horizontal than vertical interoperability, the former of which involves firms interoperating with competitors.

Linked to the risk of lack of product differentiation, interoperability may reduce incentives to innovate, as companies involved in creating standardised solutions may be less motivated to invest in new technologies. The possibility for firms to innovate is closely tied to their ability to capture the returns on their investments. If interoperability requires firms to share network benefits or adhere to uniform standards, it may reduce the proprietary value of their innovations, discouraging investment in new products and services.[76] That said, the effects of incentives to interoperate are complex. As mentioned in section 3.2, interoperability can also enhance incentives for product differentiation, leading to greater choice for consumers.

In addition, vertically integrated firms often have incentives to maintain closed systems rather than pursue interoperability, as closed ecosystems may facilitate market entry if they allow them to achieve greater value across various levels of the supply chain (see Box 4.3). This is sometimes achieved by cross-subsidising different layers within their ecosystem. For example, a company might sell hardware at a low cost to increase consumer uptake, while charging significantly above marginal cost for complementary content or services once they are adopted in the ecosystem. One example of this would be Amazon's Kindle e-readers. In 2012, Amazon had been quoted as selling these 'at cost', with profit instead coming from sales of their online content.[77] At the time, Kindle did not support some other common open eBook formats such as EPUB, and Amazon's own eBook format MOBI was unable to be read by non-Amazon software.[78] Vertically integrated entities can use this strategy to generate revenue from one area, which may also help support other parts of their business, potentially facilitating market entry in some cases.

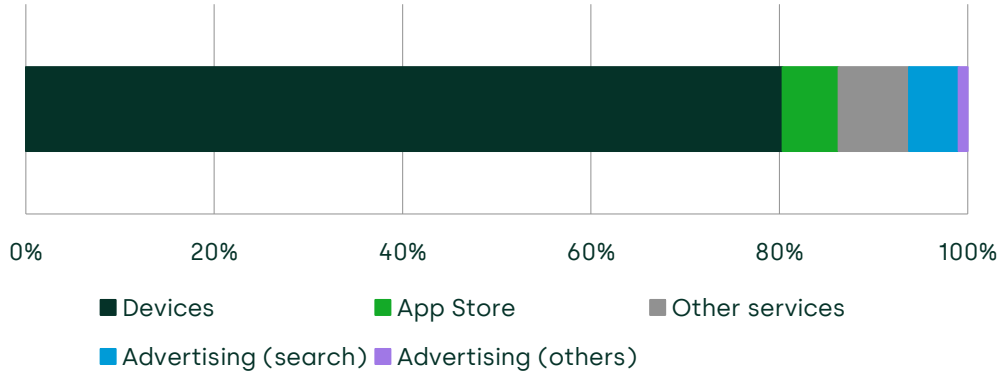
From the access seeker's perspective, there are also concerns relating to reliance on the access provider. If an access seeker becomes dependent on a provider for interoperability, they face the risk of being cut off or facing disruptions if the provider changes its strategy or withdraws support. The prospect of such reliance can deter businesses from fully committing to platform-specific investments, particularly if they perceive the access provider as having the power to change the terms or availability of access in the future.[79]

[75] Gasser, U. (2015), 'Interoperability in the Digital Ecosystem', *The Berkman Center for Internet & Society at Harvard Law School*, 6 July.
[76] Kerber, W. and Schweitzer, H. (2017), 'Interoperability in the Digital Economy', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 31 January, pp. 10–11.
[77] Reuters (2012), 'Amazon Kindle Sold "At Cost," CEO Jeff Bezos Confirms', Huffington Post, 11 October.
[78] Gasser, U. (2015), 'Interoperability in the Digital Ecosystem', *The Berkman Center for Internet & Society at Harvard Law School*, 6 July.
[79] CERRE (2022), 'Interoperability in Digital Markets', March, p. 27.

Box 4.3 Case study: Apple's integration incentives

As seen in Figure 4.1, Apple's incentive to limit third-party interoperability stems largely from the fact that a significant portion of its revenue—around 80%—comes from the sale of devices. By controlling the compatibility and functionality of these devices, Apple can maintain a closed ecosystem that encourages consumers to buy multiple products within the Apple family, ensuring continued device sales. For example, features such as AirDrop, which allows file transfers between Apple devices, audio sharing for AirPods, and Handoff for seamless task continuation across devices, are designed to work only within the Apple ecosystem. By restricting these features to Apple hardware, Apple increases the value of owning multiple devices within its ecosystem, incentivising customers to stay within the brand ecosystem. If Apple allowed seamless interoperability with third-party hardware, it could erode its ability to drive customers towards its own proprietary accessories and services. For instance, if consumers could easily connect non-Apple products to an iPhone, they might be less likely to purchase Apple's own accessories, such as AirPods, or invest in Apple's exclusive features. By limiting interoperability, Apple creates a strong incentive for customers to stay within the ecosystem, shielding Apple from competitive pressure in the broader hardware market.

Figure 4.1 Breakdown of Apple's 2021 global revenue



Source: Oxera based on Competition and Markets Authority (2022), 'Mobile ecosystems: Market study final report', 10 June.

4.3.2 Solutions

There are many cases where markets are not competitive, and in these situations, there is a clear rationale for pursuing interoperability, even if it may not align with the interests of

the access provider firm. Overcoming business barriers to interoperability may well be more challenging than addressing technical barriers, which can often be solved through the adoption of standards or technical solutions. Business barriers, conversely, are deeply rooted in the strategic interests and incentives of individual firms. For some companies, concerns over product differentiation may prevent them from embracing interoperability. For others, the desire to maintain vertical integration, allowing them to subsidise costly innovations, may incentivise them to keep their systems closed.

As discussed in sections 5 and 6, to overcome these barriers, regulation can be used to address business barriers that arise when firms with market power act to prevent or inhibit interoperability solely to preserve their market position.[80] That said, it is essential to assess barriers on a case-by-case basis, considering whether they truly hinder broader market or consumer benefits. In some instances, the barriers may serve valid business interests that ultimately benefit consumers—such as fostering innovation.[81] In other cases, the potential benefits of interoperability, including increased market competition and innovation, may outweigh the costs of overcoming these barriers. Therefore, a careful balancing of the benefits against the costs is necessary to determine the most appropriate approach.

[80] CERRE (2022), 'Interoperability in Digital Markets', March, p. 45.
[81] Kerber, W. and Schweitzer, H. (2017), 'Interoperability in the Digital Economy', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 31 January, p. 58.

5 A framework for promoting hardware interoperability

There are broadly two ways in which interoperability can arise. Specifically, it may emerge from market forces, be that from the supply side, where businesses take the initiative to create interoperable solutions, or from the demand side, where consumer interest and preferences drive the push for interoperability. However, when policymakers recognise benefits of interoperability that are not materialising naturally through market forces, they might consider mandating interoperability through regulation, such as with the DMA.

This section proposes a framework for fostering interoperability, more widely taking into account the potential benefits described in section 3 and the potential barriers in section 4. We then discuss and focus on how Article 6(7) aligns with this framework.

5.1 A general framework for promoting hardware interoperability

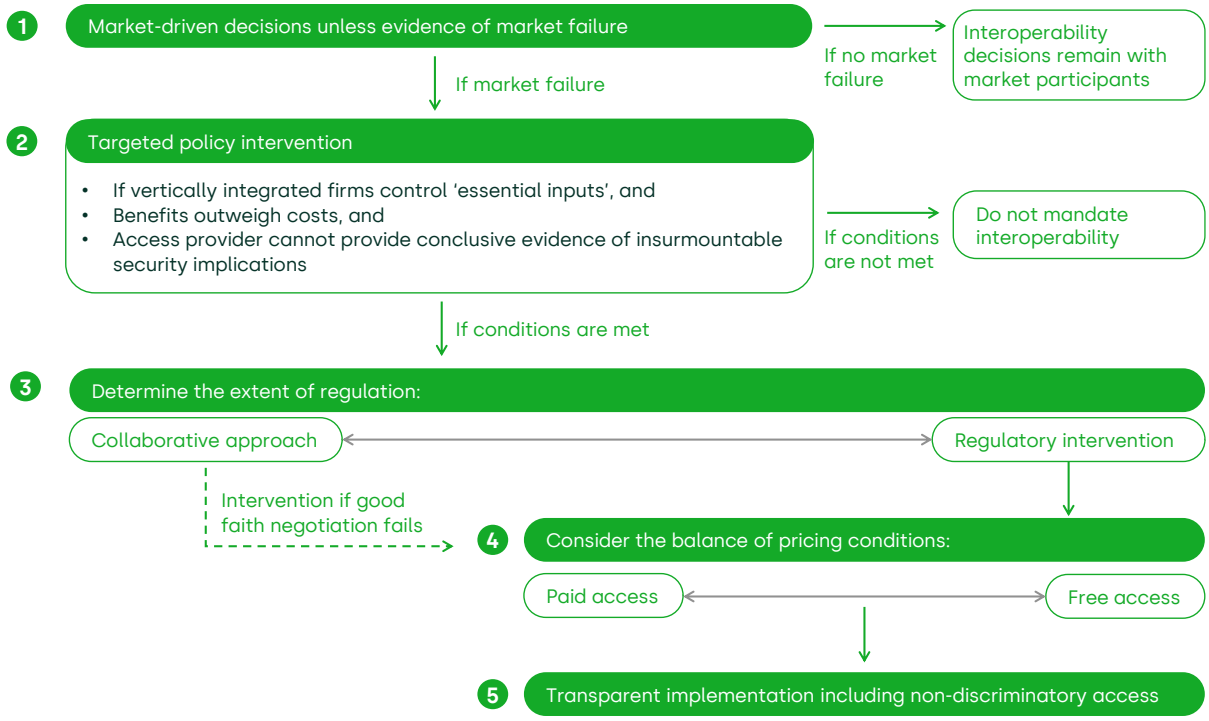
To address the trade-offs associated with hardware interoperability, it is essential to establish a structured framework that guides decision making. This framework aims to navigate the conflicting priorities by providing clear principles and practical approaches for stakeholders. This could help to identify and mitigate potential drawbacks while maximising the benefits.

The framework is designed to balance regulatory interventions with market-driven incentives, aiming to promote openness, economic growth and innovation in digital ecosystems. By balancing the diverse needs of all parties involved, such a framework can facilitate the development of interoperable systems that promote innovation, competition and long-term sustainability. As illustrated in Figure 5.1 and described in more detail below, the framework is based on five principles.

1. **Market-driven decisions:** as a general rule, in markets without substantial market failures, interoperability decisions should be left to the market. In a functioning market economy, firms act in their self-interest, which generally promotes competition.
2. **Targeted policy intervention:** where vertically integrated firms control access to essential components, and the benefits of intervention outweigh the costs, public policy intervention may be justified. However, interoperability should not be mandated in cases where there is clear evidence of insurmountable security, privacy or integrity risks.
3. **From collaborative approach to regulatory intervention:** in many cases, effective interoperability may be achieved through collaboration between access providers and third parties to agree on the form and terms of access. However, where good faith negotiations stall, or where deemed insufficient, regulators may need to intervene to determine the form and terms of access.
4. **Balanced pricing conditions:** regulators should weigh trade-offs when setting pricing for interoperability access, ensuring that gains in innovation by smaller rivals are not offset by potential reductions in innovation due to ex ante regulation.

5 **Transparent implementation:** any mandated interoperability should involve clear descriptions of the features and functionalities for which interoperability is available including non-discriminatory access conditions as well as a fast, quick and transparent resolution processes in case of unclarity or disputes.

Figure 5.1 Oxera's five-step framework for interoperability



Source: Oxera.

While this approach is intended as a universal framework for promoting interoperability, and is flexible in application, we note that Article 6(7) represents a regulatory intervention that is broadly aligned with these principles. In this instance, principles 1 to 4 are embedded in the wording of Article 6(7), while principle 5—its implementation—is now the focus of the EC. This is discussed further in section 5.2.

Principle 1: market driven decisions

As outlined in sections 3.2, 3.3, 4.14.3, there are complex interactions between the benefits and costs of achieving a higher degree of interoperability. When market participants have a clear business case for interoperability, the decision to implement it is often better driven by industry dynamics rather than regulatory mandates.

In instances where significant market failure exists or where a policy need is clearly identified, regulatory intervention may be warranted. However, such intervention should be approached with caution. As noted by Kerber and Schweitzer (2017), mandatory standards

and interoperability obligations should be imposed only when less intrusive measures are unavailable.[82] Often, the issue of technical non-interoperability can be addressed through unilateral solutions—such as adaptors or converters—which can provide an acceptable level of connectivity without the need for broader intervention.

The legal and policy focus should be on protecting market-driven solutions to interoperability problems, rather than imposing burdensome regulatory mandates. Within the framework of Article 102 of the Treaty on the Functioning of the European Union (TFEU), EU competition law may be more effective in developing a workable test to address barriers to interoperability that are created by dominant firms. Specifically, competition authorities should focus on instances where dominant firms have hindered competitors' efforts to achieve interoperability, including where they develop proprietary standards with this aim, thus harming market competition. This approach may provide sufficient remedies in most cases without resorting to the imposition of mandatory interoperability standards through regulation.

Therefore, in markets where there are no significant market failures, interoperability decisions should generally be left to the market participants. Likewise, where interoperability is already advancing organically, with a clear business rationale driving the process, external intervention may not be necessary.

Principle 2: targeted policy interventions

In certain circumstances, public policy interventions to encourage or mandate hardware interoperability may be warranted. However, this is subject to meeting three criteria.

First, such interventions are particularly justified in cases involving entrenched vertically integrated firms that control access to an 'essential component' for many hardware providers. These situations often arise where the vertically integrated firm's incentives conflict with those of other stakeholders, creating barriers to competition and innovation.

The three-criteria test established within telecoms regulation provides a useful benchmark for determining whether public policy intervention is necessary. According to this test, interventions are justified when:[83]

1 high and non-transitory barriers to entry exist;
2 there is no tendency towards effective competition;
3 competition law alone is insufficient to address the issue.

Academic literature supports this principle. CERRE (2022) suggests that vertical interoperability should only be mandated when gatekeepers are vertically integrated, and there is evidence that this structure forecloses complementors, resulting in harm that

[82] Kerber, W. and Schweitzer, H. (2017), 'Interoperability in the Digital Economy', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 31 January.
[83] CERRE (2022), 'Interoperability in Digital Markets', March, p. 28.

would not have occurred absent vertical integration.[84] Concerns regarding innovation incentives can be addressed by implementing an appropriate pricing regime.

Second, interventions should be proportional, meaning that the benefits of interoperability must outweigh the associated costs. This principle ensures that any regulatory or policy measures taken to enhance interoperability contribute positively to overall societal welfare. This approach aligns with a broader objective of ensuring that regulation is not overly burdensome and serves the public interest effectively.

Third, recognising that hardware interoperability can carry risks when it comes to the security and integrity of the systems involved, the intervention needs to devote particular attention to mitigating these impacts. This requires a detailed understanding of the potential issues, and an exploration of the most effective solutions while ensuring that these are strictly necessary and proportionate. The burden of proof, however, should first and foremost rest with the access provider, who must provide clear evidence held to a rigorous standard to prevent security claims from being used as a pretext for non-cooperation. As detailed in section 4.1, interoperability can be achieved, and in some instances can even be strengthened, with the right safeguards in place, so security and integrity risks should not be an argument against it per se.

Principle 3: from collaborative approach to regulatory intervention

The level of the regulatory intervention will depend on specific market circumstances, the level of cooperation of the newly regulated entity and their likely incentives. In the case of hardware interoperability, where mandated intervention requires different systems to work together going forward, cooperation between the access provider and the third parties seeking access can be instrumental to deciding the form and terms of access.

Collaboration allows for a constructive dialogue where third parties can articulate their needs and priorities while access providers can outline potential constraints, such as technical limitations, security requirements or the costs of providing access. Cooperation between the stakeholders can also mean that detailed rules and guidance are not necessary if there are voluntary solutions that meet the needs of all parties, such as interoperability by design.

However, where this is not the case and where good faith collaboration fails, the regulatory framework will need to be more prescriptive, and the regulator needs to have the power to intervene with binding guidelines, rules and fines.

An example of a more cooperative model that can escalate to more stringent regulation comes from the Netherlands in the context of site access for radio equipment of broadcasters. At the base level, while there is regulation in place, the model encourages negotiations between the parties involved to reach an agreement regarding access and conditions. However, if these negotiations fail, the process escalates to a dispute settlement model where the regulator is empowered to facilitate dispute resolution

[84] CERRE (2022), 'Interoperability in Digital Markets', March, p. 45.

between the parties. If still unresolved, the regulator can intervene if needed as it has the authority to impose binding decisions, including ultimately setting access prices.

Principle 4: balanced pricing conditions

When setting interoperability access prices, regulators must carefully balance trade-offs to ensure that interventions achieve their intended benefits without causing undue harm to innovation and competition. While fostering interoperability can stimulate competition and innovation among smaller rivals, regulators must also consider potential adverse impacts on the incentives of access providers, particularly where ex ante regulation is involved.

In the telecoms sector, cost-based pricing has been a common approach to setting access conditions. This model ensures that access providers receive fair compensation for their investments while enabling smaller players to compete effectively. Cost-based pricing is often calculated by reference to the long-run incremental costs of providing access, ensuring affordability for entrants while safeguarding the financial viability of incumbents.[85] However, cost-based pricing is not the only potential solution. Other approaches, such as licensing agreements, could offer access under agreed terms that reflect the value created by interoperability (see, for example, section 3.3.3).[86] Similarly, joint investments in shared infrastructure can reduce costs for all parties and foster collaborative innovation, aligning incentives more effectively.[87]

In other cases, interoperability provided by the access provider for free may also be a solution, if it is considered that a market needs to become more contestable, or when costs of interoperability are relatively low, and where these (to a large extent) can be recouped by the access provider.

Principle 5: effective and transparent implementation

The transparent implementation of mandated interoperability is crucial to ensure fair and equitable access for all stakeholders. This should involve clear descriptions of the features and functionalities for which interoperability is available and clear access conditions that explicitly outline the terms under which interoperability features can be utilised. Comprehensive documentation must also be made publicly available, detailing the technical specifications and compliance requirements necessary for third-party developers and manufacturers to engage with interoperable systems effectively. Transparency in these aspects reduces ambiguity and prevents disputes, fostering a cooperative environment among stakeholders.

[85] Confraria, J., Noronha, J., Vala, R. and Amante, A. (2002), 'On the use of LRIC models in price regulation'; *Instituto das Communicaçoes de Portugal* and CERRE (2022), 'Interoperability in Digital Markets', March, p. 32.
[86] Tsilikas, H. and Tapia, C. (2017), 'SMEs and standard essential patents: licensing efficiently in the Internet of Things', *les Nouvelles-Journal of the Licensing Executives Society*, **52**:4; CERRE (2022), 'Interoperability in Digital Markets', March, p. 33.
[87] Nimy, K. and Sudha, V. (2024), 'Analyzing The Specific Financial Requirements And Challenges Faced By Different Actors Within Agricultural Value Chains', *Library Progress International*, **44**:3, pp. 11877–11888.

Non-discriminatory access is another critical element of transparent implementation. It may be appropriate to offer access to interoperability features on FRAND terms. This approach ensures that no single access seeker is favoured or excluded, maintaining a level playing field and encouraging competition. The FRAND framework, commonly applied in intellectual property and standard-setting contexts, serves as a valuable model. For example, the European Telecommunications Standards Institute (ETSI) requires Standard Essential Patents (SEPs) to be licensed on FRAND terms, promoting open access while safeguarding innovation incentives.[88]

Existing EU regulations also offer guidance on transparency in interoperability frameworks. The European Electronic Communications Code (EECC) includes provisions requiring access to essential network infrastructure under transparent and non-discriminatory conditions, with detailed technical and pricing information to support market entrants.[89] Similarly, the Radio Equipment Directive (RED) ensures transparency by requiring manufacturers to provide sufficient documentation to support compatibility with accessories such as chargers and headsets.[90] Transparent implementation not only strengthens trust among stakeholders, but also ensures that mandated interoperability achieves its goals.

5.2 Article 6(7) under this framework

While the framework set out in section 5.1 presents an approach to promote hardware interoperability in general, Article 6(7) represents a regulatory intervention that fits within these general principles. Article 6(7) clearly mandates that:[91]

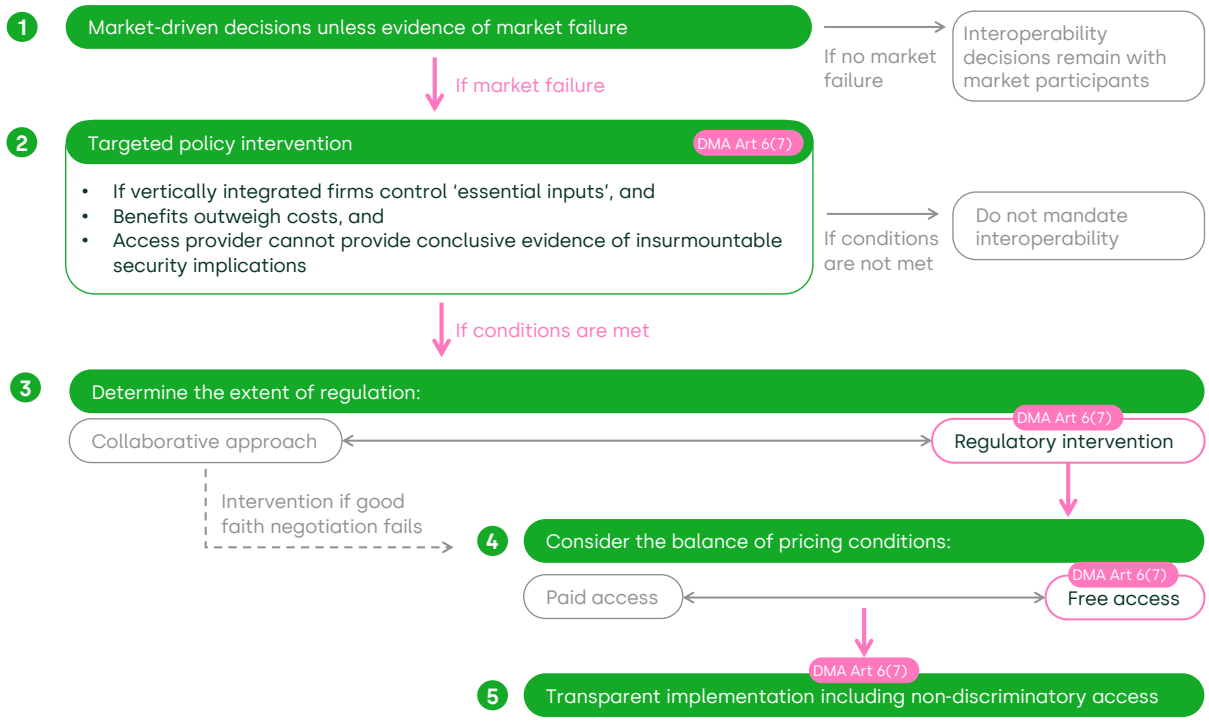
The gatekeeper shall allow providers of services and providers of hardware, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via the operating system or virtual assistant listed in the designation decision pursuant to Article 3(9) as are available to services or hardware provided by the gatekeeper. Furthermore, the gatekeeper shall allow business users and alternative providers of services provided together with, or in support of, core platform services, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware or software features, regardless of whether those features are part of the operating system, as are available to, or used by, that gatekeeper when providing such services.

The gatekeeper shall not be prevented from taking strictly necessary and proportionate measures to ensure that interoperability does not compromise the integrity of the operating system, virtual assistant, hardware or software features provided by the gatekeeper, provided that such measures are duly justified by the gatekeeper.

[88] ETSI (2007), 'Intellectual Property Rights (IPRs)', accessed 8 November 2024.
[89] See Article 61(3), which specifies that national regulatory authorities may impose obligations to provide access to network infrastructure to promote competition and ensure end-user benefits. EU (2018), 'Directive (EU) 2018/1972 establishing the European Electronic Communications Code', Article 61(3), accessed 8 November 2024.
[90] EU (2018), 'Directive 2014/53/EU of the European Parliament and of the Council', Article 10(8), accessed 8 November 2024.
[91] DMA, Article 6(7).

As reflected in the wording of Article 6(7), principles 1 to 4 of our generic framework have already been addressed by the DMA in the context of interoperability for OSs and virtual assistants. Principle 5, however, remains under consideration as the EC shifts its focus to implementation. Figure 5.2 illustrates how the provisions of Article 6(7) align with our five-step generic framework. This alignment is further analysed in the remainder of this section.

Figure 5.2 Article 6(7) and its intersection with the five-step framework



Source: Oxera.

With regard to principles 1 and 2, the EC has decided that targeted policy intervention is required in specific areas. Article 6(7) applies only to firms that are vertically integrated and that govern access to two well-defined CPS, namely the OS and the voice assistant. These were considered to be important access points for third-party hardware providers and the risk of misaligned business incentives was identified due to the gatekeeper's dual role as provider of the CPS and as a competitor.

As of the end of 2024, Article 6(7) applied to three gatekeepers with an OS: Apple (iOS and iPadOS), Google (Android OS) and Microsoft (Windows OS). To date, no gatekeepers have been designated with a voice assistant service.

With respect to principle 3, and the level of intervention that was decided upon, the legislator has decided that regulatory intervention is needed. However, it has adopted a non-prescriptive approach by establishing a feature parity obligation, rather than specifying individual features in the first instance, as the DMA is aimed at being self-

enforcing with the gatekeeper initially left to decide how to comply. That said, the DMA does have the necessary provisions to intervene if a collaborative approach does not result in effective implementation. For instance, as we discuss in section 6, in order to pre-empt arguments that Article 6(7) is not prescriptive enough to be directly enforced, the EC is intervening through specification proceedings to provide guidance on how to comply.[92] For example, specifying that a proactive interoperability by design approach should apply to new features, and that request based systems (whereby the third-parties submit tickets to the gatekeeper) may present difficulties and delay.[93] Moreover, there are other mechanisms in the DMA that can be used if needed: the EC can issue warnings, impose fines or periodic penalty payments against non-compliant firms.[94]

When it comes to principle 4 and the chosen pricing conditions, the legislators decided to mandate free access for interoperability in the application of Article 6(7) obligations (i.e. for features exclusively available to gatekeepers with OSs designated as CPSs).

Finally, the obligation to provide effective interoperability under Article 6(7) is in line with principle 5 of our framework: effective and transparent implementation. In the next section, we discuss how this works in practice and how this can be best implemented.

[92] DMA Article 8(2).
[93] European Commission, (2024), 'Digital Markets Act: Regulation (EU) 2022/1925 of the European Parliament and of the Council', Article 20(1) Regulation (EU) 2022/1925, CASE DMA.100204, SP – Apple - Article 6(7) – Process, 19 September, paras. 19-20.
[94] DMA Articles 29, 30 and 31.

6 Policy recommendations for effective implementation of hardware interoperability under Article 6(7)

As discussed in the earlier sections of this report, smartphones have become indispensable tools for consumers, serving as central hubs for a wide array of complementary devices. These connected devices—ranging from wearables to smart home gadgets—extend the functionality of smartphones, enabling diverse applications and services that are integral to daily life. At the heart of this ecosystem lies the smartphone OS, which plays a critical role in determining the extent of functionality available to users and third-party device manufacturers. It governs permissions, protocols and access to features, thereby influencing competition and innovation in the hardware and software markets.

In response to Article 6(7) and the obligations placed on OS providers, Google, as the operator of Android, conducted an internal audit and reported that their OSs were compliant with the requirements of the DMA from the outset—likely due to its more open ecosystem approach (see Box 2.5).[95] In contrast, Apple, known for its closed ecosystem, outlined plans to introduce APIs and a request-based process for third-party requiring interoperability.[96] However, this approach drew criticism from several third-party wearable manufacturers, who subsequently made informal complaints to the EC.[97]

As a consequence, the EC launched two specification proceedings in September 2024 to specify the obligations that Apple must take to ensure interoperability with iOS and iPadOS. These proceedings will formalise the regulatory dialogue between the EC and Apple, and will also provide guidance on how to fulfil the interoperability obligations, focusing on two key areas.[98]

- The first proceeding focuses on several connectivity features and functionalities, predominantly used for and by connected devices. The EC intends to specify how Apple will provide effective interoperability with functionalities such as notifications, device pairing and connectivity.
- The second proceeding focuses on the process Apple has set up to address interoperability requests submitted by developers and third parties for iOS and IPadOS. The EC will focus on the transparency, timeliness and fairness of the access process to provide interoperable hardware and software.

[95] Google Ireland Limited (2024), 'DSA Audit Implementation Report', accessed 9 December 2024; Microsoft (2024), 'Microsoft Compliance Report – Annex 10 – Windows PC (Operating System)', accessed 9 December 2024.
[96] Apple (2024), 'Apple's Non-Confidential Summary of DMA Compliance Report', 7 March, accessed 9 December 2024; Apple (2024), 'Apple's Non-Confidential Summary of DMA Compliance Report', 1 November, accessed 9 December 2024.
[97] MLex, (2024), 'Wearable makers criticize Apple's 'opaque' interoperability reviews under EU's DMA', 31 July, accessed 13 January 2025.
[98] European Commission (2024), 'Commission starts first proceedings to specify Apple's interoperability obligations under the Digital Markets Act', 19 September, accessed 9 December 2024.

As set out in section 5.2, principles 1 to 4 of our general framework have already been decided upon by the EC and embedded in the wording of Article 6(7). However, principle 5—its implementation—is now the EC's focus. Drawing from the lessons on hardware interoperability across various sectors and products that are discussed throughout this report, this section offers a set of recommendations for the effective implementation of Article 6(7).[99] These recommendations are structured into three critical areas.

- **First, there needs to be non-discriminatory access** for third parties to the same functionalities and technologies as used by the gatekeeper. In practice, this will involve opening access to relevant APIs (and documenting them accordingly), and either opening access to the proprietary technology or adopting industry standards.
- **Second, there needs to be accountability and collaboration on security and integrity** to mitigate the risks while enforcing the obligation of providing interoperability. In practice, there will need to be fair processes to screen access seekers, plus certification and verification mechanisms; however, these should avoid being unduly burdensome. Throughout the entire process, the gatekeeper needs to be timely, proactive and transparent about any potential issues and will need to collaborate with other stakeholders to find solutions that allow for effective interoperability. We recommend that the burden of proof should lie with the gatekeeper to identify and address such concerns collaboratively with stakeholders. In cases of dispute or delays, regulatory review of security issues may be warranted.
- **Third, users need to be given the ability to choose** in an informed way between different products and services—for instance, how they want to use their different devices. This requires the design and implementation of non-discriminatory, user-friendly choice architecture that does not favour gatekeeper devices over those of third parties.

As of December 2024, the EC has sent preliminary findings to Apple in the context of these two proceedings. These act as an intermediate step which allows Apple and third parties to provide feedback on the EC's proposals. Many of the EC's proposed measures align with our three recommendations, are cross-referenced in subsections below, and address features and technologies discussed in sections 2-4 of this report. A detailed comparative analysis of our recommendations and the EC's proposals is beyond the scope of this report.

6.1 Non-discriminatory access to interoperability with the OS

Article 6(7) requires gatekeepers to allow:[100]

effective interoperability with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via the operating system […] as are available to services or hardware provided by the gatekeeper.

[99] We note that while interoperability and data portability are two distinct concepts, there is complementarity between them. Our recommendations for pursuing interoperability may therefore also facilitate data portability under Article 6(9) of the DMA. By improving the compatibility of systems, interoperability can make it easier for consumers to transfer their data between services, thereby supporting the objectives of data portability outlined in Article 6(9).
[100] DMA, Article 6(7).

In line with our proposed principle 5 in section 5, this obligation sets the basis for non-discriminatory access to the features accessed and controlled though the OS, ensuring parity between gatekeepers and their competitors for similar functionalities.

It is important to note that distinctions between the OS and middleware layers may not always be clear. Gatekeepers should not sidestep interoperability requirements in the way they define the OS. CERRE (2023) highlights that compliance with Article 6(7) can be done either by ensuring access to the same features on an equal basis or by ensuring 'equivalence' of functionality—where the same capabilities are accessible to third parties even if provided at a different level.[101] Similar to the latter, Morton et. al (2023) propose the use of 'equitable interoperability', which mandates only the ability to interface and leaves companies with the flexibility to design their products. However, this approach would require the oversight of a regulator to determine if (i) the qualitative aims of interoperability have been achieved, and (ii) when new advances should be included in the scope of equitable interoperability.[102]

In cases where the gatekeeper cooperates in good faith, the equivalence or equitable options can be effective solutions that preserve innovation incentives for the gatekeeper. However, the drawback is that it may require more effort from the regulator to monitor and would need periodic updates. Where parties' incentives are not aligned, **equality of access** may be required by default in order to ensure that other solutions are not misused by the gatekeeper to circumvent the interoperability obligation. As discussed in Box 4.3, Apple's integrated ecosystem highlights the risk of favouring proprietary devices, as the company's monetisation model is closely tied to proprietary complementary products and exclusive features. Moreover, internal Apple teams can access a broader range of functionalities than third-party developers, creating an inherent competitive advantage in the development of their apps and devices.[103]

In its December 2024 proposal, the EC specified that Apple must ensure interoperability solutions provided to third-party developers are 'equally effective' as those used for its own services and hardware.[104] However, the EC acknowledges that Apple may utilise a distinct solution for its own services or hardware rather than applying the same interoperability solution made available to other developers.[105]

The examples presented throughout this report illustrate that Apple has not entirely restricted third-party interoperability, but has historically offered limited or less favourable access to certain OS features and APIs. To address these issues, we propose

[101] CERRE (2023), 'Horizontal and Vertical Interoperability in the DMA',
[102] Scott Morton, F., Crawford, G., Crémer, J., Dinielli, D., Fletcher, A., Heidhues, P. and Schnitzer, M. (2023), 'Equitable interoperability: The "Super Tool" of Digital Platform Governance', *Yale Journal on Regulation*, **40**:3, p. 1016.
[103] Scott Morton, F., Crawford, G., Crémer, J., Dinielli, D., Fletcher, A., Heidhues, P. and Schnitzer, M. (2023), 'Equitable interoperability: The "Super Tool" of Digital Platform Governance', *Yale Journal on Regulation*, **40**:3, p. 1040.
[104] European Commission, (2024), 'For public consultation: in case DMA.100203 – Article 6(7) - Apple – IOS – SP – Features for connected physical devices', 18 December, para. 31(e).
[105] European Commission, (2024), 'For public consultation: in case DMA.100204 – SP - Apple - Article 6(7) – Process', 18 December, para. 52.

operationalising non-discrimination by (i) properly documenting the APIs needed for interoperability, and (ii) giving access to the same features and technologies for the purpose of interoperability in Article 6(7) by opening the proprietary technology or adopting a set of industry standards.

6.1.1 Documentation of APIs

Effective API access and documentation plays an important role in achieving interoperability under the DMA. APIs serve as the technical bridges allowing third-party devices to connect and interact with the gatekeeper's ecosystem. Incomplete or unclear documentation can create significant technical barriers, hindering third parties' ability to implement or maintain interoperability.[106] A solution to this is the introduction of comprehensive documentation detailing the technical specifications and compliance requirements necessary for third-party developers and manufacturers to engage with interoperable systems effectively. For example, to enable interoperability for Open Banking, a dedicated and comprehensive repository of information was set up.[107] This recommendation for complete, accurate and well-documented APIs is also in line with the proposals made by the EC.[108]

Transparency in access to APIs and the necessary documentation reduces ambiguity, prevents disputes and fosters a cooperative environment among the stakeholders (see section 6.2). For example, as described in Box 6.1 below, Apple's wearables ecosystem highlights the challenges posed by inadequate API access, which creates inefficiencies on the developers' side and, by extension, affects the attractiveness of a third-party device. In this case, developers have reported difficulty accessing APIs related to messaging on iOS (e.g. iMessage, SMS, MMS) or have not been able to achieve feature parity with Apple's devices in terms of connectivity.

6.1.2 Opening access to the technology used by the gatekeeper

Recital 96 of the DMA states that where appropriate and necessary, the EC could request European standardisation bodies to develop technical standards.[109] However, in line with the DMA's goal to be self-enforcing and non-prescriptive, it leaves the initial decision on how to comply to the gatekeeper. To achieve non-discriminatory access for the purpose of interoperability under Article 6(7), the gatekeeper can either open access to its proprietary technology or adopt and implement industry-wide standards by modifying its own processes/products.

A useful parallel can be drawn with the telecoms sector, where access to incumbent infrastructure is key to promoting competition and interoperability. For example, in the UK,

[106] Meng, M., Steinhardt, S. and Schubert, A. (2020), 'Optimizing API documentation: Some guidelines and effects', Proceedings of the 38th ACM International Conference on Design of Communication, October.
[107] Open Banking (2017), 'Documents Archive', accessed 12 December 2024.
[108] European Commission, (2024), 'For public consultation: in case DMA.100203 – Article 6(7) - Apple – IOS – SP – Features for connected physical devices', 18 December, para. 31(f).
[109] DMA, Recital 96.

BT Openreach is required to grant access to its network of physical cables and infrastructure to competing service providers on an equivalent basis.[110] This ensures that all access seekers, including BT's competitors, can use the same underlying infrastructure as BT itself, fostering a level playing field. Similarly, for interoperability under the DMA, a gatekeeper providing non-discriminatory access to its proprietary technology would ensure that all users—whether third parties or the gatekeeper's own services—benefit from equivalent conditions.

As discussed in section 4.1, a firm may try to differentiate by adopting different standards or introducing new technologies. The obligation to provide interoperability in Article 6(7) means that, in future, gatekeepers will be forced to consider their innovations from a broader perspective (i.e. making sure that the feature or technology used is not accessible just to itself but also to third parties on an equal basis). According to CERRE (2023), gatekeepers are well positioned to design and manage interfaces in the short term, offering immediate solutions to the current requests for interoperability.[111] Looking ahead, this need to design features and permissions in the OS to enable access on an equal basis may reduce gatekeepers' first-mover advantages and increase the time to bring the new feature/products to market, but it enhances user choice by ensuring that new features are accessible across different providers.[112,113]

Alternatively, the gatekeeper can collaborate with third parties and the broader industry to develop new standards, ensuring compatibility and creating a shared foundation from the start. This approach minimises the need for costly adjustments or redesigns on the part of either the gatekeeper or access seekers, streamlining the process for all stakeholders. However, it can take longer to arrive at a common solution, as discussed in section 4.1.

[110] BBC News, (2016), 'Ofcom tells BT to open up cable network to rivals', accessed 12 December 2024.
[111] CERRE (2023), 'Horizontal and Vertical Interoperability in the DMA'.
[112] CERRE (2023), 'Horizontal and Vertical Interoperability in the DMA'.
[113] While the EC December 2024 proposed measures do not require Apple to provide third parties with the exact same interoperability solutions used for its own services and hardware—only that they be equally effective—it does specify that Apple must make beta versions of updated solutions available to third parties as soon as they are available for any of Apple's own connected physical devices. See European Commission, (2024), 'For public consultation: in case DMA.100203 – Article 6(7) - Apple – IOS – SP – Features for connected physical devices', 18 December, para. 31(l) and European Commission, (2024), 'For public consultation: in case DMA.100204 – SP - Apple - Article 6(7) – Process', 18 December, para. 52.

Box 6.1 Case study: APIs in wearable ecosystems

By not providing sufficient API documentation, Apple is posing a challenge for external developers. Third-party wearable devices are currently unable to fully integrate with Apple's wearables ecosystem. Specifically, when developers create an app for devices such as third-party smartwatches, they cannot use the existing Apple Watch APIs to communicate with those apps.

One area where several developers' iOS interoperability efforts have been hindered is messaging on wearables. While several other obstacles persist, by not documenting APIs for key messaging functionality, Apple has prevented developers from even requesting functionality that is available to Apple first-party devices—in particular, functionality that would allow a user to properly receive and interact with messages whose data is being processed on iOS (i.e. iMessage, SMS and MMS data).

Consequently, each third-party wearable manufacturer must develop its own APIs for every app with which it wishes to interact. This limitation increases the development workload for wearable companies, whose app developers may need to accommodate multiple APIs to support different devices. Inefficiencies arise and more resources are required for app development.

Allowing third-party wearables to participate in Apple's ecosystem would enable valuable functionalities. Crucially, seamless data synchronisation could be allowed between iPhone apps and third-party wearables without requiring internet access or explicit user actions on each device. This integration would enhance the user experience by facilitating more efficient and automated interactions between devices and increased choice for iOS users.

Source: Oxera based on Binder, M. (2024), 'Apple may be forced to stop blocking third parties from accessing Siri and more', Mashable, accessed 29 November 2024; Song, V. (2024), 'Smartwatches shouldn't make you choose between Apple and Android', The Verge, accessed 29 November 2024; Weatherbed, J. (2024), 'Apple put on notice over support for third-party watches and headphones', The Verge, accessed 29 November 2024.

6.2 Accountability and collaboration on security and integrity

Opening up integrated systems or adding additional parties through interoperability introduces additional challenges, but often these are not insurmountable. Article 6(7) specifies that, in order to safeguard the security and integrity of the OS to be opened, gatekeepers should not be prevented from taking 'strictly necessary and proportionate measures […] provided that such measures are duly justified by the gatekeeper.' This part

of the regulation should not be read as providing the gatekeeper with an excuse to avoid or delay interoperability, but rather as an impetus to collaborate to find solutions and ensure compliance. To this end, we make two recommendations: (i) the gatekeeper should carry the burden of proof to describe and motivate these challenges; and (ii) for certain forms of interoperability, proportionate certification and verification mechanisms need to be put in place to screen access seekers using a fair process.

6.2.1 The gatekeeper should carry the burden of proof on security and integrity

Under Article 6(7), the wording justifies the gatekeeper taking 'measures' to protect security and integrity. However, security and integrity concerns, as highlighted in section 4.1.2, are often invoked as reasons to restrict interoperability. To address this, a clear and detailed understanding of these concerns is needed to assess the validity of the 'measures' taken by the gatekeeper. As the developer of the OS (and, in Apple's case, also the manufacturer of the device using the OS) the gatekeeper is in the best position to identify where challenges to security and integrity can arise through hardware interoperability. We recommend that this means that the gatekeeper bears the primary responsibility for demonstrating specific security risks associated with hardware interoperability when such risks arise.[114]

However, the gatekeeper's assessments should be subject to a critical standard of evaluation to be shared with the regulator (and/or existing security and privacy regulators) and with access seekers who then can assess its validity and provide useful input before the regulator takes a decision.

An example of such a process can be found in the regulation of oil and gas infrastructure in the UK.[115] When a dispute arises between an access seeker and an infrastructure owner, the infrastructure owner is required to provide detailed information to the regulator. This includes both technical and commercial details, such as the reasons for refusing access to the service, technical reviews or studies conducted (for example, incompatibilities in specifications), any statements of capacity in cases where capacity constraints are cited, and an estimate of the business risks associated with accommodating the applicant's production.[116]

The regulator then reviews this information as part of its decision-making process. It evaluates whether the refusal is justified or if access should be granted, taking into account the evidence provided by the infrastructure owner and any input from the access

[114] We recommend that the gatekeeper should be responsible for considering and responding to all reasonable requests for interoperability. In cases where the gatekeeper receives large volumes of requests that they deem irrelevant or invalid, they may provide a brief and cursory response or denial to avoid undue burden. In such cases, the third party should retain the right to challenge the gatekeeper's decision, for example, through a dispute resolution mechanisms (as outlined below).
[115] North Sea Transition Authority (2022), 'Guidance on Disputes over Third Party Access to Upstream Oil and Gas Infrastructure', 7 November.
[116] North Sea Transition Authority (2022), 'Guidance on Disputes over Third Party Access to Upstream Oil and Gas Infrastructure', 7 November, Annex 3.

seeker. This process ensures a balanced resolution of disputes, with the regulator making the final determination.

This recommendation is broadly aligned with the EC's suggestion, which proposes that developers be adequately informed when interoperability requests are rejected or when Apple's proposed interoperability solution does not fully meet the request. The EC further recommends that, in relevant cases, developers should have the opportunity to contest such decisions through a fair and impartial mechanism, including a conciliation process where a neutral third party provides a non-binding opinion on the dispute.[117]

Transparency is crucial during these discussions, acknowledging that while proprietary information may need protection, it should not hinder compliance. The solution can involve delineating well-defined groups of stakeholders that can access different levels of confidential information while non-confidential information should be provided to all interested third parties.

To address some of the most common concerns when it comes to security and integrity risks, the gatekeeper will need to put in place additional mechanisms of screening and monitoring. These are discussed below.

6.2.2 Fair process for certification and verification mechanisms

Article 6(7)'s interoperability mandate may support a fair and controlled process for certification and verification mechanisms. For certain forms of interoperability, screening access seekers and defining their permitted actions are essential steps to safeguard against malicious actors and ensure that activities remain within approved boundaries. Ideally, following this approval process, third-party access seekers should not face significant ex ante risks beyond those encountered by the gatekeeper when offering similar services or interoperable products through the regulated OS.

Lessons from other industries demonstrate that robust security issues can be effectively managed through certification schemes that can be accessed through a fair and transparent process. For example, in Open Banking in the UK, a third-party verification process was established to ensure that only trusted participants gained access.[118] Through verification and registration, plus mandated Sandbox testing prior to full access, it ensured that only authorised entities could participate and that all interactions adhered to agreed technical and security standards.

The certification mechanism can be administered in a non-discriminatory way by the gatekeeper, it can involve independent third parties or can be a collaboration with external providers. For example, in the case of Article 7 of the DMA, which mandates a gatekeeper to provide interoperability for number-independent interpersonal communications services, Meta had to address challenges regarding end-to-end encryption that balance compliance

[117] European Commission, (2024), 'For public consultation: in case DMA.100204 – SP - Apple - Article 6(7) – Process', 18 December, paras. 6(b) and 43.
[118] Open Banking (2023), 'Regulatory', accessed 9 December 2024.

with operational integrity and user safety. Meta worked on a solution set out in a reference offer that uses the Signal Protocol as a foundation of secure communication, along with a stringent process of verification both at the start and during the use of the interoperable service. Meta's approach shows that solutions for interoperability can be designed to coexist with robust security and privacy standards while providing seamless cross-platform messaging experiences as mandated by the regulator.

While verification and certification programmes are important to safeguard security, the process must be fast and transparent. Otherwise, it risks becoming a tool for gatekeepers to circumvent or delay interoperability. The conditions for verification should be clear and well communicated to all parties, with any concerns communicated promptly to the access seeker. Although this may impose regulatory burdens on both gatekeepers and access seekers, such costs are necessary to ensure a fair and functional interoperability framework.

While the EC does not propose a verification and certification programme for third parties, it proposes that Apple's request-based process is also designed to be timely, with provisions to ensure adequate support for third parties and minimise transaction costs associated with the process.[119]

Overall, examples from industry demonstrate that collaborative and innovative approaches can address many, if not most, security challenges, with the regulator intervening in instances where security disputes are escalated. In addition, the adoption of certification and verification processes can help regulators to balance openness with security, fostering trust and enabling effective collaboration across various ecosystems.

6.3 Giving the user the power to choose through transparent consent requests

We highlighted in section 3 that end-users are potentially one of the largest beneficiaries of hardware interoperability through improved user experiences, reduced search and transaction costs, and increased choice. As such, we consider that consumers have to play a role in the effective interoperability mandated under Article 6(7). To empower them to do so, we recommend that, where necessary, users are presented with consent forms for interoperability that represent (i) transparent communication with the users, and (ii) neutral consent request for interoperability.

The EC's December 2024 proposals are largely aligned with this approach. They specified that Apple should not introduce friction, such as by providing non-neutral prompts, requiring multiple successive permission prompts where a single prompt would suffice, or

[119] European Commission, (2024), 'For public consultation: in case DMA.100204 – SP - Apple - Article 6(7) – Process', 18 December, para. 5.

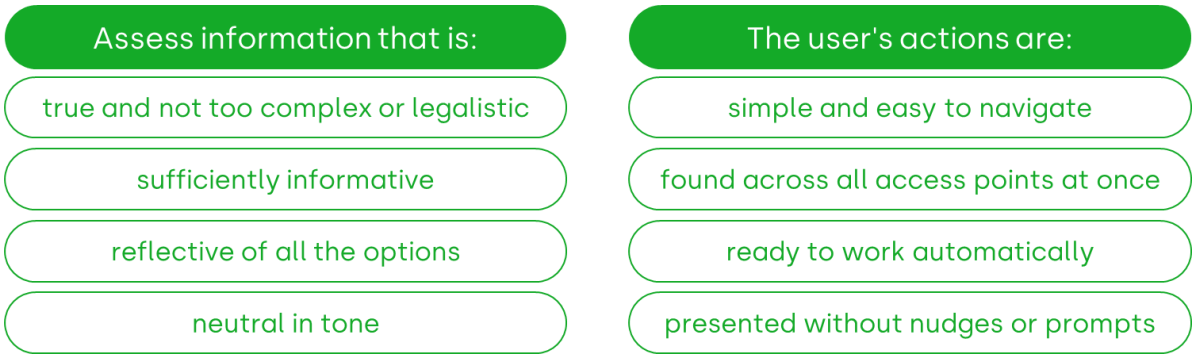
misrepresenting the risks associated with using a third-party physical device, among other measures.[120]

6.3.1 Adopt transparent communication with the users

For certain types of interoperability, it may be appropriate to require the user to take certain actions to grant permissions during the device set-up stage (e.g. setting up a third-party headset that needs to access certain connectivity features on the smartphone), or to grant access to the hardware on their device for a third-party app of their choosing (e.g. a third-party wallet that needs access to the NFC chip).

Fletcher and Vasas (2023) highlight that the design of choice architecture plays an important role in the extent and quality of the consumer choice activity and thus has an impact on the effectiveness of the DMA.[121] The information the user receives should follow best practice when it comes to the content, format, timing and frequency of the prompts. As summarised in Figure 6.1 below, Fletcher (2024) outlines several good-practice principles for the choice architecture of the user prompts.[122] For example, users need to be presented with information that is true, avoids complex language and is neutral in tone. Any warnings should be accurate and not disproportionately prominent. When a user needs to act, the navigation flow should be simple, without unnecessary steps, delays or friction. For example, presenting multiple screens or unnecessarily complex steps can deter user engagement and can affect the effectiveness of interoperability.

Figure 6.1 Best practice for online choice architecture for user prompts



Source: Oxera based on Fletcher, A. (2024), 'Choice architecture for end users in the DMA', CERRE, January, section 4.

[120] European Commission, (2024), 'For public consultation: in case DMA.100203 – Article 6(7) - Apple – IOS – SP – Features for connected physical devices', 18 December, para. 31(f).
[121] Fletcher, A. and Vasas, Z. (2023), 'Implementing the DMA: The Role of Behavioural Insights', 5 July.
[122] Fletcher, A. (2024), 'Choice architecture for end users in the DMA', CERRE, January, section 4.

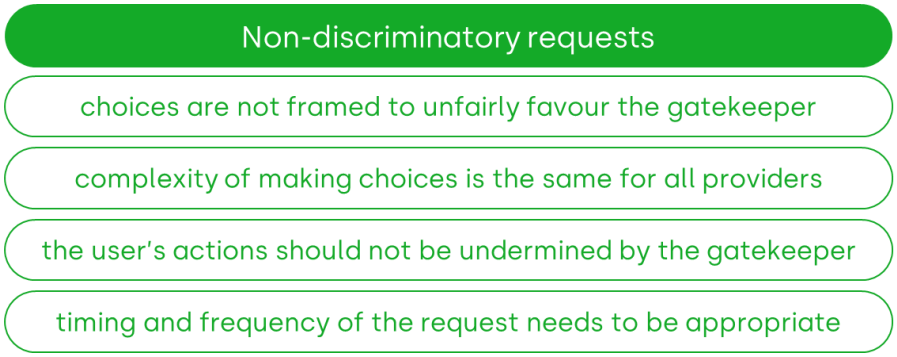
When it comes to the types of messages that gatekeepers should display, CERRE (2023) suggests that there is an interaction between the degree of certification and verification of the third parties (discussed in section 6.2) and the need for additional warning messages for users. It suggests that a stringent certification and verification process could replace the need for warning messages to be delivered to the users. While this is an appropriate solution, the gatekeeper should still have the ability to intervene and inform the user in case it becomes aware of inappropriate conduct by a third party that received access to interoperate.

6.3.2 Use neutral consent requests for interoperability

In line with the contestability objectives of Article 6(7), the way third-party providers of services and hardware, interoperating with the gatekeeper's CPS, are presented is crucial to the user's choice architecture. Any communication should ensure that both the gatekeeper and third parties are equally represented in terms of offering choices to end-users.

Fletcher (2024) outlines several best practices for this, as illustrated in Figure 6.2 below. [123] For instance, choices should not be framed to favour the gatekeeper, which means avoiding biased ranking or prominence. Further guidelines suggest that user prompts should maintain the same flow for all providers, with no follow-up actions by the gatekeeper that could undermine the user's ability to choose a third party. The timing of prompts should also avoid exploiting short attention spans.

Figure 6.2 Best practice for designing non-discriminatory user prompts



Source: Oxera based on Amelia Fletcher (2024), 'Choice architecture for end users in the DMA', CERRE, January, section 4.

There is ongoing debate about whether the gatekeeper or third-party provider should control the communication. Fletcher (2024) argues that, while third parties might benefit

[123] Fletcher, A. (2024), 'Choice architecture for end users in the DMA', CERRE, January, section 4.

from controlling the content and format, it could improve user comprehension to have a consistent format across all providers, including the gatekeeper.[124] This approach would also reduce the risk of dark patterns being used to nudge users toward choices not in their best interest.

In the context of Article 6(7) there should be no difference between the way in which the access seeker and the gatekeeper request permissions from the user. The third party may be best placed to control the messaging to the user so that it has a chance to explain how interoperability works with its product; however, when it comes to enabling certain technical features, for consistency there could be a standard screen that is used by both the gatekeeper and the access seeker.

[124] Fletcher, A. (2024), 'Choice architecture for end users in the DMA', CERRE, January, section 4.1.3.

Contact

Johan Keetelaar
Senior Adviser
+31(0) 20 899 1104
johan.keetelaar@oxera.com

oxera.com