discribe
IMAGINING SECURE DIGITAL FUTURES

Secure Hardware Adoption in the Open Data Context

Dr. Wing Man Wynne Lam
Dr. Jacob Seifert

April 2023

University of East Anglia

UNIVERSITY OF LEICESTER

The Discribe Hub+ is funded by UKRI through ESRC
Grant no: ES/V003666/1
For more information about the Hub+ please visit
www.discribehub.org

UK Research and Innovation

Acknowledgements

We thank the Digital Security by Design Social Science (Discribe) Hub+, and particularly Awais Rashid, Daniel Page and Nicola Lloyd, for their extensive support throughout this project. We sincerely thank our industry partner LNDSR (Steve Williams) for the valuable insights they have brought to this work. Finally, we are indebted to our interview participants for their time and valuable contributions.

Contents

Executive Summary

Hardware security has a fundamental role to play in protecting the IT systems that underlie today's digitalized society. In this report we take an economic approach to hardware security by investigating the factors that influence firms' decisions to adopt secure hardware. We also study the way in which the data governance framework can be used to bring firms' privately-optimal (profit-maximizing) adoption incentives into line with those that maximize the well-being of society as a whole. This economic approach is an important complement to the computer science perspective on hardware security that focuses on developing secure technologies.

We study the determinants of firms' secure hardware adoption decisions in the context of Open Banking (OB) and related Open Data (OD) markets in which third-party providers (TPPs) are granted access to the data that firms collect about their customers. While this form of data sharing has the potential to generate significant benefits, it is also exposes consumer data to cyber-risks. Given the particularly sensitive nature of the data involved in OD markets such as banking and energy, it is important to understand how firms' hardware adoption decisions interact with their data sharing choices. These interactions matter when it comes to understanding the indirect effects that data governance measures targeting firms' data sharing activities may have on their secure hardware adoption decisions, for example.

The background to this investigation of secure hardware adoption incentives in OD markets is provided in the form of an overview of the existing UK data governance framework. This framework describes not only the features of existing OD schemes and the role that security plays within them, but also the rules, regulations, standards and guidance that influence firms' behaviour with respect to cybersecurity, data privacy, anonymization, interoperability, data ethics and responsible innovation more broadly.

We then approach the question of secure hardware adoption incentives from two methodological perspectives. First, we analyse primary data that was collected in a series of interviews with industry participants. This analysis provides detailed insights into the factors that promote and hinder secure hardware adoption in OD markets, as well as the strengths and weaknesses of the existing data governance framework.

Several open questions emerge from this primary data analysis, which we subsequently address using a novel game-theoretic model of hardware adoption and data sharing decisions in OD markets. We first clarify the nature of the interactions arising between firms' hardware

adoption and data sharing incentives and demonstrate that the former cannot be understood in isolation of the latter. We also derive the conditions under which market failures arise in terms of the under- or over-adoption of secure hardware and the over- or under-sharing of data relative to the social optimum. The model allows us to compare the effectiveness of data governance interventions targeting the benefits that firms derive from data sharing and the costs of secure hardware adoption, though we show that neither succeeds in correcting market failures completely. Finally, we use the model to show that, while competition tends to reduce the extent to which secure hardware is adopted and data is shared in OD markets, it may increase or decrease social welfare relative to monopoly. The report closes with an overview of important directions for future research in this area.

List of Abbreviations

AI	Artificial Intelligence
AISP	Account Information Service Provider
API	Application Programming Interface
ASPSP	Account Servicing Payment Service Provider
CA 2013	Communications Act 2013
CFPB	Consumer Financial Protection Bureau
CHERI	Capability Hardware Enhanced RISC Instructions
CMA	Competition and Markets Authority
DPA 2018	Data Protection Act 2018
DPDI	Data Protection and Digital Information Bill
EU	European Union
FAPI	OpenID Financial Grade API
FCA	Financial Conduct Authority
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
IoT	Internet of Things
MPAN	Meter Point Administration Number
MPRN	Meter Point Reference Number
NCSC	National Cyber Security Centre
OB	Open Banking
OBIE	Open Banking Implementation Entity
OBS	Open Banking Standard
OD	Open Data
OECD	Organisation for Economic Co-operation and Development
OES	Operator of Essential Services

NIS [Regulations]	Network and Information Systems [Regulations]
PCI DSS	Payment Card Industry Data Security Standard
PDB	Pensions Dashboard Programme
PECR	Privacy and Electronic Communications Regulations
PISP	Payment Initiation Service Provider
PSD2	Revised Payment Services Directive
PSRs 2017	Payment Services Regulations 2017
RDSP	Relevant Digital Service Provider
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
SWG	Strategic Working Group
SYSC	Senior Management Arrangements, Systems and Controls
TPP	Third-Party Provider

Part 1

Introduction

This report investigates the factors that influence firms' secure hardware adoption decisions. The importance of understanding firms' incentives to adopt secure hardware is underlined by the growing costs of cyber-crime. Globally, these are expected to reach $10.5-17.7 trillion annually by 2025 (Statista, 2022; World Economic Forum, 2023). At the same time, it is increasingly being recognized that mitigating these cyber-risks requires security that is implemented at the hardware level in addition to the software level (Intel, 2022; US Department of Commerce, 2022a). This report complements the computer science perspective on hardware security by studying the factors that influence firms' decisions to adopt secure technologies. We study this question in the particular setting of OB and related OD markets in which consumer data is shared with TPPs.[1] The importance of these markets lies in the sensitivity of the consumer data they are built on (e.g. bank transaction and energy consumption data) as well as the fact that data sharing creates new security threats that, in turn, affect the strategies that businesses adopt with respect to cybersecurity.

The Capability Hardware Enhanced RISC Instructions (CHERI) project illustrates the benefits of implementing security at the hardware level. CHERI extends conventional hardware instruction-set architectures with new features that enable fine-grained memory protection and scalable software compartmentalization.[2] In contrast to software patches that can correct individual coding vulnerabilities, CHERI and related hardware-based solutions have the potential to eliminate broad classes of vulnerabilities associated with common programming languages such as C and C++. Since hardware represents the physical foundation on which software and all other code is run, hardware security provides a baseline level of protection that affects the effectiveness of all higher-level security processes (US Department of Commerce, 2022b,c). In the case of CHERI, 31%-67% of vulnerabilities reported to the Microsoft Security Response Center in 2019 could be addressed in this way (Microsoft, 2020).

[1] This use of the OD term follows McKinsey & Company (2021) and Experian (2020). In the UK, 'Smart Data' is similarly used as an umbrella term for Open Banking and related schemes.

[2] See *https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/* for details.

While improvements to the security of a firm's IT systems reduce the risk of hackers gaining unauthorized access to consumer data, the voluntary sharing of consumer data between firms can generate substantial economic benefits (McKinsey & Company, 2016). This motivates the UK's Open Banking Standard, the revised Payment Services Directive (PSD2) of the European Union (EU), and the ongoing rulemaking process of the US Consumer Financial Protection Bureau (CFPB) in relation to financial data rights (CFPB, 2022). These OB frameworks create rules governing the sharing of customer data between financial institutions and TPPs that use this data to provide a range of account aggregation and payment services (US Department of Commerce, 2022a). In addition to generating economic benefits, the more widespread sharing of sensitive data also has the potential to generate security risks, however, for example when hackers exploit fraudulently-obtained data to submit unauthorized payment instructions. Moreover, extending the use of data by combining and porting different data sets between firms may create both security and privacy concerns (Forbes, 2012; Lam and Liu, 2020). Forbes (2012) explain how a data set on consumers' demographic characteristics, which may seem innocuous at first glance, can lead to more sophisticated and effective targeting of consumers when combined with targeted data sets capturing customers' credit card information and purchase histories. These combined data sets are invaluable not only to firms and advertisers but also to cyber adversaries, which further underlines the importance of hardware security in OD markets. Recent research has shown that 45% of retail banking customers and 54% of small business customers identify security as their biggest concern in relation to open banking data sharing (PwC, 2018).

It is anticipated that OD schemes will extend beyond payments in the future to cover a broader range of financial products such as savings and investments (Open Finance, see Deloitte, 2022) as well as new markets including telecommunications (Open Communications, see Ofcom, 2020), energy (Midata, see Ofgem, 2020) and pensions (see Pensions Dashboards Programme, 2022), see Figure 1. Moreover, the idea that increased data sharing can be a means of improving market outcomes extends beyond OD initiatives. Data sharing is seen as an important way for the UK's Digital Markets Unit to promote consumer welfare in digital markets, for example (HM Government, 2022a). Data sharing is also a key pillar of the UK's National Data Strategy (HM Government, 2020a; Frontier Economics, 2021), the EU Data Act (European Commission, 2022) and related policies globally (OECD, 2015, 2019). This further motivates our focus on secure hardware adoption in OD markets specifically and on the implications of data sharing for secure hardware adoption incentives more generally. Finally, our analysis of the interactions between secure hardware adoption and data sharing is applicable to the Digital Markets, Competition and Consumers Bill. This bill was introduced to the UK Parliament on April 25, 2023, and deals explicitly with the issue of regulatory coordination in digital markets.

The background to our investigation of secure hardware adoption incentives in OD markets

	Open Banking	Open Finance	Open Economy
Scope of Data	• Transactions Data • Accounts Data • 'Know Your Customer' Data	• Payroll Data • Insurance Data • Investments Data • Pension Data • Loans & Mortgage Data	• Travel Data • 'Internet of Things' Data • Social Data • Utilities Data • Government Data • Lifestyle Data • Healthcare Data • Personal Devices Data
Scope of OD Services	• Account Aggregation • Payments Initiation • Onboarding • Personal Financial Management	• Service Switching • Buy Now, Pay Later • Cashflow-based Lending • Employee Benefits • Enhanced Credit Scoring • Round-up Investments • Automated Tax Filing • Micro-insurance	• Lifestyle Goals • Personalized Discounts • Behaviour-driven Rewards • Carbon Footprint Tracker • Utility Services Switching • Customized Travel Solutions • Subscription Management • Rental Management • Public Benefit Schemes • Healthcare Financing

Figure 1. From OB to the Open Economy
(Sources: Mod5r, WhiteSight, Panagiotis Kriaris)

is provided in the form of a review of the UK data governance framework. The data governance framework describes the rules, regulations, standards and guidance covering cybersecurity, data privacy, anonymization, interoperability, data ethics and responsible innovation that collectively determine the way in which firms can use data (The Royal Society, 2020). We also discuss the specific features of OB and related OD schemes in this connection.

We begin our investigation of secure hardware adoption incentives by analysing primary data that was collected in the course of a series of interviews with regulators and private firms in a variety of relevant industries. These interviews emphasize that security is an important driver of firms' hardware adoption decisions. They also highlight deficiencies in the speed at which secure hardware is currently being adopted, however, suggesting that the market might not provide adequate incentives for firms to adopt secure hardware. A number of detailed recommendations also emerge from this data concerning the factors that drive firms' decisions to adopt secure hardware, the effect of competition on hardware adoption decisions and the optimal design of the data governance framework.

Several open questions emerge from this primary data analysis, which we address using a novel game-theoretic model exploring hardware adoption and data sharing decisions in OD markets. These open questions concern hardware adoption incentives and the nature of market failures in OD markets, the effectiveness of data governance interventions in correcting these market failures and the impact that competition has on secure hardware adoption incentives and social welfare. We show, firstly, that OD schemes are important for hardware adoption

decisions in the sense that firms' incentives to adopt secure hardware are positively related to the degree of data sharing. We also make precise the nature of the market failures alluded to by our interview participants. In particular, we show that there are always cases in which the market leads to levels of hardware adoption and data sharing that fall short of those that maximize the well-being of society. When competing firms sell products that are sufficiently similar to one another, we also show that the market can generate hardware adoption and data sharing incentives in excess of the social optimum, however. We study data governance interventions that target the magnitude of the data sharing benefits that accrue to firms (e.g. by restricting the type of products that can be offered to consumers within OB) and the costs of hardware adoption. While both policies can have beneficial effects in terms of reducing the prevalence of market failures, neither succeeds in eliminating these market failures completely. Finally, we study the impact that market structure has on secure hardware adoption incentives. We show that competition tends to reduce both secure hardware adoption and data sharing, though it may increase or decrease social welfare.

The report is structured as follows. Part 2 provides an overview of the UK data governance framework. Part 3 presents our primary data analysis, before Part 4 discusses our theoretical results. Part 5 concludes.

Part 2

The UK Data Governance Framework

This part reviews the data governance framework applicable to firms operating in OD markets in the UK. This will encompass the frameworks underlying OB and related OD initiatives themselves (see Part 2.1) as well as the complementary system of rules, regulations and standards that apply more generally in the areas of cybersecurity, data privacy, anonymization, interoperability, data ethics and responsible innovation (see Part 2.2).

The purpose of this review is to highlight the roles played by regulation and market forces in determining secure hardware adoption and data sharing incentives in the OD context. This background will also motivate the economic setting of our theoretical model in Part 4.

2.1 The Open Data Context

OB is the most well-developed of the OD schemes currently operating in the UK and is the focus of Part 2.1.1. We then discuss extensions of OB into wider financial services (Part 2.1.2), as well as OD schemes currently planned or operating in the energy, communications and pensions markets (Parts 2.1.3 - 2.1.5).

2.1.1 Open Banking

The origins of OB in the UK lie in the EU's efforts to promote competition and innovation in the payments market. These efforts led to PSD2,[3] which was passed by the Council of the European Union in 2015 and was implemented in the UK from January 2018 onwards in the form of the Payment Services Regulations 2017 (PSRs 2017). PSD2 requires banks and other financial institutions (collectively, 'Account Servicing Payment Service Providers' or ASPSPs)

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

that provide payment accounts to customers to make their customers' financial data available, subject to consent, to TPPs of financial services.

TPPs include FinTechs and other new entrants to the payments market, consistent with the competition-enhancing goal of the original legislation, but also established banks and financial institutions. TPPs act as 'Account Information Service Providers' (AISPs) and 'Payment Initiation Service Providers' (PISPs) within the framework of PSD2. AISPs access consumer data in a read-only capacity and provide services such as account aggregation and budgeting tools. AISPs can also allow customers to share their financial data for the purposes of credit and affordability checks in the course of a loan application, for example.

PISPs, on the other hand, are granted read/write access to consumer data. Authorized PISPs are permitted to initiate payments on behalf of a customer. This has applications in the consumer area, for example in the form of money management applications that automatically transfer funds between accounts to avoid overdraft fees. In the business domain, the services provided by PISPs can allow greater flexibility in the management of incoming and outgoing payments.[4]

The activities of both AISPs and PISPs within OB contrast with traditional banking insofar as data transfers and payment instructions no longer flow exclusively between the user and that user's bank. The nature of these interactions is illustrated in Figure 2 below.[5]

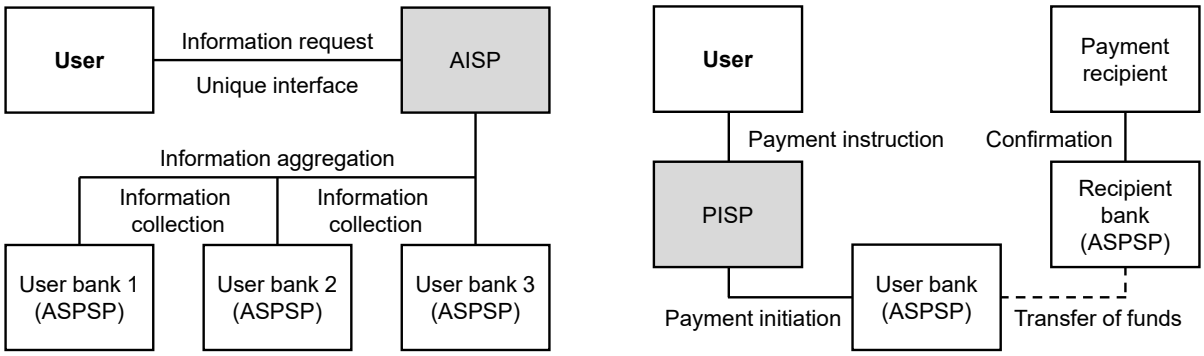


Figure 2. AISP and PISP account access models

The OB framework reflected in PSD2 and the PSRs 2017 creates a *right* on the part of consumers to make use of the services of AISPs and PISPs and a corresponding *obligation* on financial institutions to provide secure channels of communication that facilitate those transac-

[4] AISPs and PISPs must be registered with the Financial Conduct Authority (FCA). As of 21 February 2023, the FCA Financial Services Register contained 193 AISPs and 96 PISPs. See *https://register.fca.org.uk/s/search?predefined=AIPISP*.

[5] This figure is based on material accessible at *https://www.kearney.com/financial-services/the-open-banking-series/open-banking*.

tions. Two relevant provisions of the PSRs 2017 are highlighted below:[6]

> "A credit institution must grant payment service providers of the types referred to in paragraphs (a) to (f) of the definition of "payment service provider" in regulation 2(1), and applicants for authorization or registration as such payment service providers, *access to payment accounts services on an objective, non-discriminatory and proportionate basis*."
>
> Regulation 105(1), paragraph (a), PSRs 2017, emphasis added

> "Where a payer gives explicit consent in accordance with regulation 67 (consent and withdrawal of consent) for a payment to be executed through a payment initiation service provider, the payer's account servicing payment service provider *must communicate securely with the payment initiation service provider* in accordance with the regulatory technical standards adopted under Article 98 of the payment services directive."
>
> Regulation 69(2), paragraph (a), PSRs 2017, emphasis added

These provisions effectively make participation in OB compulsory for financial institutions in the UK, although, as discussed below, market forces still affect the manner in which they participate in OB.

Subsequent to the UK's departure from the EU, a number of amendments to the UK framework of payments regulation are expected. A review and Call for Evidence was launched in relation to the PSRs 2017 in January 2023 (HM Treasury, 2023). This consultation identifies several areas of potential reform, including the application of Strong Customer Authentication (SCA, discussed further below), settlement time frames, information requirements and termination practices. Given the EU's concurrent review of PSD2 with a view to implementing a further revised PSD3,[7] there is scope for significant EU-UK divergence in the area of payments regulation and OB in future.

Application Programming Interfaces

Secure data sharing within OB is facilitated by Application Programming Interfaces (APIs). The UK approach to developing APIs originated in the Competition and Market Authority's (CMA's) market investigation into retail banking, which published its final report in August 2016. Based on the conclusions of this report, the CMA ordered the nine largest UK banks at the time (the CMA9) to implement a common approach to OB based on the use of standardized APIs. The Open Banking Implementation Entity (OBIE) was established to oversee the development of

[6] See also Articles 66 and 67 of PSD2.

[7] See *https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-psd2-review_en*.

the resulting Open Banking Standard (OBS), which covers API and security-profile specifications in addition to customer experience and operational guidelines.[8] The API specifications contained in the Open Banking Standard include:

- **Read/Write API Specifications:** these specify how TPPs connect to banks for read access, for example when fetching balance information, and write access, when initiating payments.
- **Open Data API Specifications:** these set out how banks create access endpoints for TPPs. It defines how TPPs should be able to use a bank's read/write API.

This UK approach to API development and standardization is highly regulatory in nature, even compared to that of the EU, which, despite common ground in the form of the PSD2, has left the development of APIs largely to the market. Nonetheless, the OBS does not mandate a specific set of APIs that banks must use, rather banks develop their own APIs to comply with the requirements set out in the OBS.

Security Considerations

OB brings about significant security benefits relative to the alternative practice of screen scraping (credential sharing). Screen scraping involves consumers sharing their account access credentials with TPPs who use that information to access the accounts on their behalf. The drawbacks of this approach include the fact that sharing account usernames and passwords with a TPP enables it (and any other party with that information) to access significantly larger volumes of sensitive data than are typically required for the service in question. From the ASPSP perspective, banks and financial institutions remain solely liable towards their customers, even for losses that arise in connection with a TPP accessing customer accounts in the course of screen scraping (Deloitte, 2018). This highlights the importance of security within the OB setting. Screen scraping has now been superseded by a requirement for ASPSPs to provide a dedicated interface (an API) through which TPPs can access account details securely, see below.

Security aspects of OB are addressed in the security profiles that form part of the OBS. The authorization framework underpinning OB is built around the OpenID Financial Grade API (FAPI) specification, which provides implementation guidelines based on a REST/JSON data model protected by an OAuth profile, and Connect Client Initiated Backchannel Authentication that supports decoupled interaction methods.[9]

[8] The OBIE is a private body whose governance, composition and budget are determined by the CMA. It is funded by the CMA9 and overseen by the CMA, the FCA and HM Treasury. The transition to a future entity that will succeed the OBIE is currently in progress, see Joint Regulatory Oversight Committee (2023).

[9] Technical details of these security profiles are available at *https://standards.openbanking.org.uk/security-profiles/*.

An additional layer of payment security in OB is mandated in the form of SCA. This requirement is set out in Regulatory Technical Standards (RTS) that were originally created in conjunction with PSD2[10] and in Article 100 of the PSRs 2017:

> "A payment service provider must apply strong customer authentication where a payment service user–
>
> (a) accesses its payment account online, whether directly or through an account information service provider;
>
> (b) initiates an electronic payment transaction; or
>
> (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses."
>
> Regulation 100(1), PSRs 2017

All UK payment services providers were required to comply with the above provision and with the EU RTS from 14 September 2019. Subsequently, these technical standards have been replaced by technical standards on strong customer authentication and common and secure methods of communication that were created by the FCA in accordance with Regulation 106A of the PSRs 2017 (SCA-RTS). In practice, SCA implies a requirement for two-factor authentication whenever a customer accesses a payment account online, initiates a payment or carries out any action that could imply a risk of fraud.

More recent changes to the SCA-RTS have sought to balance the security provisions underlying OB against the usability of OB services (see FCA, 2021). The FCA's Policy Statement PS21/19 exempts customers using AISPs from the requirement to reauthenticate with their ASPSP every 90 days, for example, instead requiring them to confirm every 90 days that they still consent to the AISP accessing their account (Article 36(6) SCA-RTS). Other changes relate to the requirement for ASPSPs to develop dedicated interfaces rather than adapting existing online platforms for TPP use and to dynamic linking, which allows for minor revisions to transaction amounts subsequent to a transaction having been completed. These changes came into force March 2022.

Important security vulnerabilities nonetheless exist in OB. These place OB firmly within the scope of overarching legislation in the area of cybersecurity that will be discussed in Part 2.2. In particular, APIs are vulnerable to a variety of attacks that exploit the construction of the API interface to deposit malware, steal data and perform other types of unauthorized operations. Credential stuffing is one example, which uses stolen usernames and passwords to trick the API into recognizing a valid ID. Recent research by private advisory companies in this area has

[10] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

reported that 95% of surveyed organizations experienced an API security incident in the most recent 12 month period (Salt Security, 2022).[11] Hardware-based solutions that rely on trusted execution environments have been proposed as one security innovation that can reduce risks by avoiding the need for a TPP to access, store or process customer data in unencrypted form altogether (US Department of Commerce, 2022a).

Market Forces and Regulation

It is apparent from the preceding discussion that the UK has adopted a heavily regulation-focused approach to OB. This is reflected in its initial implementation of OD through PSD2 and the PSRs 2017, as well as the centralized approach to adopting common standards for APIs and security profiles through the OBS. While the broad terms on which OB has been adopted are closely related to the EU approach, the EU has, unlike the UK, largely delegated the task of standardization to markets. In the US, the approach to OB has been almost entirely driven by markets (US Department of Commerce, 2022a).

Nonetheless, it is important to note that, even in the UK, significant scope exists for market forces to shape the strategies that firms adopt with respect to data sharing and data protection in OB. For instance, there is no single official API that banks and financial institutions must adopt. Rather banks develop their own APIs that should comply with the specifications set out in the OBS. This leaves significant scope for banks to curtail the volume and quality of data that is actually shared within OB. This issue has been highlighted by the CMA (see CMA, 2023) against a backdrop of complaints from other market participants concerning the extent of data access (Financial Times, 2022). It also follows that many business decisions that ASPSPs make in OD markets are likely to be driven not only by mandated industry standards but also by the competitive behaviour of rival firms. This is an important motivating factor for economic, incentives-based research in this area.

2.1.2 Open Finance

The successful establishment of OB in the UK has led to proposals to extend its scope beyond payments. A Joint Regulatory Oversight Committee was set up by the CMA, FCA and the Payment Systems Regulator in March 2022 to expand the scope of OB. In February 2023 the Strategic Working Group (SWG) convened by this Committee delivered its recommendations for the future development of OB (see Open Banking Strategic Working Group Secretariat, 2023). Following consultations with OB industry stakeholders, end-user representatives and independent subject matter experts, the SWG discusses extensions of OB into adjacent financial markets in addition to improvements in ecosystem reliability, customer protection and fraud prevention, and enhancements to existing technical standards.

[11] Additional vulnerabilities are discussed in Forbes (2022).

In the payments domain, variable recurring payments are identified as one avenue for enhancing OB. These allow customers greater control over regular outgoings than they are currently afforded by Direct Debits and card-on-file instructions. Beyond this, the notion of Open Finance encompasses savings, lending, investment and pension products, building on access to a larger set of consumer data. Widening data access beyond financial data to include identity attributes is also emphasized as a potential means of driving innovation and ensuring inclusion. This raises additional concerns in relation to the sensitivity of combined data sets (see Introduction).

The UK Government has committed to creating a legislative and regulatory framework to oversee the development of Open Finance, in keeping with its earlier approach to OB. Implementation of this new regime is expected from 2023 or 2024 onwards (Deloitte, 2022).

2.1.3 Midata in Energy

Midata in energy was conceived as a means of allowing consumers to share their energy data securely with third parties. The envisioned consumer benefits centre around innovative products and services, developed by TPPs, that should facilitate tariff comparisons and consumer switching. Midata is currently paused given overlaps with Ofgem's Switching Programme and Market-wide Half-Hourly Settlement Programme.[12]

2.1.4 Open Communications

Data sharing similarly lies at the heart of the Open Communications proposals that Ofcom consulted on in 2020. This initiative envisages a framework of secure sharing of data on consumers' use of digital services in order to simplify the comparison of services and promote switching.

2.1.5 Pensions Dashboard

The Pensions Dashboard Programme (PDB) is intended to make it easier for individuals to access and control information about an their pensions savings, which may be split across a number of different schemes including the State Pension. The UK Government intention to create pensions dashboards is formalized in the Pension Schemes Act 2021 and The Pensions Dashboards Regulations 2022. Data, technical and reporting standards have been published by the PDB and remain subject to approval by the Secretary of State for Work and Pensions at the time of writing.[13]

[12] See *https://www.ofgem.gov.uk/energy-policy-and-regulation/policy-and-regulatory-programmes/midata-energy-programme*.

[13] For details, see *https://www.pensionsdashboardsprogramme.org.uk/standards/*.

2.2 The Wider Context

This part extends the discussion of the UK data governance framework beyond the standards and regulations developed in the course of OB's growth in the UK to include rules and regulations in the areas of cybersecurity (Part 2.2.1), data privacy, anonymization and interoperability (Part 2.2.2) and data ethics and responsible innovation (Part 2.2.3). We discuss governance aspects that affect firms operating in OD markets directly (e.g. the UK GDPR), as well as provisions that govern related markets in which firms face very similar economic incentives with respect to data sharing and secure hardware adoption (e.g. the NIS Regulations). These are relevant given the potential expansion of OD initiatives in markets such as energy and healthcare (see Figure 1).

2.2.1 Cybersecurity

In general terms, there is no single law governing firms' cybersecurity choices.[14] Instead, these fall under a variety of legislative instruments that either target cybersecurity in a more limited sense, or that have other objectives such as national security or sectoral regulation as their primary goal. The approach of these regulations is broadly principles-based rather than prescriptive. This is designed to give the law the flexibility to keep up with the evolving nature of technology and cyber-threats. These regulations also do not intend to make firms immune to cyber-attack but rather aim to achieve a level of cybersecurity that appropriately balances the associated costs and benefits.

Data Protection Act (2018), UK GDPR & Data Protection and Digital Information Bill

The General Data Protection Regulation (GDPR) governs the manner in which personal data is collected, shared or otherwise processed. It does so by defining a series of rights for data subjects and obligations on controllers and processors.[15] Although the GDPR has applied directly in EU member states since May 2018, its principles were also incorporated into UK law via the Data Protection Act 2018 (DPA 2018). The DPA 2018 also goes beyond the GDPR in some areas, for example concerning the processing of personal data by law enforcement and intelligence organisations, and it sets out specific UK exemptions. Following Brexit, the GDPR has become part of the body of retained EU law and is referred to as the UK GDPR. The GDPR itself is therefore now referred to as the EU GDPR in the UK. The UK GDPR and DPA 2018 represent the principal overarching pieces of data protection legislation in the UK.

[14] This part draws on practice notes maintained by Practical Law and Lexis PSL. An extended discussion of the cybersecurity regulatory context is contained in Lam and Seifert (2021).

[15] A *controller* decides on the manner in which data is processed. A *processor* is a separate legal entity from a controller that acts entirely under instruction from the controller with respect to data processing activities. In the OB context, both ASPSPs and TPPs are data controllers.

The obligations of controllers are summarized in six data protection principles contained in the UK GDPR. Controllers are responsible for ensuring compliance with each of them (the accountability principle). Of these data protection principles, the sixth relates directly to cybersecurity. It states that data should be

> "processed in a manner that ensures *appropriate security of the personal data*, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
>
> Article 5(1)(f), UK GDPR, emphasis added

The balancing of risks against rewards in determining the appropriate level of cybersecurity is made explicit in Article 32:

> "Taking into account the state of the art, *the costs of implementation* and the nature, scope, context and purposes of processing as well as *the risk of varying likelihood and severity* for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure *a level of security appropriate to the risk*."
>
> Article 32(1), UK GDPR, emphasis added

As this Article also states, the measures businesses are required to take in order to comply with the security principle include those of a technical nature (both hardware and software-based) and an organisational nature (e.g. training, policies and procedures).

Other provisions of the UK GDPR can be seen as imposing additional cybersecurity requirements on firms. In particular:

1. data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" (Article 5(1)(e), UK GDPR),[16]

2. the processing of personal data undertaken by controllers should build on the data protection by design and default principle (Article 25(1), UK GDPR), and

3. only data that is necessary for the purpose at hand should be processed (Article 25(2), UK GDPR).

[16] Another security-related context that builds on this principle is the Payment Card Industry Data Security Standard (PCI DSS), applicable to merchants and payment processors, which prohibits storing payment card verification codes once a transaction has been authorized (Rule 3.2.2, PCI DSS v3).

The latter of these points relates to the data minimization and purpose limitation principles of the UK GDPR. These are particularly relevant in light of the discussion of screen scraping and the use of dedicated interfaces (APIs) for TPPs to access data in the OB framework. It is worth noting that many of the measures that have been proposed to reduce security risks in OB revolve around further reducing the extent to which data is processed or shared between ASPSPs and TPPs in unencrypted form (see US Department of Commerce, 2022a).

These security principles are enforced by the Information Commissioner's Office (ICO). Any incident leading to a breach of personal data must be notified to the ICO within 72 hours of the controller becoming aware of it, where feasible (Article 32(1), UK GDPR). Similarly, processors must inform their controller without undue delay following a cyber-breach (Article 33(2), UK GDPR). Enforcement powers held by the ICO include information notices (requests for information), assessment notices (inspections to determine compliance with legislation), enforcement notices (requiring a controller or processor to take a particular action) and penalty notices. In the case of the latter, failure to ensure appropriate security measures can result in fines of up to the greater of £17.5 million or 4% of annual global turnover (Article 83(5), UK GDPR). The ICO may take enforcement action, even without a data breach having occurred. In practice, reputational costs and private actions for damages are likely to represent further incentives to ensure appropriate levels of cybersecurity.

In July 2022 the Data Protection and Digital Information Bill (the DPDI) was introduced to Parliament following the Government's 'Data: a new direction' consultation. The DPDI complements the data protection provisions contained in the UK GDPR and the DPA 2018, among others. It is not seen as a radical departure from the prevailing approach that closely mirrors that of the EU, with much focus instead being given to the simplification of existing rules. The areas touched on by the DPDI include international data transfers (reducing the 'adequacy test' for third countries to a lower standard in the form of a 'data protection test'), legitimate interests and automated decision making, among others. Finally, the DPDI is also seen as containing provisions favourable to the continued expansion of OD (Smart Data) schemes in the UK by facilitating data sharing between businesses (OneTrust, 2022).

Cybersecurity in the Financial Services Sector

The financial services sector is subject to cybersecurity regulations in addition to those stemming directly from the OBS, UK GDPR and DPA 2018. In particular, providers of financial services including banks, insurance companies and financial advisers are subject to sector-specific cybersecurity regulations that are enforced by the FCA. These cyber-regulations stem from two sources: the Principles for Business and the Senior Management Arrangements, Systems and Controls (SYSC), both of which are contained in the FCA Handbook.

The SYSC are responsibility standards for company directors and senior management in financial firms. They contain rules that were previously part of the Capital Markets Directive

(2006/49/EC) and the Markets in Financial Instruments Directive (2004/39/EC). Some of these rules directly or indirectly impose cybersecurity requirements on financial firms, in particular insofar as they relate to securing systems, managing risks, reducing the risk of financial crime and ensuring customer confidentiality. For instance, SYSC 3.2.21 states that "a firm should have appropriate systems and controls in place to fulfil the firm's regulatory and statutory obligations with respect to adequacy, access, periods of retention and security of records." These requirements also relate explicitly to the security of data that is transmitted: "a common platform firm[17] must have sound security mechanisms in place [...] to guarantee the security and authentication of the means of transfer of information" (SYSC 4.1.1). Other relevant SYSC rules include SYSC 6.1 (Compliance), SYSC 7 (Risk control) and SYSC 8 (Outsourcing).

Similarly, the third Principle for Business (PRIN 2.1.1, FCA Handbook) requires a firm to "take reasonable care to organize and control its affairs responsibly and effectively, with adequate risk management systems." Under Principle 11, regulated firms have a duty to report cyber-attacks to the FCA. A similar requirement also exists under Rule 7 of the Prudential Regulation Authority Rulebook.[18]

Network and Information Systems Regulations 2018

The Network and Information Systems Regulations 2018 (SI 2018/506) (NIS Regulations) are the UK enactment of the Network and Information Security Directive ((EU) 2016/1148) (Cybersecurity Directive).[19] These regulations impose a number of cybersecurity-related obligations on two classes of firms:

1. Operators of essential services (OESs): firms that operate in important sectors such as energy, transport, health and digital, and which rely on network and information systems to perform their economic role.

2. Relevant digital service providers (RDSPs): firms that provide certain types of digital services in the UK, including online marketplaces, search engines and cloud computing services.

In contrast to the Cybersecurity Directive, banking and financial market infrastructures are not covered by the NIS Regulations. These areas are instead monitored by the FCA, see above.

In each case, threshold requirements in terms of firm size must be met in order for an OES or RDSP to fall within the scope of the NIS Regulations. For OESs, and depending on the sector in which they operate, these requirements are set out in Schedule 2 to the NIS

[17] This term describes firms, such as banks, building societies and designated investment firms, which were simultaneously subject to the Capital Markets Directive and the Markets in Financial Instruments Directive.

[18] Cybersecurity concerns have also been raised in connection with consultations on the Operational Resilience rules, see *https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2021/march/ps621.pdf*.

[19] This EU legislation has since been updated in the form of the NIS 2 Directive that came into force in 2023.

Regulations. For RDSPs, small and micro businesses are generally exempted. OESs and RDSPs are required to self-identify to their designated competent authority. The designated competent authority varies for OESs according to the sector of their operations as reflected in Schedule 1 to the NIS Regulations. All RDSPs are subject to the oversight of the ICO.

Unlike the GDPR and DPA 2018, the focus of the NIS Regulations is not the security of the data being processed, but rather the security of the IT infrastructure on which the essential services provided by OESs and RDSPs rely. These provisions can therefore be seen as particularly relevant for hardware security. OESs and RDSPs satisfying the threshold requirements fall under the NIS Regulations precisely because outages of the networks and systems they control could lead to substantial damage to consumers and the wider economy.

The main security obligations of OESs under the NIS Regulations are to:

> (1) "take *appropriate and proportionate technical and organisational measures to manage risks* posed to the security of the network and information systems on which their essential service relies.
>
> (2) take *appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems* used for the provision of an essential service, with a view to ensuring the continuity of those services."
>
> Regulation 10, NIS Regulations, emphasis added

The measures adopted under (1) must "ensure a level of security of network and information systems appropriate to the risk posed" (Regulation 10(3)). An important difference to the UK GDPR lies in the fact that OESs (and RDSPs) may not take the cost of implementing cybersecurity measures into account when deciding on their appropriateness. Rather appropriateness in the context of the NIS Regulations is based on the "state of the art", that is the measures currently available to them.

With regard to RDSPs, the security requirements are somewhat lighter than for OESs. Services provided by RDSPs are typically less critical to the continued normal operation of the wider economy. An "RDSP must identify and take appropriate and proportionate measures to manage the risks posed to the security of network and information systems on which it relies to provide" (Regulation 12(1)). These measures must "(having regard to the state of the art) ensure a level of security of network and information systems appropriate to the risk posed" (Regulation 12(2)).

The reporting obligations under the NIS Regulations are similar to those under the UK GDPR. An OES or RDSP must notify its designated competent authority without delay and no later than 72 hours after becoming aware of a security breach that has a significant impact on the continuity of the service which the OES or RDSP provides (Regulations 11, 12). It is

important to note, in contrast to the UK GDPR, the absence of the phrase “where feasible” in this notification provision.

Enforcement of the NIS Regulations with respect to OESs falls to distinct and sector-specific designated competent authorities, such as Ofcom in the case of digital infrastructure. The ICO is the competent authority for all RDSPs. Fines under the NIS Regulations are not linked to global annual turnover, but instead follow tiered, static, upper limits depending on the infringement up to a maximum of £17 million. The possibility of double jeopardy, whereby an organization is fined under both the UK GDPR and the NIS Regulations for the same event, is not ruled out. Other enforcement powers of designated competent authorities include information notices, inspections and enforcement notices.

Communications Act 2003

Section 105 of the Communications Act 2013 (CA 2013) concerns the security of public electronic communications networks and services. These terms describe, respectively, “an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public” and “any electronic communications service that is provided so as to be available for use by members of the public” (Section 151). Providers of public electronic communications networks and services “must take technical and organisational measures appropriately to manage risks to the security of public electronic communications networks and public electronic communications services” (Section 105A). They must also inform Ofcom of any security breaches having a significant impact on the operation and availability of those networks and services (Section 105A).

Privacy and Electronic Communications Regulations 2003

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)[20] implement the European e-Privacy Directive (2002/58/EC) into UK law. The PECR imposes obligations on providers of public electronic communications services that mirror those under Article 4 of the e-Privacy Directive. In particular, providers must “take appropriate technical and organisational measures to safeguard the security of that service” (Regulation 5(1)). The appropriateness criterion is satisfied in this context “if, having regard to (a) the state of technological developments, and (b) the cost of implementing it, [a measure] is proportionate to the risks against which it would safeguard” (Regulation 5(4)).

Enforcement of the PECR lies in the hands of the ICO. Security breaches must be notified “without undue delay” (Regulation 5A(1)), although this notification requirement disappears if

[20] As amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (SI 2011/1208).

data has been adequately encrypted (Regulation 5A(6)(a)). Enforcement powers of the ICO include audits and enforcement notices, as well as fines of up to £500,000.

Computer Misuse Act 1990

The Computer Misuse Act 1990 differs from the above legislation in that it defines a number of cyber-crimes that hackers may commit, rather than imposing security obligations on data processing firms or operators of critical networks and services. Crimes covered by the Computer Misuse Act 1990 include unauthorized access or interference with a computer, distributed denial of service attacks and the creation of hacking tools. The Computer Misuse Act 1990 has subsequently been amended by the Serious Crime Act 2015, which created the new offence of impairing a computer such as to cause serious damage.

European Regulation with Extraterritorial Effect in the UK

Post-Brexit, the EU GDPR will continue to affect UK businesses that are controllers or processors and that have an establishment in the EU, that offer goods or services to EU data subjects, or that monitor the behaviour of EU data subjects (Article 3, EU GDPR). UK firms may also be subject to member state enforcement of the Cybersecurity Directive (EU) 2016/1148. This may involve UK digital service providers having to comply with additional registration, security and notification requirements in those EU markets in which they operate.

2.2.2 Data Privacy, Anonymization & Interoperability

Data privacy describes the manner in which personal data is collected, stored and, importantly, *shared with third parties* (The Royal Society, 2020). In broad terms, the UK Common Law Duty of Confidentiality holds that legal authority or justification is required before personal information that was submitted in confidence can be further disclosed. This often translates into a requirement for consent, although the UK GDPR sets out a number of other legal bases for data sharing (data processing), including when such sharing is necessary under previously agreed contractual terms or when it is in a person's vital interests (Article 6, UK GDPR).

Beyond this, the principles and individual rights contained in the UK GDPR and DPA 2018 apply directly to firms' data sharing activities. Data sharing must, for example, respect individuals' right to be informed, their right to restrict processing and their right to object to data transfers between firms. The right to data portability grants data subjects a positive as opposed to a limiting right in relation to data sharing insofar as it assures them of the option to transfer their data from one provider to another, if desired.

In terms of data transfers involving public bodies, the Investigative Powers Act 2016 restricts the extent to which law enforcement and the security and intelligence agencies can obtain

communications data. Finally, among other provisions, the Digital Economy Act 2017 sets out the rules under which the Office for National Statistics accesses data held by public authorities in the course of producing national statistics such as the census.

Data anonymization can be seen as means of preserving privacy, even in situations where data is shared between firms. In particular, provided the data subject is no longer identifiable in the anonymized data set, that data is no longer the subject of data protection laws and fewer legal restrictions apply to its sharing or other processing. The DPA 2018, for instance, applies to personal data on 'an identified or identifiable living individual' (Article 3(2), DPA 2018). The anonymization code of practice contains guidance for firms in terms of their treatment of anonymized data and the effectiveness of data anonymization methods (ICO, 2012). A similar code also exists in the sphere of data sharing in order to allow firms more easily to comply with the data protection legislation discussed above in the course of their data sharing activities (ICO, 2021).

The closely related concept of interoperability refers to a process of standardization that allows data gathered and processed in one context to be compatible with processing activities in a range of other contexts. This has received particular attention in the UK in the context of government-held data. The Data Standards Authority, for example, has been leading cross-government work on data standards to facilitate interoperability in the context of the UK's broader National Data Strategy (see Central Digital & Data Office, 2021, 2022).

It is clear that, within the OD context, the consumer benefits derived from more widespread sharing of consumer data with TPPs come at the cost of reduced consumer privacy. Several aspects of the OB context address this trade-off explicitly. The FAPI specification underlying the security profiles contained in the OBS encourages users to comply with the ISO/IEC 29100 privacy framework, for example.[21] Moreover, the notion that more widespread data sharing can drive consumer benefits extends beyond markets that are subject to OD initiatives. For instance, in the context of promoting competition in digital markets, interoperability and data sharing are seen as key tools that the Digital Markets Unit should use to achieve its goals (HM Government, 2022a).

Of course, data privacy is also closely linked to security in the sense that we may reasonably suppose that, the more widely data is shared, the greater the likelihood that it becomes subject to a cyber-attack. Implementing appropriate policies in the area of data privacy requires the trade-offs between the costs and benefits of data sharing to be analysed carefully. These trade-offs are the subject of our theoretical analysis in Part 4 that considers secure hardware adoption incentives in OD markets.

[21] See *https://openid.net/specs/openid-financial-api-part-2-1_0.html*.

2.2.3 Data Ethics & Responsible Innovation

Data ethics concerns the potential harms stemming directly or indirectly from the collection, storage and processing of personal data. In many cases these potential harms are already subject to the framework of regulations described above, for example in the context of the broad range of processing activities captured under the UK GDPR. Beyond compliance with relevant regulations, a series of guidelines aim to guide both private entities (Open Data Institute, 2021) and public entities (HM Government, 2020b) towards an ethically sound approach to the processing of personal data.

One particular area that has been subject to both rapid technological innovation and ethics concerns is artificial intelligence (AI). AI has the potential to disrupt established markets but at the same time is largely controlled by established firms that command a significant share of relevant digital markets (Foreign Policy, 2021). AI is seen as a driver of future competitiveness (HM Government, 2022b) but also raises concerns in relation to discrimination, not least in financial markets (EU Agency for Fundamental Rights, 2022). The initiatives taken by UK regulators to support a responsible use of AI include the ICO's guidance in the areas of AI and data protection, explaining decisions made with AI, its AI and Data Protection Risk Toolkit and its AI Auditing Framework and AI blog resources (ICO, 2022a,b,c). Similarly, the Equality and Human Rights Commission Strategic Plan 2022-2025 identifies AI as a strategic priority (Equality and Human Rights Commission, 2022), while the Medicines and Healthcare products Regulatory Agency has consulted on potential changes to regulation to ensure the safety of medical devices in addition to launching the Software and AI as a Medical Device Change Programme (HM Government, 2022c,d).

Part 3

Primary Data Analysis

We begin our analysis of the factors driving secure hardware adoption by analysing primary data that was collected during interviews with industry participants. Our data collection exercise is summarized in Part 3.1. Parts 3.2 and 3.3 describe the results of a quantitative and qualitative investigation of this data, respectively, before Part 3.4 highlights important open questions that emerge from this analysis. These open questions are subsequently addressed using the theoretical model that we present in Part 4.

3.1 Primary Data Collection

A total of seven interviews were conducted with interviewees representing a range of professional backgrounds. The profile of our interview participants is summarized in Table 1 below.

Interviewee Area of Work	Number
Local Government & Regulatory	2
Energy	1
Finance & FinTech	2
Technology	2
Total Interviews	*7*

Table 1: Interview data collection

Our interview participants cover important sectors from the viewpoint of OD initiatives, principally the financial and energy markets. We also benefited from the insights of specialized technology firms and a national regulator. Finally, the insights of our local government interviewee are highly relevant in this context given the importance of data collection and data sharing for the provision of public services at the local authority level.

In addition to carrying out these interviews, we have benefited from interactions with our

industry partner LNDSR in the course of virtual site visits on 20 May 2022, 9 February 2023 and 14 April 2023.

3.2 Quantitative Data Analysis

Several interview questions invited respondents to provide numerical responses on a 5-point scale concerning the adoption of secure hardware, the importance of OD initiatives, and the characteristics of the UK data governance framework. These questions and the average response values are indicated below.[22]

Question	**Av. Score**
Secure Hardware Adoption	
On a scale of 1-5 (1=not at all, 5=extremely), how important is security when it comes to firms' decisions to adopt new hardware?	4.3
On a scale of 1-5 (1=not at all, 5=extremely), how concerned are firms that the hardware they adopt is 'digitally secure by design'?	2.8
On a scale of 1-5 (1=totally insufficient, 5=totally sufficient), how do you judge the pace at which secure hardware is currently being adopted?	2.5
OD Initiatives	
On a scale of 1-5 (1=not at all, 5=extremely), how important are OD initiatives in your area of work?	4.1
On a scale of 1-5 (1=not at all, 5=extremely), how significant are potential concerns about security in the context of OD schemes?	4.3
The UK Data Governance Framework	
On a scale of 1-5 (1=not at all, 5=completely), how well do you think the existing UK data governance framework succeeds in balancing the benefits and risks associated with secure hardware adoption?	3.5

We see that interview participants attribute an important role to security in hardware adoption decisions. Nonetheless, respondents also believe that firms attach only moderate importance to hardware being digitally secure by design, perhaps due to limited understanding, awareness and access to the technology. In addition, the pace at which secure hardware is being adopted is viewed as being marginally insufficient. This suggests market failures might exist with respect to secure hardware adoption, an issue to which we will return in Part 4.

These responses also indicate that OD initiatives are perceived as important within our

[22] In the case of our local government interviewee, these questions relate to local authorities rather than firms.

interviewees' areas of work. This reinforces the idea that data sharing incentives matter in the markets that we focus on. Security concerns are viewed as important in OD markets, which connects with our discussion of the data governance framework in Part 2. Finally, there is a moderately positive view, on average, of the role that the existing data governance framework plays in balancing risks and rewards in the area of secure hardware adoption.

These results emphasize the importance of the research questions that we are pursuing insofar as they indicate the importance of security as part of firms' hardware adoption decisions in general and within the OD context specifically. They also provide an initial and high level indicator of perceptions regarding the UK data governance framework. Understanding the reasons behind these numerical responses requires us to look in more detail at the qualitative responses provided by our interviewees, which we do as part of the qualitative data analysis that follows.

The average responses presented above were calculated on the basis of the seven interviews that we conducted in the course of our project, see Table 1. Our interview strategy in this project has focused on gaining in-depth insights from subject matter experts with specific professional backgrounds rather than achieving statistical significance on the basis of a large and random sample. The questions set out above indicate the scale to be used in individual responses, which resulted in average scores that fall between the extremes of 'not at all' / 'totally insufficient' and 'extremely' / 'completely'. On this continuous 1-5 scale, a score of 3 can be interpreted as a neutral response ('somewhat' / 'moderately'), with answers either side of this central value indicating a tendency, on average, towards a more positive or negative view. Finally, besides the restricted sample size, the generalizability of our quantitative results is limited by the specific time period in which these interviews were conducted (2022-23) as well as their geographic focus (all but one of our interviewees were UK-based).

3.3 Qualitative Data Analysis

We structure our qualitative analysis into the following categories: (i) factors that influence secure hardware adoption decisions, (ii) specific issues in relation to hardware adoption and data sharing that arise in OD markets, (iii) the impact of competition and (iv) the UK data governance framework.[23]

Secure Hardware Adoption

Factors that promote secure hardware adoption

A_1 **Security concerns** can drive firms' decisions to adopt new hardware. CHERI can bring concrete benefits in this context. For example, it may allow new software to be put into

[23] Details of the methodology underlying our qualitative data analysis are provided in the Appendix.

operation sooner by protecting against memory-access vulnerabilities. This matters in the blockchain context, for example, which has frequent iterations of the software renewal cycle. CHERI can be an important contributor to the required upgrade of our IT infrastructure from the ground up.

A_2 The **sensitivity of the data** that is being protected affects the benefits of increased hardware security in the form of reduced liability for cyber-attacks and therefore the incentive to adopt new technologies. In the energy context, an important distinction can be drawn between network systems data and much more sensitive personal data related to energy supply.

A_3 Since firms' decisions are driven by profit considerations, *several* respondents highlighted that expected liability for future cyber-attacks can drive secure hardware adoption. Some level of risk may be seen as business tolerable, however, and some sectors (e.g. video consoles) may provide lower incentives. **Liability rules** that hold providers of financial services liable for cyber-breaches rather than the suppliers of technology can incentivize secure hardware adoption in the financial sector, for example.

A_4 Market regulations such as the NIS Regulations (see Part 2.2.1) and licensing conditions for energy network operators can push regulated firms to adopt secure hardware in order to meet **minimum requirements**. In these cases, the regulator typically faces a similar balancing exercise with respect to the benefits of requiring additional security and the associated costs as do competing firms in a market setting.

A_5 Some regulated companies may be **risk averse**, which can lead to **over-compliance** when firms implement levels of security above the minimum level.

A_6 Using regulation as a means of promoting hardware adoption is easier in markets in which firms are subject to **existing regulations**, even if those regulations are not specifically targeted at cybersecurity. Thus ensuring digital security is easier among banks, which are already extensively regulated, than among Big Tech platform firms that also offer many retail banking services, for example.

A_7 TPPs in OD markets are more digitally-enabled and **technologically nimble** than established firms. Reputational effects associated with this digital business model mean such firms are more likely to adopt secure hardware to support their digital operations.

A_8 The concern for **privacy** in the context of Web3 and blockchain can also promote secure hardware adoption.

Factors that hinder secure hardware adoption

A_9 *All* respondents discussed **cost** and limited resources as a factor hindering secure hardware adoption. Among these costs, people's time and staff retraining are important factors, perhaps even more so than the direct costs of acquiring new hardware and ensuring system compatibility. *Several* interviewees highlighted interoperability as another important cost.

A_{10} *Several* respondents highlighted the importance of **culture** for secure hardware adoption. Where awareness of the importance of hardware security is lacking, regulations that try to enforce a minimum standard are likely to be less effective. Relatedly, it was observed that a concern for security may be found within the Chief Information Officer, Chief Security Officer and Chief Information Security Officer roles but less so on the business side.

A_{11} *Several* respondents highlighted that businesses are driven by **commercial considerations** and not the security of new technologies per se. New technologies that provide similar outcomes to those achieved by existing, albeit less sophisticated workarounds will be perceived as non-essential from a business perspective. It can be costly to replace such workarounds, which adds to the acquisition cost of new hardware.

A_{12} Since hardware security is driven by commercial considerations, security needs to tie in with **usability and affordability aspects** rather than being promoted as a stand-alone feature, which would increase concerns about adoption costs. Security does not play an important role in and of itself unless the hardware is being acquired for a dedicated security purpose. Firms are unlikely to accept reduced performance in exchange for improved security. Business considerations again dominate security per se.

A_{13} Regulations can hinder as well as promote secure hardware adoption. In markets subject to **price regulation**, for example, hardware adoption decisions are coordinated with periodic price reviews. Information that is acquired by experimenting with new technologies in between price reviews can be lost, leading to lower adoption. Once firms meet minimum regulatory requirements, there are limited incentives to improve security further (there are no advantages to being super-compliant).

A_{14} In markets with price regulation, it can also be difficult to split the costs of adoption into a **trial period** that precedes full adoption. Greater certainty is needed with respect to adoption here because the additional spend needs to be justified in detail in the context of the periodic price review.

A_{15} **Planning horizons** can be long, particularly in price-regulated markets. If existing technologies have been put in place to meet security requirements for the next 10 years, say,

firms will be reluctant to acquire new hardware to replace those approved technologies before the end of the 10 year period.

The impact of firm size and sector

A_{16} The importance that is attached to security by start-up firms can vary markedly and depends in large part on whether **security personnel** are part of the initial team. *Most* respondents emphasized that start-ups tend to be more focused on revenue generation, however, and that hardware security considerations become a priority only once market survival has been assured. Start-ups do not differentiate themselves in the market by claiming to perform existing functions more securely.

A_{17} On the other hand, large incumbents face greater **complexity** when adopting new hardware given the challenge of ensuring interoperability with legacy systems. This factor favours adoption by smaller, younger firms. There is a trade-off between the availability of resources, which favours adoption by large firms, and being digitally nimble, which favours smaller firms.

A_{18} Several of the features highlighted above, in particular the periodic nature of price reviews, apply particularly at the network level of the energy market. Other sectors, such as hydrogen production and oil and gas extraction, are subject to licences that cannot be changed after issuance. In these cases, obliging firms to follow **guidelines or industry best practice** for data sharing can be a means of maintaining security.

A_{19} Security was highlighted as particularly important in the context of Big Tech firms that provide **systemically important infrastructure**, in healthcare and the power generation sector. *Several* interviewees highlighted the importance of security in the banking sector given the sensitive nature of the data involved and the systemic importance of large banks. The telecommunications sector was highlighted as an example of particularly high levels of security. Retail and video consoles were highlighted as examples of sectors in which security plays a lesser role.

A_{20} **Local authorities** are likely to wait until a new architecture or other new technology becomes mainstream. Interoperability with legacy systems raises particular challenges in this context. Similarly, public sector bodies are also more likely to select a standard offering rather than pursuing bespoke requirements from hardware vendors. Local authorities are likely to look for an acceptable level of security and are unlikely to exceed minimum requirements as set out by the National Cyber Security Centre (NCSC), for example.

Consequences of security vulnerabilities

A_{21} *Several* respondents commented on the importance of **spillovers** or externalities: in some cases, vulnerabilities in one sector can lead to damages in related areas of the economy. Energy is one example of this. Vulnerabilities in low-voltage substations can translate into harm across hospitals, schools, homes, businesses, industry, etc. *Several* participants highlighted banks as another example. Vulnerabilities at one bank can inhibit the functioning of affiliated banks, decrease confidence in the banking sector as a whole and lead to negative effects in the real economy.

A_{22} The damages of cyber-attacks extend beyond monetary losses associated with lost data, secrets and credentials to **risks to life** in the aeronautics and safety-critical sectors. Much of this revolves around the nature of the data that is compromised.

A_{23} Damages arise not only from loss or manipulation of data, but also from manipulation of **algorithms** that are fed by this data. This can generate significant harm in the context of medical advice, for example. These concerns remain, even in settings where algorithms are fed by publicly available data.

A_{24} **Connected devices** (energy smart appliances) that are going online represent a particular threat, though these are mitigated through PAS Standards 1878 and 1879 and the NIS Regulations.

A_{25} Despite the security standards discussed in the OB context above (see Part 2.1.1), vulnerabilities do remain a concern in the context of bank APIs, for example imitation attacks.

A_{26} It was highlighted that several security vulnerabilities have arisen in the past that were inherent to hardware.

A_{27} In the local authority context, data losses can expose particularly vulnerable members of society to harm.

The OD Context

Specific features of OD markets

O_1 The OBS allows banks flexibility with respect to the design of their APIs. The costs of designing APIs means that large incumbent banks lead in this area. This means there can be spillover effects from large banks designing good APIs. These banks are, however, incentivized to develop poorly functioning APIs that **limit data access** (see Market Forces and Regulation above for further discussion of this point).

O_2 The nature of security risks arising in OD markets depends on the nature of the data that is being shared. Sharing of energy systems data raises fewer concerns than sharing personal data, for example. This explains the caution around the Midata in energy scheme.

O_3 The importance of security in OD markets will grow in line with the number of people using these services. This relates back to the point about liability above (see A_3).

O_4 Data sharing is fundamental in many contexts outside OD markets. For instance, data sharing facilitates the provision of coordinated local services such as health and social care. This data sharing is done on the basis of formal data sharing agreements and technical controls that would involve encryption as a minimum when data is being transferred.

Benefits of data sharing

O_5 OD can lead to different types of consumer benefits. In developing markets, OB can be a means of **increasing access** to basic financial services. In more developed economies, OB can increase consumer choice and thereby weaken the market power of incumbents.

O_6 Data sharing in energy markets, including commercial and systems data, can generate significant benefits (e.g. using data from smart meters to detect gas leaks). As such, the focus in these markets is on justifying decisions not to share data, as opposed to explaining why data can be shared. As noted above, sharing of personal energy usage data remains a more challenging proposition given the risks involved (A_2). There is a related question of what actually constitutes personal data in energy markets. Smart meter Meter Point Administration Numbers (MPANs) and Meter Point Reference Numbers (MPRNs) are treated as personal data, for example, which increases security but can constrain operations.

O_7 One benefit of data sharing is the propagation of **best practice** in energy and banking markets. Thus firms that begin to interact with incumbent banks will typically be required to meet the same level of security as those incumbent banks.[24]

The Impact of Competition

C_1 Competition can drive firms to cut costs, which may lead to **reduced adoption** of secure hardware where this is deemed non-essential. This can impose externalities on other market participants when the failure of one firm leads to a loss of consumer trust in the

[24] The UK GDPR and DPA 2018 require data controllers to put in place minimum contractual obligations on processors, see *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/accountability-and-governance/contracts/*.

security of the remaining firms. These externalities would in principle be internalized by a monopolist who bears full responsibility for the consequences of their business decisions.

C_2 In order for some OD markets to function correctly, some **data monopolies** will be needed. This will involve concentrating information and control over information in centralized registers so that they can be accessed by other market participants. These data monopolies require coordination and coordinated security.

C_3 *Several* respondents highlighted that competition can also exert positive effects on secure hardware adoption when super-compliance confers a **competitive advantage** on firms. This depends on the extent to which security advantages can be effectively marketed.

C_4 In the context of centralized regulations that mandate a particular technology, it was highlighted that this can have negative effects in terms of eliminating competition and conferring **pricing power** onto approved vendors.

The UK Data Governance Framework

G_1 *Several* interviewees stated that **culture** matters. This culture reflects an awareness of the importance of security and compliance with relevant regulations.

G_2 *Most* respondents highlighted the advantages of **combining bottom-up and top-down approaches** to regulation. Thus in the energy markets, it was deemed preferable to dispense funds to network firms via price controls, but to grant them flexibility as to how to use those funds and to give them opportunities to communicate any failures resulting from their chosen strategy (*most* respondents favoured this technology-neutral approach). Similarly, *most* respondents said that guidelines should be principles-based and not mandate specific technologies.

G_3 One disadvantage of a top-down regulatory approach was the complexity of **enforcing** the rules and auditing this enforcement process. Similarly, a centralized, one-size-fits-all approach can impose excessive costs and is unlikely to cover 100% of cases.

G_4 A **minimum security standard** that is enforced by regulation was seen as necessary by one respondent for large financial firms and, in the banking context, the regulator should set the standards in terms of API security. Where standards are in place, these can be raised over time.

G_5 **Guidance** plays an important role, for example in relation to the way in which data can be opened up in energy markets while taking commercial sensitivity and national security considerations into account. In the financial context, the FCA Consumer Duty was noted as another example of how positive outcomes for consumers can be promoted.

G_6 As we move from OB to Open Finance, it will be important to understand the **interactions between OB and the GDPR**. It will also be important to ensure a level playing field for Big Tech and banks. In general, it can be difficult to define the privacy and security responsibilities of the different regulators that are active in this space, including the banking authority, competition authority and the consumer protection authority.

G_7 Where regulations are in place, it was highlighted that these should apply equally to large and small firms. It was also stated that a **dedicated cybersecurity regulator** may be appropriate given the broad range of responsibilities covered by existing regulators.

G_8 One advantage of the existing data governance framework is that is provides a clear set of guidelines to follow. One disadvantage is its excessive complexity.

3.4 Open Questions

Our primary data analysis shows that security plays an important role in hardware adoption decisions. Nonetheless, security is only one of several factors that incentivize firms to adopt new hardware. Business considerations dominate in firms' decisions as to whether or not to adopt new, more secure hardware. This means that adopting hardware in order to lower the risk of cyber-attacks is more likely when the data that is being protected is more sensitive, when firms' liability in the event of a breach is higher, and when risk-aversion pushes firms to implement security above the minimum requirements of existing regulations. Hardware adoption incentives are reduced to the extent that the associated costs are viewed as prohibitive from a business perspective and to the extent that the prevailing security culture leads to the benefits of secure hardware adoption being underestimated.

In terms of OD markets specifically, the relevance of hardware adoption decisions in this context was underlined by the security risks participants identified in terms of sharing sensitive data. While these security risks represent a cost of data sharing, there are also substantial benefits. In addition to the benefits highlighted in the overview of OD schemes in Part 2.2.1, data sharing between firms can also be a means for security best practice to spread throughout an industry, for example.

Finally, we received interesting insights concerning the design of the UK data governance framework. One important conclusion that emerges from this analysis is that participants generally favour a balance between top-down and bottom-up approaches. This is in contrast to the results of a separate primary data analysis conducted in the context of cybersecurity investments (see Lam and Seifert, 2021), where interview participants generally favoured a centralized approach to regulation. One possible reason why a more decentralized approach is viewed favourably in the context of hardware adoption as opposed to shorter-run security investments is the difficulty of measuring the true costs of adopting secure hardware, especially

when hardware adoption is a long-run decision (for example, the planning horizon can extend up to 10 years in some contexts, as noted by our interviewees). This cost assessment is complicated by the fact that, in the hardware adoption context, adoption costs have to consider relevant opportunity costs of *not* adopting (rewriting unsafe code, reputational costs, legal costs, fines, etc.) which may be highly specific to individual firms and difficult for a regulator to verify when assessing whether hardware adoption has reached a level commensurate with cyber-risks (Microsoft, 2020). By contrast, short-run business investments in security services may be easier to measure and more comparable across firms and are therefore better suited to a more centralized approach.

Several important open questions remain after this primary data analysis:

1. *Hardware Adoption Incentives & Data Sharing.* Our interviewees have highlighted the fact that data sharing in OD markets creates new cybersecurity risks, and that the incentives to adopt secure hardware depend on the benefits this brings in terms of reducing firms' liability for data breaches. This suggests that firms' decisions to share data in the OD context and to adopt secure hardware are likely to be interrelated. The precise form and significance of these interactions remain to be made precise, however.

2. *Market Failures.* Our respondents have highlighted that firms are not adopting secure hardware quickly enough (the market displays under-adoption). This highlights the potential for firms' privately-optimal hardware adoption decisions to fall short of the levels that society as a whole would prefer. It remains to determine in which circumstances such market failures arise. Given the interactions between secure hardware adoption and data sharing, it is important to consider potential market failures in these areas jointly.

3. *Data Governance & Regulation.* To the extent that market failures do arise, our respondents have highlighted a number of data governance features that can mitigate these failures (guidance, minimum standards, improving the security culture, etc.). The effectiveness of these alternative measures in bringing firms' privately-optimal data sharing and hardware adoption decisions into line with the social optimum has not been formally analysed yet.

4. *Competition.* Finally, competition was highlighted as exerting important effects. Participants believed that a monopolist's incentives to adopt secure hardware may exceed or fall short of those generated in a market with competing firms. So far the impact of market structure on data sharing, hardware adoption and social welfare remains unexplored from an analytical perspective, however.

We now proceed to address these open questions in the context of a theoretical model.

Part 4

Theoretical Results & Evidence

In this part we describe the structure and main results of the game-theoretic model developed in Lam and Seifert (2023a). This model addresses the question of secure hardware adoption incentives in OD markets in which firms also make decisions with respect to data sharing. An overview of the model assumptions is given in Part 4.1, before Part 4.2 discusses how the results of this model address the open questions emerging from our primary data analysis. We draw further implications for the UK data governance framework by connection this theory with practice in Part 4.3.

4.1 Model Overview

In general terms, a game-theoretic model consists of three elements:

1. *players*: those entities that are confronted with some type of decision,
2. for each player, their available *strategies*: these define the various courses of action that each player may take, and
3. for each player, their *payoffs:* these translate any given collection of strategy choices, one for each player in the game, into monetary or other rewards.

A game-theoretic model is solved by considering which strategy each player will choose in order to maximize their payoff for given strategy choices by the other players. Loosely speaking, an equilibrium of the game describes a collection of strategy choices, one for each player in the game, such that no player can increase their payoff by changing the strategy choice they have made, holding fixed what every other player in the game is doing. One advantage of a theoretical model of this type is the flexibility it affords us in terms of studying the impact that various data governance interventions are likely to have on the equilibrium and welfare outcomes of the game.

In our model the players are two firms, firm 1 and firm 2. Each firm offers a digital product or service for sale to a market of consumers. Importantly, firms collect a volume of personal

data from each consumer who buys their product or service. This data may represent personal information that consumers submit when signing up for the product or service, as well as data that is collected passively through cookies and location tracking, for example. The firms' products are 'horizontally differentiated' from each other, which means that consumers do not share a common view as to which of the two products is preferred to the other when the products are sold at identical prices. Instead, consumers display differing tastes for the attributes reflected in each product.[25]

The economic questions we are interested in relate to firms' incentives to adopt secure hardware in OD markets, that is in markets where data sharing decisions matter. To that end, we allow firms' *strategies* to capture, firstly, their decision as to whether or not to adopt a secure piece of hardware. Secondly, firms decide whether or not to share the data they collect from consumers with a third party that provides a separate good or service to consumers. Finally, firms select the price τ at which to sell their product.

Any firm that adopts the secure hardware derives a benefit insofar as the likelihood of it becoming the victim of a cyber-attack falls. In particular, any firm that does not adopt the secure hardware becomes the victim of a cyber-attack with probability p^H. This probability falls to $p^L < p^H$ if the secure hardware is adopted. We reflect the private costs to firms of adopting the secure hardware in a parameter c. As highlighted in Part 3.4, this cost should be thought of as including the opportunity costs of *not* adopting secure hardware (e.g. rewriting unsafe code). A successful cyber-attack generates consumer damage of η per affected user, which rises to $\eta(1+\phi)$ if data has been shared with the third party. Firms are held fully liable for the damages arising from cyber-attacks. On the other hand data sharing also generates a benefit equal to Δ per consumer whose data has been shared.

The timing of the game is summarized in the form of a game tree in Figure 3. In the first instance, firms simultaneously make their data sharing and hardware adoption choices. Thereafter, they select the optimal price to charge. The optimal price a firm charges will therefore typically depend on whether or not it and its rival have shared data with the third party and whether or not they have adopted the secure hardware.[26] In Figure 3, $h_i = A$ denotes the decision of firm i, $i = 1, 2$, to adopt the secure hardware, while $h_i = a$ denotes firm i's decision not to adopt the secure hardware. Similarly, $d_i = S$ denotes the decision by firm i to share data with the third party, while $d_i = s$ denotes firm i's decision not to share data. The optimal price charged by firm i, conditional on a given profile of first-stage hardware adoption and data sharing choices (d_1h_1, d_2h_2), is denoted by $\tau_i^{(d_1h_1,d_2h_2)}$. Similarly, $\pi_i^{(d_1h_1,d_2h_2)}$ denotes firm i's equilibrium profits given d_i, h_i and profit-maximizing pricing behaviour in the second stage.

A strategy for either firm consists of a hardware adoption and data sharing choice in the first stage, combined with a complete contingent pricing plan in the second stage (one price

[25] In the economics literature, this method of representing the market is known as Hotelling competition.

[26] Note that this element of sequential decision making takes this model slightly beyond the simple structure highlighted above. Nonetheless the economic intuition underlying its solution remain broadly the same.

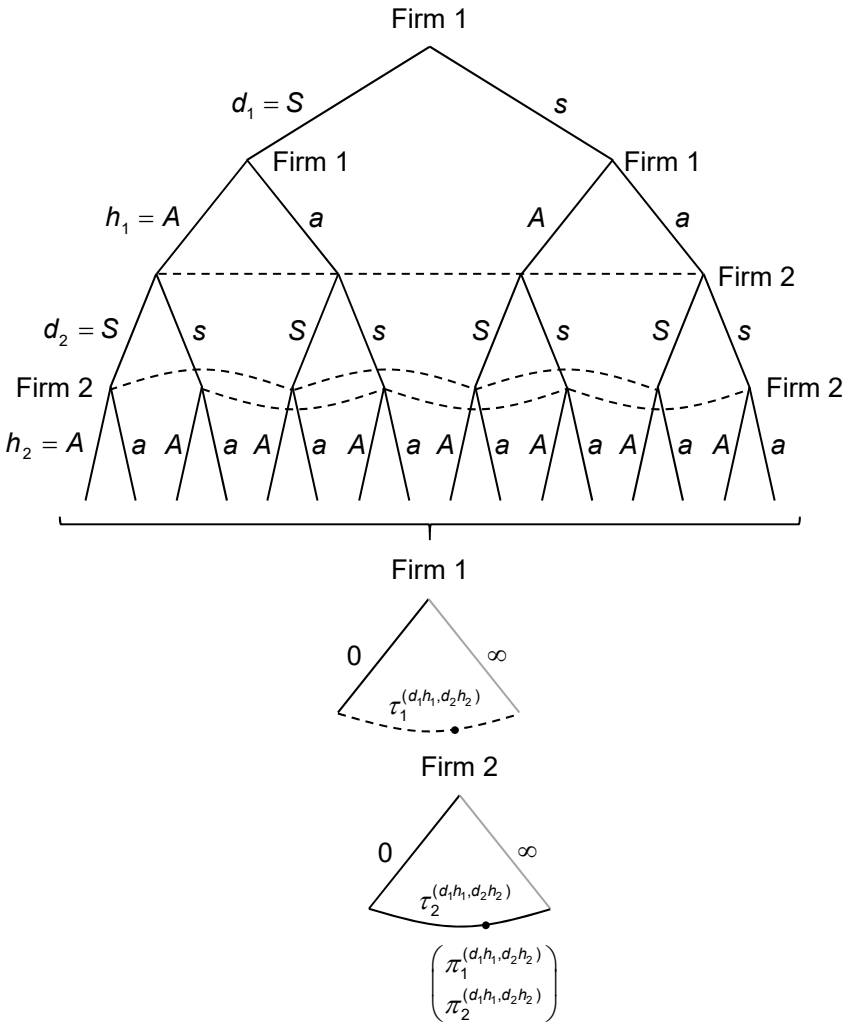


Figure 3. Game tree. Dashed lines connect decision nodes between which a player cannot distinguish, capturing decisions that are made simultaneously with earlier moves

for each possible outcome in stage 1). Given that each of the two firms has four possible combinations of first-stage hardware adoption and data sharing decisions, there are 16 cases that must be checked with respect to optimal prices in the second stage. In each case, optimal prices are derived by maximizing the respective firms' profit functions, which are built up in an intuitive manner from the model parameters described above and additional parameters capturing the properties of the market demand (see Lam and Seifert, 2023a, for details).

Given these optimal second-stage prices, the optimal first-stage hardware adoption and data sharing decisions are derived by identifying the parameter values at which a given profile of hardware adoption and data sharing choices (d_1h_1, d_2h_2) is free from profitable deviations for both firms, given that firms anticipate profit-maximizing prices in the following stage.[27] In

[27] In technical terms, this process of backward induction allows us to identify the subgame perfect Nash equilibria of the dynamic game.

general terms, each of the 16 cases features six possible deviations that firms might make, since each firm has three hardware adoption and data sharing choices that it could alternatively resort to. Joint consideration of these 96 deviation opportunities and their profitability in light of the model parameters allows the equilibrium outcome of the game to be determined.

4.2 Addressing Open Questions

Having outlined the general structure of the model, we now discuss how it can be used to address the open questions highlighted in Part 3.4.

4.2.1 Hardware Adoption Incentives & Data Sharing

The first open question concerns the determinants of firms' incentives to adopt secure hardware when firms also face a choice with respect to data sharing. It is helpful to relate the choices that firms make in these respects to two important model parameters: firstly, the adoption costs c; secondly, the benefits of data sharing Δ. As we discuss further when we link our theory to practice in Part 4.3, these parameters can capture a wide range of factors influencing data sharing and hardware adoption and also connect with several possible interventions to the data governance framework.[28]

Figure 4 describes the market outcomes in terms of data sharing and hardware adoption. This figure shows whether data is shared by one firm ('partial sharing'), both firms ('full sharing') or neither ('no sharing'), and whether secure hardware is adopted by one firm ('partial adoption'), both firms ('full adoption') or neither ('no adoption') for different levels of the adoption cost c and the data sharing benefit Δ. We see that the costs of hardware adoption and the benefits of data sharing influence firms' incentives to adopt secure hardware and to share data in intuitive ways. For a given data sharing benefit Δ, for example, the extent of hardware adoption in the market falls from full adoption to partial adoption to no adoption as the associated costs increase. Likewise, for a given cost of adoption c, the extent of data sharing in the market tends to be larger when the associated benefits Δ are large.

Figure 4 also sheds light on the interactions between firms' hardware adoption and data sharing incentives. These interactions are crucial in the context of OD markets. In particular, we can see that firms' incentives to adopt secure hardware can change, even if the cost of adoption remains constant. For example, for a given cost of adoption between $\overline{c}_2$ and $\overline{c}_3$, the market displays no adoption for low values of the data sharing benefit parameter Δ, which changes to partial adoption for intermediate levels of Δ and full adoption at high levels of Δ. The reason is that, as the benefits of data sharing increase and firms are more incentivized to

[28] A further important factor that drives incentives in the model concerns the magnitude of the security benefits associated with the new hardware, that is $p^H - p^L$. These benefits affect the position of the $\overline{\Delta}$ and $\overline{c}$ thresholds in Figure 4 below.

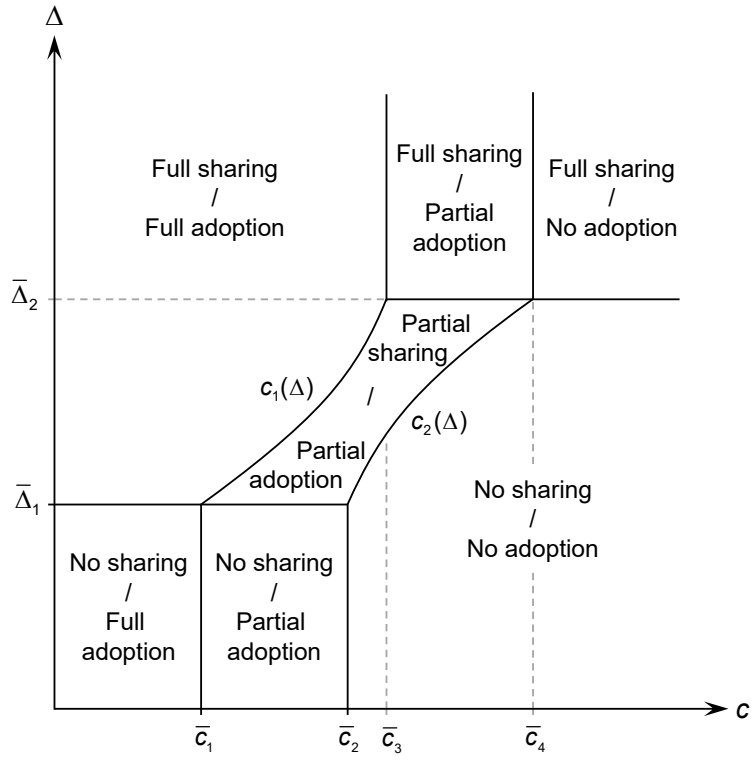


Figure 4. Market outcomes for hardware adoption and data sharing.

share data with the third party, their liability in case of a successful cyber-attack also increases. This increases the returns to investments in cyber-security, such that firms are more likely to adopt the secure hardware in order to reduce the likelihood of a successful breach.

This allows us to state:

Result 1. *Firms' incentives to adopt secure hardware in OD markets are positively related to the degree of data sharing.*

4.2.2 Market Failures

So far we have described the market outcomes that arise when firms select their hardware adoption and data sharing strategies to maximize profits. In order to determine whether or not market failures arise in this context we need to compare these privately optimal (profit-maximizing) decisions with the socially optimal decisions that society as a whole would impose on firms.[29] A market failure occurs whenever the market leads to hardware adoption or data sharing incentives that exceed or fall short of this socially optimal benchmark. In those cases,

[29] 'Society as a whole' in this context relates to the concept of total welfare, which is defined as the sum of firms' profits and consumer surplus.

it is interesting to consider what data governance measures can succeed in aligning privately and socially optimal decisions.

To facilitate this analysis, we need to consider the hardware adoption and data sharing decisions that maximize the well-being of society. In this social optimum, consumers are allocated to each of the two firms in order to maximize welfare, rather than allowing demand to be determined by price competition between the firms. It should be noted that this analysis represents a theoretical benchmark in terms of the maximum well-being that society could attain rather than a practical guide as to how desirable outcomes in OD markets can be achieved.

The socially optimal hardware adoption and data sharing decisions are qualitatively similar to those that were derived in the private optimum above and are presented in Figure 5. Data sharing and hardware adoption decisions display similar interactions to those described in Result 1 above. This goes back to the observation by our interviewees that regulators face similar trade-offs between reducing cyber-vulnerabilities and the associated costs when deciding a minimum level of security to impose in OD markets (see *A4*).

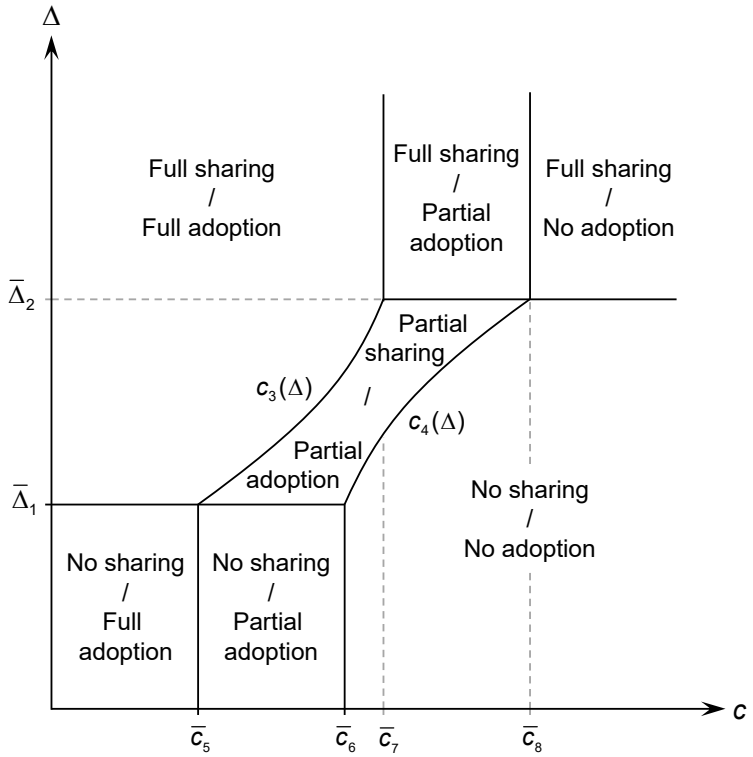
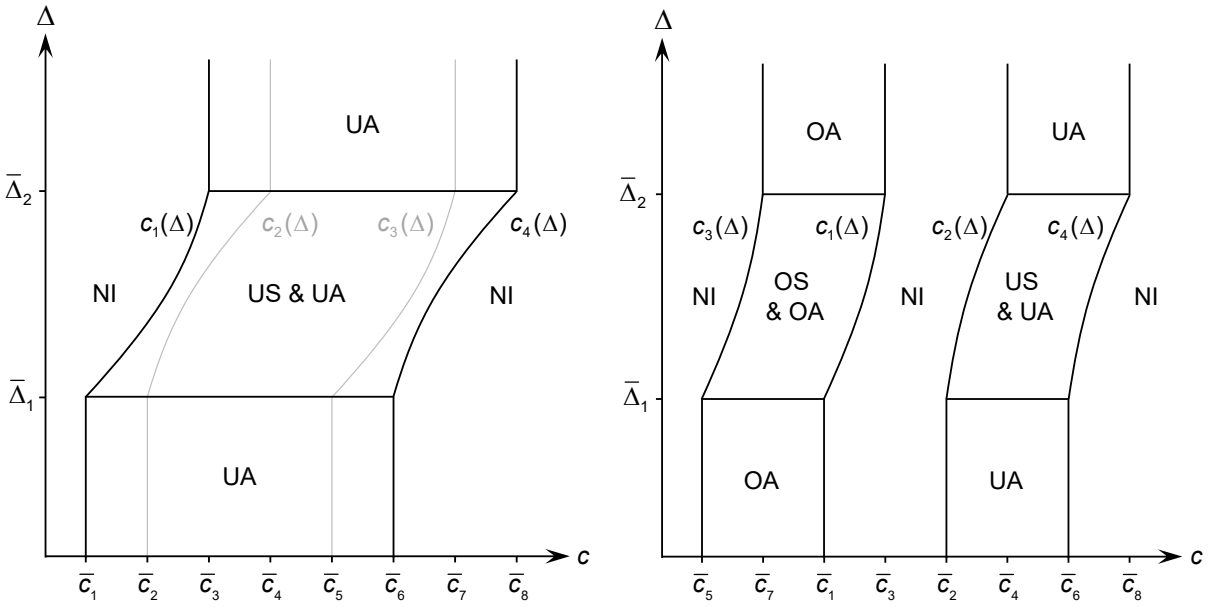


Figure 5. Socially optimal hardware adoption and data sharing outcomes

The differences between Figures 4 and 5 lie in the levels of the cost thresholds $\overline{c}_1 - \overline{c}_8$. In order to identify whether a market failure occurs when hardware adoption and data sharing decisions are left to firms that maximize profits, we need to overlay the partitions in Figures 4 and 5. This is done in Figure 6 below. In this figure, we distinguish between two cases. Panel

(a) depicts the case in which the firms produce highly differentiated products, while panel (b) shows the case in which the firms' products are relatively homogeneous or similar to one another. This figure highlights the situations in which the market equilibrium leads to under-adoption (UA), under-sharing (US), over-adoption (OA) and over-sharing (OS) relative to the social optimum. If none of these market failures arises, private and socially optimal decisions coincide with one another and we require no intervention (NI).



(a) Highly differentiated products **(b)** Less differentiated products

Figure 6. Potential market failures in data sharing and secure hardware adoption

It is interesting to note that the type of market failure that arises is linked to the nature of competition in the market. When firms sell highly differentiated products, the only market failures relate to under-adoption and under-sharing. When firms' products are less differentiated (more homogeneous), it is possible to have situations in which firms adopt secure hardware and share data over and above the levels that maximize the well-being of society as a whole.

Result 2. *The market always generates under-sharing and under-adoption for some levels of c and Δ. When firms' products are sufficiently homogeneous, over-sharing and over-adoption can arise in some cases.*

This result can be understood as follows. When firms sell highly differentiated products, the market can be viewed as less competitive because consumers are more reluctant to switch from purchasing the good or service from their preferred firm. In this context, the competitive advantage that a firm gains by adopting secure hardware or by sharing consumers' data is relatively small in terms of the number of additional customers it can attract. When firms'

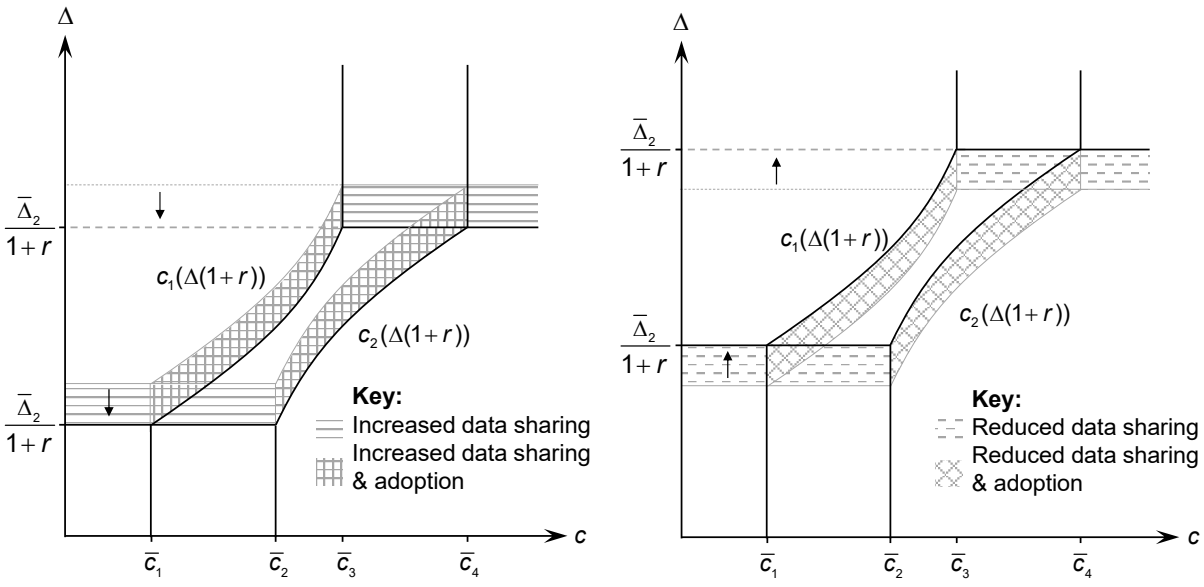
products are more homogeneous, however, the degree of competition between firms is more intense and firms can compete with each other in terms of hardware adoption and data sharing to such an extent as to generate over-sharing and over-adoption in some cases.

We now consider the nature of the data governance measures that might resolve the market failures identified above.

4.2.3 Data Governance & Regulation

Given the interactions between firms' hardware adoption and data sharing decisions described above, it is interesting to consider the extent to which interventions targeting the magnitude of the data sharing benefit Δ can correct the market failures identified in Figure 6 above. Consider a policy r that, if implemented, results in firms earning data sharing benefits equal to $\Delta(1+r)$. The case of positive r can be thought of in terms of relaxations of technical requirements governing data anonymization, encryption and interoperability, for example. The case of a negative r corresponds to stricter requirements in these areas or a tax on data sharing profits (see further Part 4.3).

The consequences of these policies in terms of changing the market-wide hardware adoption and data sharing outcomes is summarized below.



(a) Pro-sharing policies ($r > 0$) **(b)** Anti-sharing policies ($r < 0$)

Figure 7. Correcting market failures through data sharing policies

We see that, by shifting the $c_1(\Delta(1+r))$ and $c_2(\Delta(1+r))$ thresholds rightwards, pro-sharing policies can correct market failures relating to under-sharing and under-adoption when the firms' products are highly differentiated (panel (a) of Figure 6). Nonetheless, promoting secure hardware adoption by encouraging data sharing also creates new regions in which firms over-

share data relative to the social optimum. Moreover, since $c_1(\Delta(1+r))$ and $c_2(\Delta(1+r))$ always move in the same direction, it is not possible to correct the over-sharing and over-adoption failures that occur when firms sell similar products without simultaneously worsening the under-sharing and under-adoption failures that occur in other regions of the parameter space. Finally, it is possible to show that, despite the beneficial effects of r in some cases, this policy cannot align the market outcomes in terms of hardware adoption and data sharing completely with the socially optimal outcomes.

A related policy could involve subsidies on hardware adoption costs c. These policies have similar effects to those described in the context of r above, though they do not affect the $\overline{\Delta}_1$ and $\overline{\Delta}_2$ thresholds. Nonetheless, it is again the case that no policy exists in this class that perfectly aligns market outcomes with the socially optimal ones. Therefore we have:

Result 3. *Policies targeting data sharing benefits and hardware adoption costs can mitigate market failures in some cases but they cannot perfectly align privately and socially optimal hardware adoption and data sharing incentives.*

We now consider the final open question, which concerns the role of competition.

4.2.4 Competition

The preceding discussion has considered how market incentives can be more closely aligned with the social optimum in a market comprising two competing firms. A related question concerns the role that market structure itself plays in determining data sharing and hardware adoption incentives. The degree of competition matters in this context because investments in hardware adoption depend largely on what a firm's rivals do in OD markets. For example, in the banking and energy sectors, the market can be highly competitive at the retailing stage. To assess the effectiveness of promoting competition as a means of improving consumer welfare in OD markets, it is crucial to consider the impact that greater competition has on firms' hardware adoption and data sharing decisions.

We may explore the impact of competition by comparing market outcomes in the baseline model described above, featuring competition between two firms, with those arising when the market is instead served by a single monopolist. Consider, therefore, the market outcomes for secure hardware adoption and data sharing that would arise if the market were served by a single monopolist. These outcomes are summarized in the (c,Δ) space below.

In principle, competition can exert both positive and negative effects on hardware adoption and data sharing incentives. On the one hand, competition generates new incentives for hardware adoption and data sharing when doing so allows a firm to steal market share from its rival (the business stealing effect). Indeed, we have seen that, when firms' products are

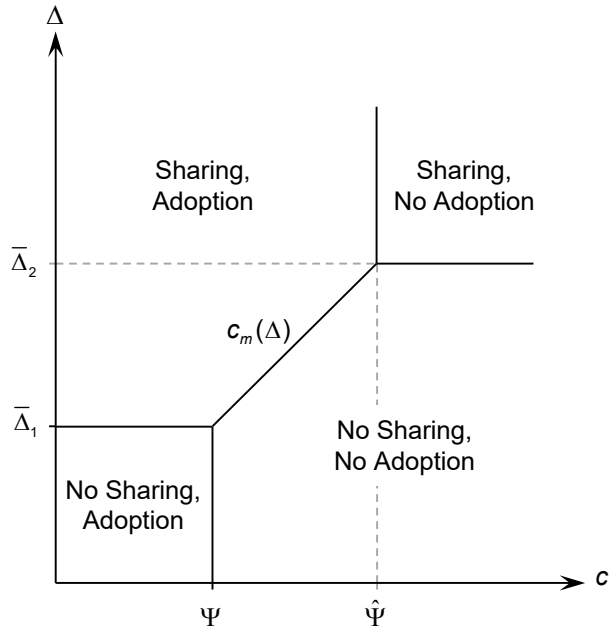


Figure 8. Data sharing and hardware adoption outcomes in the monopoly case

relatively homogeneous, competition between firms can lead to hardware adoption and data sharing levels that go beyond the socially optimal level (Figure 6). On the other hand, when demand is concentrated within a single monopolistic firm, the liability for cyber-damages is similarly concentrated at a single firm, which consequently enjoys greater marginal benefits from secure hardware adoption (the demand effect).

By overlaying Figures 4 and 8 we can see that the latter effect dominates, see Figure 9. Regardless of the level of the data sharing benefit Δ, competition reduces secure hardware adoption for intermediate levels of the adoption cost parameter c. For intermediate levels of Δ, competition can also reduce data sharing, thereby reducing the effectiveness of OD initiatives themselves.

The negative effect of competition on hardware adoption incentives is due to the differences in the marginal returns derived from the costly adoption of a new technology described above. A monopolist serves the entire market and therefore the benefit in terms of reduced liability for cyber-damages applies across a relatively large group of consumers. By contrast, each competing firm serves only a subset of consumers, and therefore the benefit in terms of reduced liability for the cyber-damages they suffer is similarly scaled down. For very high (low) levels of the adoption cost parameter, adopting the secure hardware is suboptimal (optimal), regardless of the market structure.

A similar logic explains why competition can, in some circumstances, reduce data sharing. When demand is split between multiple firms, individual firms can extract fewer data sharing benefits from consumers via the third party, all else equal, than does a monopolist that serves

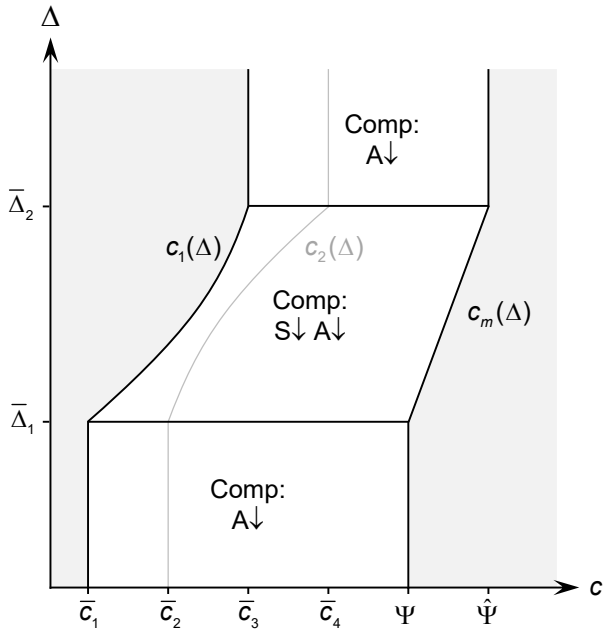


Figure 9. Comparison of market outcomes: competition vs. monopoly

the entire market. Therefore it is possible that these data sharing benefits outweigh the associated costs in terms of increased cyber-risk for the monopolist but not for a competing firm. Interestingly, in order for competition to reduce data sharing, it is necessary for competition also to reduce secure hardware adoption. This is intuitive since, without the secure hardware, competing firms are even less likely to share data and incur the associated cyber-risks than is a monopolist that has adopted the secure hardware.

It is nonetheless possible to show that the impact of competition on *welfare* is ambiguous, even when competition unambiguously reduces hardware adoption and data sharing. Competition generates welfare benefits in the form of product differentiation that allows consumers to purchase goods or services that are closer to their preferences. Depending on the specific case being considered, these benefits can outweigh or fall short of the welfare benefits that monopoly brings in terms of increased security, increased data sharing and the avoidance of duplicate investments into identical technologies.

Result 4. *Competition tends to reduce hardware adoption and data sharing but may increase or decrease social welfare.*

We conclude this discussion by connecting the structure and results of this model more closely with practice.

4.3 Linking Theory to Practice

Our model captures the economic setting of OD markets in which data sharing by firms leads to economic benefits while at the same time generating new cyber-risks. This cyber-risk is mitigated by the (costly) adoption of secure hardware. We now reflect in more detail on how the model parameters connect with the issues highlighted in our primary data analysis, and on the implications that emerge from our analysis for the UK data governance framework.

Model Parameters

The damages resulting from cyber-breaches are reflected in the η parameter. This η represents the monetary damages that consumers suffer as the result of fraudulent payment instructions or imitation attacks in the OB context (see Part 2.1.1), for example, but also broader non-monetary harms that were identified by our interviewees. The level of η will generally vary depending on the specific market setting and the sensitivity of the data that is being shared (A_2, A_3, A_{27}, O_2). This data may be sensitive enough for data breaches to generate threats to life (A_{22}), which translates here into particularly high levels of η. Finally, η is also likely to be related to the size of the market in which firms operate (O_3). The fact that damages resulting from a cyber-attack at one firm may spill over to other firms (A_{21}) is reflected here in the ϕ parameter, which measures the extent of cyber-damages arising at the third party, conditional on data having been shared by a firm that suffers a data breach.

The benefits that data sharing between firms and TPPs can generate are the main motivation for OD schemes. These are reflected in the model in the Δ parameter. In addition to the direct benefits of OD schemes discussed in Part 2.1, this parameter can be related to the wider gains from data sharing that our interviewees identified. For example, Δ may relate to benefits associated with increased access to financial services and increased consumer choice in the OB setting (O_5). In energy markets, Δ may reflect the benefits associated with reduced gas leaks when smart meter data is shared more widely (O_6).

The hardware adoption cost c reflects the monetary costs of purchasing new technology. In addition to these direct costs, it can reflect the costs associated with time and staff training and ensuring interoperability with legacy systems (A_9, A_{20}). The level of c may also be positively related with the complexity of replacing existing technological work-arounds (A_{11}), reductions in system usability (A_{12}), the costs associated with pre-adoption trial periods (A_{14}) and the length of planning horizons (A_{15}). As discussed in Part 3.4, c should also be seen as reflecting the opportunity costs of failing to adopt secure hardware, such as the costs of rewriting unsafe code or the reputational costs associated with unresolved vulnerabilities (Microsoft, 2020).

Data Governance & Market Implications

Our results have highlighted a number of potential market failures that can arise when hardware adoption and data sharing choices are left to the market (Result 2). The tendency for under-adoption of secure hardware in particular to arise goes back to the list of factors our interviewees identified as obstacles to secure hardware adoption. Besides costs (A_9), these include issues around awareness (A_{10}) and the perception that hardware security may be of secondary importance beside other commercial considerations (A_{11}), especially when new hardware has usability implications (A_{12}). This result also connects with the relatively low score we identified in the quantitative analysis of our primary data in relation to the rate at which secure hardware is currently being adopted (Part 3.2).

At the same time, we have discussed measures that impact the magnitude of data sharing benefits and hardware adoption costs, which can mitigate but not totally resolve these market failures (Result 3). In terms of data governance interventions, we have seen that policies that promote or hinder data sharing by increasing or decreasing the magnitude of data sharing benefits can partially resolve market failures in relation to under-adoption or over-adoption. These types of policies are closely related to various aspects of the data governance framework. For example, the degree to which firms benefit from data sharing depends on the degree to which data that is shared must be anonymized, must meet interoperability requirements of other firms and providers. This connects with the comments of interviewees emphasizing a preference for a balance between top-down and bottom-up approaches (G_2, G_3).

In terms of top-down measures, we can interpret policies that impact the cost of adoption c in terms of fines for non-adoption in the context of a minimum security standard, for example (G_4). Bearing in mind that c reflects the opportunity cost of non-adoption, c may be lowered by increasing the reputational costs of cyber-attacks, for example via data ethics and responsible innovation rules. In terms of the bottom-up approach, our interviewees have highlighted the importance of guidance in this area (G_5, G_8).

Our model also highlights the importance of taking interactions between hardware adoption and data sharing incentives into account. An illustrative example concerns the distinction between data anonymization (the irreversible modification of personal data to prevent re-identification of the data subject) and pseudonymization (which allows data controllers and third parties to re-identify individuals by reference to additional information) (Article 4(5) UK GDPR). While anonymization may provide greater security in and of itself, if it reduces the value that third-parties can extract from this data when it is shared it may also discourage data sharing and, indirectly, the adoption of more secure hardware. The broader message is that data sharing needs to be taken into account when assessing firms' incentives to adopt secure hardware.

Finally, our model sheds light on the role of competition in incentivizing hardware adoption and data sharing. We have seen that, in line with the insights gathered from our interviews,

competition is associated with diverse effects that tend simultaneously to promote hardware adoption through a business stealing effect (C_3) and to hinder adoption due to the demand effect (C_1, C_2, C_4).

Part 5

Conclusion

This report investigates firms' incentives to adopt secure hardware in OD markets, in which data may also be shared with third-party firms. Since OD schemes typically involve especially sensitive consumer data, such as bank transaction and energy consumption data, these markets are particularly relevant for the study of secure hardware adoption incentives. While OB and OD schemes are motivated by the substantial economic benefits that data sharing can create, the more widespread sharing of data can also generate additional cyber-risks when there is a chance of hackers gaining unauthorized access to that data. For this reason, it is reasonable to suppose that hardware adoption and data sharing incentives may be interdependent in OD markets. In order for secure hardware adoption incentives to be accurately described in the OD context, these interdependencies between hardware adoption and data sharing must be taken into account.

We first provide an overview of the UK data governance framework. This includes a description of OB, the most well-developed of the existing OD schemes in the UK. We highlight that security considerations already play a significant role, for example in the form of the RTS that mandate strong customer authentication. Since the data governance framework governing the use of data in OD markets extends beyond the specific structures underlying OB, however, we also discuss the broader rules and regulations in the areas of cybersecurity, data privacy, anonymization, interoperability, data ethics and responsible innovation.

Our investigation of hardware adoption incentives begins with an analysis of primary data that was gathered through interviews with both regulators and private sector firms. At a general level, these interviews highlight the importance of security in firms' hardware adoption decisions. They further provide detailed insights into the factors that promote and hinder secure hardware adoption in OD markets. In terms of their view of the data governance framework, it was notable that participants emphasized the advantages of a balanced approach between bottom-up and top-down regulation. This contrasts with the results that were reported in the analysis of previous interviews, which displayed a preference for a centralized approach to regulation in the context of investments in cybersecurity (see Lam and Seifert, 2021).

We also present the results of an original game-theoretic model that allows us to formalize hardware adoption incentives in OD markets. We show, firstly, that OD markets indeed represent an important and distinct class of markets for the study of hardware adoption incentives in the sense that a firm is more likely to adopt secure hardware when data is shared with a TPP because data sharing increases its expected liability in the case of a cyber-attack. Our model also makes the nature of market failures precise. While we find that there are always cases in which the market does not provide adequate incentives for secure hardware adoption (and data sharing), we also show that firms can over-adopt and over-share when their products are sufficiently homogeneous. Interventions to the data governance framework can impact the nature of these market failures in a variety of ways, of which we focus on measures that either change the data sharing benefits accruing to firms or the cost of adopting secure hardware. While these measures can resolve market failures to some extent, we find that they do not guarantee that the market will always generate the socially preferred outcome in terms of hardware adoption and data sharing. Finally, we show that, while competition reduces both hardware adoption and data sharing, it may increase or decrease social welfare.

These results concerning the interactions between hardware adoption and data sharing incentives in OD markets extend existing economic research in the area of digital security.[30] In future work it will be interesting to explore the implications of the interactions we identified in the OD setting for the broader Open Economy, including Internet of Things (IoT), lifestyle and healthcare data.

Another future research avenue is the institutional design of cybersecurity regulation. Part 2.1.1 shows that the UK has adopted a regulation-focused approach to OB rather than relying on markets as the US has done. As noted by our interviewees, one disadvantage of such a top-down regulatory approach lies in the costs of ensuring effective and coherent enforcement with existing laws. Moreover, there are coordination costs between organizations in practice. For instance, there are a number of existing authorities in the UK which can be considered candidates for enforcing cybersecurity rules, for example, the NCSC, the ICO, as well as the banking, competition and consumer protection authorities. The government could also designate a higher-level authority to oversee cybersecurity issues, as noted by our interviewees. However, Lam (2021) cautions that conferring status to an overarching authority without improving coordination issues between authorities and organizations could be detrimental to society as a whole. The nature and type of these coordination issues and the best mitigating coordination mechanism could be a fruitful area for future research.

These challenges also extend to the international context given the cross-border nature of many digital interactions, globally linked supply chains and the associated cyber-threats. The importance of extending cooperation in the area of cybersecurity across borders has been em-

[30] While previous research in this area is rather limited, Lam and Seifert (2023b) study related interactions between data privacy and cybersecurity when firms can make investments that reduce the probability of cyber-attacks.

phasized in World Economic Forum (2021), who highlight the advantages of the NCSC's Cyber Assessment Framework in terms of its alignment with international counterparts such as the US National Institute of Standards and Technology Cybersecurity Framework, for example. The difficulty of reaching international agreements in relation to consumer data is emphasized by the legal challenges to the updated EU-US Privacy Shield (the Trans-Atlantic Data Privacy Framework). These challenges in the context of international coordination of data privacy regulation are particularly relevant in light of the interactions between data privacy (data sharing) and cybersecurity that we highlight in this report.

Finally, there is a lot of scope to extend the investigation of data privacy and cybersecurity issues in the specific context of AI. Our results, interpreted broadly in terms of the adoption of new technologies, are very relevant in light of the discussions around the speed of adoption of generative AI. While many companies are racing to develop new technologies and bring them to market, adoption costs in this area are impacted by the evolving data governance framework (Part 2.2.3), with some countries banning specific AI chatbots entirely. Generative AI raises data access challenges, both in terms of the way in which inputs are gathered to train the model and the way in which this data is subsequently shared through interactions with users. Cybersecurity issues arise because, as we have shown, data sharing typically necessitates higher degrees of security, especially when the combination of different data sources has the potential to create a unified data set that is far more sensitive than the original data sets, so that the damages of cyber-vulnerabilities are correspondingly large.

Appendix:
Details of Qualitative Data Analysis

Our qualitative data analysis is based on the method of inductive thematic analysis (Patton, 1990; Boyatzis, 1998; Braun and Clarke, 2006; Mihas, 2023). This method allows patterns (themes) to be identified in complex qualitative data sets. Our data set in this case comprises the responses that we collected from interview participants to the series of open-ended questions that we put to them in the course of our interviews. We followed existing standards for applying the method of thematic analysis within the social sciences by first familiarizing ourselves with the broad data set, searching and reviewing themes before producing our report (see Braun and Clarke, 2006, for further details).

The themes that we have identified relate in a direct way to the research questions that this project is exploring, concerning the factors that promote and hinder the adoption of secure hardware and the specific role played by data sharing, for example. Beyond this, we have sought to balance the objective of giving a broad thematic description of our entire data set with that of going into detail on specific themes by providing an extensive list of detailed points within each theme. This is important to give an idea of the breadth of the responses that we received. Where appropriate, we have emphasized the relevance of individual points within a theme by indicating the frequency with which they occurred throughout our series of interviews ('several / all respondents highlighted', etc.).

The advantage of this approach lies in the flexibility it affords us in extracting relevant messages from our qualitative interview data. The disadvantages include the fact that alternative ways of grouping the data into themes may also have been chosen. We have dealt with this issue by going into extensive detail within each theme so that the outcomes of our interviews are represented at a broad level. Another potential drawback of separating responses into themes is that connections and interactions between the themes may not emerge clearly. This is particularly relevant in light of the interactions between secure hardware adoption and data sharing that we emphasize in our theoretical model (Part 4). We have dealt with this by beginning the presentation of our results with the broader themes concerning the drivers of secure hardware adoption at a general level, before moving on to more detailed themes such as the

relevance of OD markets. In this way, the later themes and the points included within them can be read in the context of the earlier, foundational points.

Bibliography

BOYATZIS, R. E. (1998). *Transforming Qualitative Information: Thematic Analysis and Code Development*. Thousand Oaks, Calif.: Sage.

BRAUN, V. and CLARKE, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, 3 (2), 77–101.

CENTRAL DIGITAL & DATA OFFICE (2021). Data Standards Authority Strategy 2020 to 2023. *https://www.gov.uk/guidance/data-standards-authority-strategy-2020-to-2023*.

CENTRAL DIGITAL & DATA OFFICE (2022). Data Sharing Governance Framework. *https://www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework*.

CFPB (2022). Outline of Proposals and Alternatives Under Consideration for the Personal Financial Data Rights Rulemaking. *https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf*.

CMA (2023). CMA Letter to HSBC About Breaches of the Retail Banking Order. *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1129899/CMA_letter_to_HSBC_about_breaches_of_the_Retail_Banking_Order.pdf*.

DELOITTE (2018). Open Banking Around the World: Towards a Cross-Industry Data Sharing Ecosystem. *https://www.deloitte.com/global/en/Industries/financial-services/perspectives/open-banking-around-the-world.html*.

DELOITTE (2022). Open Finance: Preparing for Success. *https://ukfinancialservicesinsights.deloitte.com/post/102hlis/open-finance-preparing-for-success#:~:text=Open%20Finance%20is%20part%20of,communications%2C%20energy%2C%20and%20finance*.

EQUALITY AND HUMAN RIGHTS COMMISSION (2022). Strategic Plan 2022–25. *https://www.equalityhumanrights.com/sites/default/files/about-us-strategic-plan-2022-2025.pdf*.

EU AGENCY FOR FUNDAMENTAL RIGHTS (2022). Bias in Algorithms: Artificial Intelligence and Discrimination. *https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf*.

EUROPEAN COMMISSION (2022). Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy. *Press Release of February 23, 2022*, *https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113*.

EXPERIAN (2020). Open Data and Open Banking – What Does the Future Hold? *https://www.experian.co.uk/blogs/latest-thinking/data-insights-and-analytics/open-data-and-open-banking-what-does-the-future-hold/#:~:text=In%20an%20open%20banking%20world,key%20to%20enhancing%20customer%20relationships*.

FCA (2021). Changes to the SCA-RTS and to the Guidance in 'Payment Services and Electronic Money – Our Approach' and the Perimeter Guidance Manual. *Policy Statement PS21/19*, *https://www.fca.org.uk/publication/policy/ps21-19.pdf*.

FINANCIAL TIMES (2022). Fintechs say UK Credit Cards Restrict Access to Consumers' Own Data. October 9, 2022.

FORBES (2012). How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. February 16, 2012.

FORBES (2022). How Open Banking Changes The Attack Surface. June 29, 2022.

FOREIGN POLICY (2021). Big Tech's Stranglehold on Artificial Intelligence Must Be Regulated. *https://foreignpolicy.com/2021/08/11/artificial-intelligence-big-tech-regulation-monopoly-antitrust-google-apple-amazon-facebook/*.

FRONTIER ECONOMICS (2021). Increasing Access to Data Across the Economy. *A report prepared for the Department for Digital, Culture, Media and Sport*, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974532/Frontier-access_to_data_report-26-03-2021.pdf*.

HM GOVERNMENT (2020a). National Data Strategy. *Policy Paper*, *https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy*.

HM GOVERNMENT (2020b). Data Ethics Framework. *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923108/Data_Ethics_Framework_2020.pdf*.

HM GOVERNMENT (2022a). Government Response to the Consultation on a New Pro-Competition Regime for Digital Markets. *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1073164/E02740688_CP_657_Gov_Resp_Consultation_on_pro-comp_digital_markets_Accessible.pdf*.

HM GOVERNMENT (2022b). Establishing a Pro-Innovation Approach to Regulating AI. *https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement*.

HM GOVERNMENT (2022c). Software and AI as a Medical Device Change Programme. *https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme*.

HM GOVERNMENT (2022d). Consultation on the Future Regulation of Medical Devices in the United Kingdom. *https://www.gov.uk/government/consultations/consultation-on-the-future-regulation-of-medical-devices-in-the-united-kingdom*.

HM TREASURY (2023). Payment Services Regulations: Review and Call for Evidence. *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1128749/Payment_Services_Regulations_Review_and_Call_for_Evidence.pdf*.

ICO (2012). Anonymisation: Managing Data Protection Risk Code of Practice. *https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf*.

ICO (2021). Data Sharing Code of Practice. *https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice-1-0.pdf*.

ICO (2022a). AI and Data Protection Risk Toolkit. *https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection-0-0.pdf*.

ICO (2022b). Explaining Decisions Made With AI. *https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-artificial-intelligence-1-0.pdf*.

ICO (2022c). Guidance on AI and Data Protection. *https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection-0-0.pdf*.

INTEL (2022). Intel Study: Secure Systems Start with Hardware. *https://www.intel.com/content/www/us/en/newsroom/news/study-secure-systems-start-hardware.html*.

JOINT REGULATORY OVERSIGHT COMMITTEE (2023). Recommendations for the Next Phase of Open Banking in the UK. *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1150988/JROC_report_recommendations_and_actions_paper_April_2023.pdf*.

LAM, W. (2021). A Theory of Status and Coordination in Organizations. *Oxford Economic Papers*, 73 (2), 837–855.

— and LIU, X. (2020). Does Data Portability Facilitate Entry? *International Journal of Industrial Organization*, 69, 102564.

— and SEIFERT, J. (2021). Regulatory Interactions and the Design of Optimal Cybersecurity Policies. *Commissioned Project Report, ESRC Digital Security by Design Social Science (Discribe) Hub+*, *https://static1.squarespace.com/static/5f8ebbc01b92bb238509b354/t/618cf3a82f816f66d11dd4cc/1636627370520/Lam+Seifert+Final+Project+Report.pdf*.

— and — (2023a). Data Sharing and Secure Hardware Adoption. *Working Paper*.

— and — (2023b). Regulating Data Privacy and Cybersecurity. *Journal of Industrial Economics*, 71 (1), 143–175.

MCKINSEY & COMPANY (2016). The Age of Analytics. Competing in a Data-Driven World. *McKinsey Global Institute Report*, *https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world*.

MCKINSEY & COMPANY (2021). Financial Data Unbound: The Value of Open Data for Individuals and Institutions. *Discussion Paper*, *https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world*.

MICROSOFT (2020). Security Analysis of CHERI ISA. *Microsoft Security Response Center Paper*, *https://github.com/microsoft/MSRC-Security-Research/blob/master/papers/2020/Security%20analysis%20of%20CHERI%20ISA.pdf*.

MIHAS, P. (2023). Qualitative Research Methods: Approaches to Qualitative Data Analysis. *International Encyclopedia of Education*, vol. 12, 4th edn., Elsevier, pp. 302–313, *https://doi.org/10.1016/B978-0-12-818630-5.11029-2*.

OECD (2015). *Data-Driven Innovation: Big Data for Growth and Well-Being*. Paris: OECD Publishing, *https://doi.org/10.1787/9789264229358-en*.

— (2019). *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*. Paris: OECD Publishing, *https://doi.org/10.1787/276aaca8-en*.

OFCOM (2020). Open Communications – Enabling People to Share Data with Innovative Services. *Statement of November 10, 2020*, *https://www.ofcom.org.uk/consultations-and-statements/category-1/open-communications*.

OFGEM (2020). Update on the Midata in Energy Programme. *Open Letter of May 27, 2020*, *https://www.ofgem.gov.uk/publications/update-midata-energy-programme*.

ONETRUST (2022). UK: Overview of the Data Protection and Digital Information Bill. *https://www.dataguidance.com/opinion/uk-overview-data-protection-and-digital-information*.

OPEN BANKING STRATEGIC WORKING GROUP SECRETARIAT (2023). The Future Development of Open Banking in the UK. *Final report for the Joint Regulatory Oversight Committee*, *https://www.openbanking.org.uk/wp-content/uploads/SWG-Report-The-Future-Development-of-Open-Banking-in-the-UK-Feb-2023.pdf*.

OPEN DATA INSTITUTE (2021). Data Ethics Canvas. *https://theodi.org/wp-content/uploads/2021/07/Data-Ethics-Canvas-English-Colour.pdf*.

PATTON, M. Q. (1990). *Qualitative Evaluation and Research Methods*. Newbury Park, Calif.: Sage, 2nd edn.

PENSIONS DASHBOARDS PROGRAMME (2022). Progress Update Report: April 2022. *https://www.pensionsdashboardsprogramme.org.uk/wp-content/uploads/2022/04/PDP-Progress-Report_April-22.pdf*.

PWC (2018). The Future of Banking is Open: How to Seize the Open Banking Opportunity. *Report*, *https://www.pwc.co.uk/financial-services/assets/open-banking-report-web-interactive.pdf*.

SALT SECURITY (2022). Salt Security State of API Security Report Reveals API Attacks Increased 681% in the Last 12 Months. Press Release of March 2, 2022.

STATISTA (2022). Estimated Cost of Cybercrime Worldwide from 2016 to 2027. *https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide/#:~:text=Estimated%20cost%20of%20cybercrime%20globally%202016%2D2027&text=The%20global%20cost%20of%20cybercrime,U.S.%20dollar%20mark%20in%202023.*

THE ROYAL SOCIETY (2020). The UK Data Governance Landscape. *https://royalsociety.org/-/media/policy/projects/data-governance/uk-data-governance-explainer.pdf*.

US DEPARTMENT OF COMMERCE (2022a). Cybersecurity Considerations for Open Banking Technology and Emerging Standards. *National Institute of Standards and Technology Report 8389*, *https://doi.org/10.6028/NIST.IR.8389-draft*.

US DEPARTMENT OF COMMERCE (2022b). Hardware-Enabled Security: Policy-Based Governance in Trusted Container Platforms. *National Institute of Standards and Technology Report 8320B*, *https://doi.org/10.6028/NIST.IR.8320B*.

US DEPARTMENT OF COMMERCE (2022c). Hardware-Enabled Security: Machine Identity Management and Protection. *National Institute of Standards and Technology Report 8320C*, *https://doi.org/10.6028/NIST.IR.8320C.ipd*.

WORLD ECONOMIC FORUM (2021). To Counter Cyber Risks to Critical Sectors such as Aviation We Need International Collaboration. *https://www.weforum.org/agenda/2021/04/cybersecurity-aviation-international-regulation/*.

WORLD ECONOMIC FORUM (2023). Why we Need Global Rules to Crack Down on Cybercrime. *https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/*.