THE JOURNAL OF INDUSTRIAL ECONOMICS 0022-1821
Volume LXXI March 2023 No. 1

REGULATING DATA PRIVACY AND CYBERSECURITY*

WING MAN WYNNE LAM†
JACOB SEIFERT‡

This paper studies firms' data privacy and cybersecurity choices. We emphasise the strategic interdependence between these decisions and demonstrate that security in both the market equilibrium and the social optimum tends to be higher when data is shared. We also identify important market failures in the sense that firms tend to under-invest in security and over-share data. Our welfare analysis of a minimum security standard, disclosure and consumer education policies, liability rules and consumer mitigation strategies highlights the need for a co-ordinated approach to regulation.

'If data are the new oil, data breaches should be treated like oil spills.'
– The Economist, August 10, 2019[1]

I. INTRODUCTION

CONSUMER DATA ARE AN INCREASINGLY VALUABLE COMMODITY in today's digitalized economy. The global data market is valued at $25–49 billion, and the share of Amazon's c.$1.5 trillion market valuation that is accounted for by consumer data has been estimated at 16%.[2] Against this backdrop, the decisions that firms make with respect to disseminating consumer data are

*We thank the Editor, Alessandro Bonatti, and two referees for helpful comments that have substantially improved the paper. We also thank David Ulph, Tommaso Valletti, seminar participants in Norwich and participants of the 2021 Royal Economic Society Conference for helpful feedback and discussion. Financial support from the ESRC Digital Security by Design Social Science (Discribe) Hub+ (grant number ES/V003666/1) is gratefully acknowledged by both authors. The usual disclaimer applies.

†Authors' affiliations: Norwich Business School and Centre for Competition Policy, University of East Anglia, Norwich Research Park, Norwich, NR4 7TJ, UK.
e-mail: wing.m.lam@uea.ac.uk
‡School of Business, Department of Economics, Finance and Accounting, University of Leicester, Leicester, LE1 7RH, UK.
e-mail: jacob.seifert@leicester.ac.uk

[1] For a historical perspective on big oil vs. big data in regulation, see Lamoreaux (2019).

[2] Li *et al.* [2019], Statista [2018] and OnAudience [2018]. Market size figures capture expenditure on collecting, purchasing and processing data.

of substantial policy interest. We here distinguish between two important avenues via which dissemination may occur. *Data privacy* describes the voluntary agreements that firms make to share data. *Cybersecurity* captures firms' efforts to prevent the unauthorised accessing of data by computer hackers. The main contributions of this paper are to analyse the interactions between firms' optimal privacy and cybersecurity strategies, and to study the regulatory implications of firms' interdependent decision making in these areas.

The importance of regulating firms' privacy and cybersecurity activities is emphasised by high-profile security breaches and instances of excessive data sharing. Cambridge Analytica's harvesting of Facebook profile data is perhaps the most well-known privacy breach of recent times (Guardian [2018]).[3] On the cybersecurity side, hacks have targeted numerous businesses including Facebook (Financial Times [2018]) and credit rating agency Equifax (BBC [2019]). More recently, Zoom Video Communications has become the subject of a class action lawsuit over its practice of sharing consumer data with third parties, at the same time as it faces broader scrutiny over its cybersecurity policies (Business Insider [2019]). This illustrates precisely the issues that lie at the heart of our paper.

Privacy and security breaches of this nature are subject to a growing framework of regulations. The UK General Data Protection Regulation (UK GDPR) sets out a number of principles for the processing of consumer data, which includes data sharing.[4] It also makes provisions for the protection of data, with substantial penalties for firms that fail to ensure adequate security.[5] These penalties may take the form of reimbursements to consumers or administrative fines (Articles 82 and 83 UK GDPR), which, in the context of our model, determine the liability rule according to which cyber-damages are divided between firms and consumers.

Separately, there have been a number of dedicated initiatives to promote cybersecurity. In the UK, measures that have been put in place to promote cyber-investment include a 2015 voucher scheme and the 2016 Early Stage Accelerator Programme (HM Government [2015, 2016]).

The US currently lacks an overarching federal privacy law and has relied instead on a system of private litigation and ex post enforcement

[3] Facebook's privacy policies have also been scrutinised in connection with data sharing deals with Amazon, Apple, Netflix and Spotify (New York Times [2018]), and in connection with the integration of social messaging applications (Financial Times [2019]).

[4] The UK GDPR is the retained EU law version of Regulation (EU) 2016/679 (the EU GDPR), which is incorporated into UK law through Section 3 of the European Union (Withdrawal) Act 2018, subject to the amendments in Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

[5] The sixth data protection principle requires data to be 'processed in a manner that ensures appropriate security'. Article 32 UK GDPR requires firms to 'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk'.

against deceptive or unfair practices under Section V of the Federal Trade Commission Act. In this regard the Federal Trade Commission, the de facto federal privacy regulator, has made clear that it sees the provision of appropriate data security as a required 'fair' trading practice (Raul and Mohan [2018]). At state-level, the California Consumer Privacy Act of 2018, which came into force in January 2020, is notable in terms of the move it represents towards a more European style, obligation-based system of privacy regulation.

This paper addresses the issues of data privacy and cybersecurity in a model comprising two firms, a data controller and a third party. The data controller provides a service to consumers who, besides incurring a direct cost, submit a volume of personal data in exchange for access to this service. This data may capture name, address, and other details required by the data controller, or information that is collected passively via browser cookies. The third party offers a separate service to consumers, the value of which is higher when it has access to the data collected by the data controller. The reasons for which this might occur include product customization and price targeting, for example (McKinsey and Company [2016]).

Consumers in this market are divided into two types: *sophisticated* and *naive*. While a sophisticated consumer takes firms' data sharing practices into account when deciding whether or not to submit personal information, a naive consumer disregards risks that stem from data sharing.[6] Data sharing implies risk due to the possibility of cyber-attacks. In particular, data sharing is assumed to facilitate cyber-attacks in the sense that, if data has been shared between firms, damages from a successful cyber-attack on the data controller spill over to the third party. The precise form of these cyber-intrusions is kept general in the model but may reflect impersonation, social engineering or ransomware attacks, among others.

The degree of risk faced by consumers and firms depends on the liability rule governing the allocation of cyber-damages. When the data controller is liable for its own cyber-damages, leaving consumers liable for damages at the third party, privately optimal security investments increase in response to data being shared (privacy being lowered), provided the damage of any individual cyber-attack is not too large. This ties back in to the question of how data sharing affects security investments, as in the Facebook and Zoom cases. This negative relationship between privacy and security is the net result of several effects that data sharing exerts on investment incentives. Firstly, holding the price fixed, demand falls when data is shared but also becomes more responsive to the chosen level of security due to the presence of sophisticated

[6] According to the Data & Marketing Association (DMA), for example, '[t]he proportion of UK society who show little or no concern with the issue of digital privacy or data exchange has increased from 16% of the population in 2012 to 25% [in 2017].' DMA [2018].

consumers. Secondly, there are indirect effects running through the firm's optimal price.

Our welfare benchmark is the second-best in which the social planner determines the welfare-maximising level of cybersecurity and the data sharing outcome but, unlike in the theoretical first-best, leaves prices to be determined by the market. This is the more relevant reference point for regulation, since we focus on UK GDPR style policies rather than direct controls over price that are more common in regulated natural monopolies.

We demonstrate that this second-best is also characterised by a negative relationship between privacy and security: security investments are higher when data is shared. Nonetheless, we identify important market failures in the sense that the firm under-invests in cybersecurity regardless of the data sharing outcome, and also over-shares data unless close to the entire consumer population is sophisticated. In all other cases, the firm exploits the inability of naive consumers to anticipate follow-on cyber-damages by over-sharing data relative to the social planner.

We study several regulatory interventions that may resolve these market failures. Firstly, we demonstrate that a minimum security standard can achieve the second-best in some settings, but in others fails to do so because the standard induces the firm to share data inefficiently. Secondly, we show that disclosure and consumer education policies, which increase the fraction of sophisticated consumers in the population, tend to reduce welfare unless they succeed in deterring the firm from sharing data. Moving to a setting in which the data controller is liable for all cyber-damages, irrespective of whether they arise at the controller or the third party,[7] similarly improves welfare only if it deters data sharing. Finally, allowing consumers to adopt strategies to mitigate the damage they suffer from cyber-attacks crowds out firms' security investments and may also lead to lower welfare in equilibrium.

These results suggest that a co-ordinated approach to regulation, which accounts for firms' interdependent data sharing and cybersecurity choices, is needed. Unilateral regulations that focus on only one dimension may not succeed in achieving the second-best and, in some cases, can even lower welfare. This result is also in the spirit of the recent calls for increased regulatory co-ordination made by the National Infrastructure Commission [2019] and the Competition and Markets Authority [2021] in the context of the newly-formed Digital Regulation Cooperation Forum.

The economic literature has so far considered data privacy and cybersecurity questions in isolation of one another. The issue of data privacy has been approached from different perspectives, of which the literature on information sharing between firms is most closely related to our paper

[7] In the recent settlement between Equifax and the Federal Trade Commission, for example, the firm agreed to take responsibility for checking that the third parties with which it shares data have adequate cyber-defences in place, see BBC [2019].

(see Acquisti *et al.* [2016] for a recent review). For instance, Taylor [2004] shows that firms prefer to disclose their customer lists to other firms when consumers are naive. Calzolari and Pavan [2006] study a more general common agency model with varying degrees of correlation between agents' product valuations. They characterise the conditions under which the transmission of information between firms can benefit or harm both firms and consumers.

There is also an emerging literature on information disclosure by consumers. For instance, Ichihashi [2020] shows that firms are made better off by committing not to use information for price discrimination in order to encourage consumers to disclose more information, but this commitment makes consumers worse off due to potential product mismatch.

In Argenziano and Bonatti [2021], a firm transacting with consumers in early periods can share the information it gathers about consumers with a firm that transacts in a later period. This information linkage between firms allows firms that transact later to adapt their price and quality level to a consumer's inferred willingness to pay. In this context, voluntary consent requirements are shown to increase consumer surplus, while other forms of privacy regulation have ambiguous welfare implications.

While much of the literature in this area similarly focuses on how information disclosure facilitates behavioural price discrimination (see Bergemann and Bonatti [2019] for a review), our paper is the first to address the interactions between data privacy and security. Our notion of privacy is very broad and relates to a firm's intentional choice to share data with a third party in order to realise a private gain, the nature of which is kept general.[8] Security, on the other hand, relates to the unintentional dissemination of information that occurs when hackers gain unlawful access to data. Since the liability for damages caused by a data breach is typically split between firms and consumers, firms share consumers' concern with preventing cyber-attacks.

On the cybersecurity side, the existing economic literature is sparse. Lam [2016] studies the investments made by a software developer into both ex ante attack prevention and ex post damage control, but does not consider data sharing incentives. She finds that the developer over-invests in damage control because they ignore the externalities that this imposes on consumers in the form of precautionary costs, but under-invests in attack prevention due to substitutability between investment types. Choi *et al.* [2010] study ex post incentives to disclose vulnerabilities. They show that, when the damage of cyber-attacks is large relative to the cost of installing updates, firms' private incentives to disclose vulnerabilities coincide with the social optimum.

[8] This is also in keeping with the UK Data Sharing Code of Practice, which defines *privacy information* as the 'information that organisations need to provide to individual data subjects about the collection and use [i.e. transfer] of their data'.

Another related paper is Jullien *et al.* [2020]. In this paper, firms choose a level of privacy 'precaution', which reflects the likelihood with which a consumer's data is sold to third parties in order to facilitate targeted advertising. Importantly, targeted advertising can result in negative experiences for consumers, for example as a result of cyber-intrusions made possible by access to their data. This notion of precaution therefore encompasses both data privacy and cybersecurity. The authors show that, while greater precaution protects consumers from malicious use being made of their data, it also limits their opportunities to learn about the risks of dealing with third parties and to enjoy beneficial matches with them.

The paper is organised as follows. Section II describes the model. Section III analyses the market equilibrium and Section IV the social planner's problem. Section V studies the welfare implications of a minimum standard on security, disclosure and consumer education policies, stricter liability rules, and consumer mitigation strategies. Section VI concludes. Supplementary calculations are contained in the Mathematica file that accompanies this paper online.

II. THE MODEL

Consider a model with two firms, a data controller and a third party. These firms serve a population of consumers of normalised size one. Consumers are divided into two types. A fraction θ are sophisticated while the remaining $1-\theta$ consumers are naive, $0 \leq \theta \leq 1$. As motivated in the Introduction, a given consumer's type will determine whether or not they are able to act rationally on information provided by firms about their data sharing activities (see further Section III).

The data controller provides a service to consumers of value u. Consumers are differentiated in terms of the value they attach to this service. In particular, we assume that u is distributed uniformly on $[0, 1]$ across consumers. In exchange for access to the data controller's service consumers submit a quantity of personal data and pay a price τ to the firm. This price may be interpreted as a monetary payment, such as subscription fees, or a non-monetary payment. The latter includes costs of data collection that are imposed on consumers, for example via advertising in the online platform context, that simultaneously generate revenues for the firm.

The third party provides a separate service to consumers, the value of which depends on whether or not it has access to the data collected by the data controller. We normalise the value of the third party service without data access to zero, which increases to $\Delta > 0$ when data is shared. We assume that this value is extracted entirely from consumers by the data controller via the third party. Finally, the cost of providing both services is normalised to zero.

II(i). *Cyber-Attacks and Cyber-Damages*

In this market, the data controller may be subject to a cyber-attack by computer hackers. Hackers successfully attack the data controller with probability $p(s)$, which is a function of the data controller's chosen level of cybersecurity $s \geq 0$. The cost to the data controller of achieving a given level of cybersecurity is denoted by $c(s)$. At a general level, we require these functions to satisfy

$$p'(s) < 0, \quad p''(s) \geq 0, \quad c'(s) > 0, \quad \text{and} \quad c''(s) > 0.$$

In order to derive closed-form solutions, the majority of our analysis will be based on the following specific functional forms for p and c (from now on, our 'example'):[9]

$$p(s) = 1 - s \quad \text{and} \quad c(s) = \frac{1}{2}s^2. \tag{1}$$

The damage suffered per consumer as a result of a successful cyber-breach at the data controller is equal to $\eta > 0$. If data has been shared with the third party, we suppose that a cyber-attack on the data controller leads to a follow-on attack at the third party, the damage of which cannot, however, exceed that of the initial attack. That is, conditional on data having been shared, a successful cyber-attack on the data controller leads to follow-on damages equal to $\phi\eta$ at the third party, $0 < \phi < 1$. Note that we may also, therefore, interpret ϕ as the probability of a follow-on attack in this setting.

In our baseline model, the data controller is liable for damages resulting from a cyber-attack on itself, while consumers are liable for damages resulting from any follow-on attack on the third party. This is consistent with Anderson and Murdoch [2010], for example, who show that banks may set terms that shift liability to customers in the case of credit cards. The difficulty of holding firms liable for cybersecurity failures in practice is also highlighted by invoice hijacking cases in the art sector, for example, in which courts have declined to hold vendors liable for damages resulting from diverted payments (see, e.g. Farrer and Co. [2020]). Equilibrium behaviour in this liability for partial damages setting is studied in Section III below.

It will be convenient for the analysis that follows to denote total cyber-damages, conditional on a successful hack on the data controller, by

$$\hat{\eta} := \eta(1 + \phi), \tag{2}$$

and also to introduce the following, related variable:

$$\hat{\hat{\eta}} := \eta(1 + \theta\phi) \leq \hat{\eta}. \tag{3}$$

[9] Attack probability functions that are linear in vulnerability are standard in the information security literature, see Gordon and Loeb [2002] and related work.

In order to ensure that our solutions are interior throughout, we assume that $0 < \hat{\eta} < 1$. This also implies that $\hat{\hat{\eta}} < 1$ and requires us to restrict the domain of η, for general $\phi \in (0,1)$, to the interval $\left(0, \frac{1}{2}\right]$. Note that η being small enough also ensures equilibrium existence in every case considered in this paper. Finally, we also assume that Δ cannot be too large. This condition on Δ is made precise in Appendix A.

In what follows, we will differentiate between outcomes according to whether or not data is shared between firms. In terms of notation, the value of a given variable z when data is shared will be denoted by z^Y, while z^N denotes the value of the same variable when data is not shared.

III. EQUILIBRIUM: LIABILITY FOR PARTIAL DAMAGES

The timing of the game is the following. First, the data controller simultaneously invests in security s, sets the price τ, and announces the data sharing policy it will pursue (sharing vs. no sharing) once consumers submit their data. Second, consumers decide whether to submit their data and, conditional on data being submitted, the data controller implements its data sharing policy. Data sharing decisions announced by the data controller in stage 1 are assumed to be binding at stage 2.[10]

Conditional on data not being shared, the data controller faces the following profit maximisation problem:

$$\max_{\tau^N, s^N} \pi^N = \left[\tau^N - p\left(s^N\right)\eta\right]\left(1 - \tau^N\right) - c\left(s^N\right). \tag{4}$$

In this expression, the term in square brackets reflects net revenue per consumer, while $1 - \tau^N$ captures consumer demand.

Taking derivatives with respect to the choice variables τ^N and s^N yields, respectively, the following first-order conditions:

$$\tau^N = \frac{1}{2}\left[1 + p\left(s^N\right)\eta\right] \tag{5}$$

and

$$\frac{\partial \pi^N}{\partial s^N} = -p'(s^N)\eta(1 - \tau^N) - c'(s^N) = 0. \tag{6}$$

[10] This holds in the presence of a supervisory authority that fines firms for misleading consumers, for example. Under Article 83(5) UK GDPR, firms that fail to notify data subjects of how their data will be shared can be fined up to £17.5 million or 4% of worldwide turnover.

Recalling that a fraction θ of consumers are sophisticated, the data controller's profit maximisation problem, conditional on data being shared, is

$$\begin{aligned}\max_{\tau^Y, s^Y} \pi^Y = \theta \left[\tau^Y - p\left(s^Y\right)\eta + \Delta\right]\left[1 - \tau^Y - p\left(s^Y\right)\phi\,\eta\right] \\ + (1-\theta)\left[\tau^Y - p\left(s^Y\right)\eta + \Delta\right](1-\tau^Y) - c\left(s^Y\right).\end{aligned} \tag{7}$$

The first line of this expression captures net revenues earned from sophisticated consumers. These consumers anticipate the risk of cyber-damages arising from attacks on the third party, and therefore submit data to the data controller only when their valuation is sufficiently high to offset not just the purchase price, but also this risk, that is when $u \geq \tau^Y + p\left(s^Y\right)\phi\eta$. Naive consumers, captured in the second line of (7), do not adjust their demand in response to this risk.

In this case, the first-order conditions with respect to τ^Y and s^Y result, respectively, in

$$\tau^Y = \frac{1}{2}\left[1 - \Delta + p\left(s^Y\right)\eta(1-\theta\phi)\right] \tag{8}$$

and

$$\begin{aligned}\frac{\partial \pi^Y}{\partial s^Y} = \underbrace{-p'(s^Y)\eta\left[1 - \tau^Y - p(s^Y)\theta\phi\eta\right]}_{\text{total demand effect}} \\ \underbrace{-p'(s^Y)\theta\phi\eta\left[\tau^Y - p(s^Y)\eta + \Delta\right]}_{\text{demand responsiveness effect}} - c'(s^Y) = 0.\end{aligned} \tag{9}$$

Increasing cybersecurity investments reduces the data controller's expected liability in proportion to the level of demand, see the terms in the first line of (9), while simultaneously provoking a demand response, the first terms on the second line.

To facilitate further comparison, consider our example in (1). In this setting, the data controller's chosen level of cybersecurity and the associated equilibrium profits, conditional on data not being shared, are equal to

$$s^{N*} = \frac{\eta(1-\eta)}{2-\eta^2}, \tag{10}$$

and

$$\pi^{N*} = \frac{(1-\eta)^2}{2(2-\eta^2)}. \tag{11}$$

Recalling the definition of $\hat{\hat{\eta}}$ from (3), the same variables in the case where data is shared are equal to

$$s^{Y*} = \frac{\hat{\hat{\eta}}(1 + \Delta - \hat{\hat{\eta}})}{2 - \hat{\hat{\eta}}^2} \tag{12}$$

and

$$\pi^{Y*} = \frac{\left(1 + \Delta - \hat{\hat{\eta}}\right)^2}{2\left(2 - \hat{\hat{\eta}}^2\right)}. \tag{13}$$

The following result describes the effect that data sharing has on cybersecurity investments when the data controller is liable for partial damages.

Proposition 1. Given liability for partial cyber-damages, privacy and security are negatively related in the market equilibrium, $s^{Y*} > s^{N*}$, if

$$\eta \leq \frac{1}{2}\left(3 - \sqrt{5}\right) \approx 0.38. \tag{14}$$

Proof. Algebraic comparison of (10) and (12) reveals that $\eta \leq \frac{1}{2}(3 - \sqrt{5})$ is sufficient for a negative relationship. A positive relationship, that is $s^{Y*} < s^{N*}$, arises if and only if $\eta > \frac{1}{2}(3 - \sqrt{5})$, $\theta\phi > \frac{2-\eta(4-\eta)}{\eta(2-\eta)}$ and $\Delta \leq \frac{\phi[2\eta(2+\phi)-2-\eta^2(1+\phi)]}{(2-\eta^2)(1+\phi)}$. See Supplementary Calculations. ■

Comparing (6) and (9) for given τ and s reveals contrasting effects of data sharing on investment incentives. On the one hand, the presence of sophisticated consumers reduces demand when data is shared, which lowers investment incentives through the total demand effect. On the other hand, demand under data sharing becomes responsive to the level of security investment, which increases the incentive to invest relative to the no sharing case—the demand responsiveness effect. A comparison of (5) and (8) for given s reveals an additional, indirect effect: the price τ tends to be lower under data sharing. This boosts total demand but weakens the demand responsiveness effect.

The overall relationship between privacy and security rests on the relative magnitudes of these effects. Omitting second-order terms, the demand responsiveness effect is positive in terms of its impact on investment levels and proportional to η. Moreover, a lower price boosts security investment incentives, as $\frac{\partial}{\partial \tau^Y}\left(\frac{\partial \pi^Y}{\partial s^Y}\right) < 0$. The difference in the total demand effects, while tending to reduce investment levels under data sharing relative to no sharing, is only second-order since it is proportional to η^2. Provided that η is not too large, the firm must therefore invest more in security when data is shared.

Empirical research has shown that small and medium-sized data breaches account for the majority of cases by far (Mann [2015]). While very large cyber-attacks do occur, they are, by contrast, extremely rare and sector-specific. In light of this, it follows that Proposition 1 highlights the most economically relevant parameter range for η. The analysis that follows will therefore assume that η is not too large, such that (14) holds.

Assumption 1. $\eta \leq \frac{1}{2}\left(3-\sqrt{5}\right)$.

The following result considers the impact that consumer sophistication θ has on equilibrium outcomes when data is shared.

Lemma 1. Conditional on data being shared, an increase in the proportion of sophisticated consumers increases equilibrium cybersecurity levels, that is $\frac{\partial s^{Y*}}{\partial \theta} > 0$, if and only if

$$\Delta > \overline{\Delta}_I := \frac{\hat{\eta}(4-\hat{\eta})-2}{2+\hat{\eta}^2},$$

but necessarily decreases equilibrium profits, $\frac{\partial \pi^{Y*}}{\partial \theta} < 0$.

Proof. Characterising s^{Y*} in terms of $\hat{\eta}$ as in (12), the effect of θ acts entirely through $\hat{\eta}$. In other words, $\operatorname{sgn}\left[\partial s^{Y*}/\partial\theta\right] = \operatorname{sgn}\left[\partial s^{Y*}/\partial\hat{\eta}\right]$. Noting that $\frac{\partial s^{Y*}}{\partial \hat{\eta}} = \frac{2(1+\Delta)-\hat{\eta}\left[4-\hat{\eta}(1+\Delta)\right]}{(2-\hat{\eta}^2)^2}$ proves the first part of the result. As for the second part, by the Envelope Theorem we have $\frac{d\pi^{Y*}}{d\theta} = \frac{\partial \pi^{Y*}}{\partial \theta} = -[\tau^{Y*} - p(s^{Y*})\eta + \Delta]p(s^{Y*})\phi\eta < 0$, and where the square-bracketed term represents equilibrium net revenue per user, see (7). ■

We can see from (9) that higher θ weakens the total demand effect but strengthens the demand responsiveness effect in the first-order condition characterising the controller's optimal security investment. Moreover, the marginal impact of θ on the strength of the demand responsiveness effect is increasing in Δ. Thus, when Δ is large enough, the impact of θ on the demand responsiveness effect dominates and s^{Y*} increases with θ.

By the Envelope Theorem, profits necessarily fall as the fraction of sophisticated consumers rises. This is because total demand falls as θ increases.

Finally, we may characterise the data controller's data sharing decision as follows.

Proposition 2. Given liability for partial cyber-damages, the data controller shares data with the third party whenever $\Delta > \overline{\Delta}_\pi$, where

$$\overline{\Delta}_{\pi} := -(1-\hat{\eta}) + (1-\eta)\sqrt{\frac{2-\hat{\eta}^2}{2-\eta^2}} > 0 \tag{15}$$

is increasing in θ.

Proof. The sharing threshold is derived from an algebraic comparison of (11) and (13), details of which are contained in the Supplementary Calculations. By inspection of (15), we see that $\operatorname{sgn}\left[\partial\overline{\Delta}_{\pi}/\partial\theta\right] = \operatorname{sgn}\left[\partial\overline{\Delta}_{\pi}/\partial\hat{\eta}\right]$. Since

$$\frac{\partial\overline{\Delta}_{\pi}}{\partial\hat{\eta}} = 1 - \frac{\hat{\eta}(1-\eta)}{\sqrt{(2-\hat{\eta}^2)(2-\eta^2)}} > 0, \tag{16}$$

$\overline{\Delta}_{\pi}$ is increasing in θ. ■

A higher fraction of sophisticated consumers in the population therefore reduces the likelihood that firms will share data. This result follows directly from Lemma 1, which states that increases in θ necessarily reduce the firm's profits under data sharing, and the fact that θ has no effect on the firm's profits when data is not shared, see (4).

IV. SOCIAL PLANNER'S PROBLEM

The theoretical first-best in this market is achieved by a social planner who controls (a) which consumers submit data to the data controller, (b) whether or not this data is shared between firms and (c) the level of cybersecurity. It is possible to show that this first-best is only achievable in practice if the regulator controls not only the firm's investment and data sharing decisions, but also the price τ. Details of this analysis are provided in Appendix B.

Absent price regulation, the relevant welfare benchmark is the second-best, in which the social planner takes the firm's pricing behaviour in (5) and (8) as given. As our focus is on UK GDPR style regulation of privacy and security rather than price controls that are more commonly observed in regulated natural monopolies, our regulatory analysis that follows will build on a comparison of the market equilibrium to this second-best outcome.

In the absence of data sharing, the planner therefore chooses the security investment level s^N to maximise

$$W^N = \int_{\tau^N}^{1} \left[u - p\left(s^N\right)\eta\right] \mathrm{d}u - c\left(s^N\right),$$

$$\text{s.t. } \tau^N = \frac{1}{2}\left[1 + p\left(s^N\right)\eta\right]. \tag{17}$$

On the basis of (1), this leads to the following second-best investment levels when data is not shared:

$$\tilde{s}^N = \frac{3\eta(1-\eta)}{4-3\eta^2}. \tag{18}$$

When data is shared, the social planner chooses the investment level s^Y to maximise

$$\begin{aligned} W^Y = \theta \int_{\tau^Y + p(s^Y)\eta\phi}^{1} \left[u + \Delta - p\left(s^Y\right)\hat{\eta}\right] \mathrm{d}u \\ + (1-\theta) \int_{\tau^Y}^{1} \left[u + \Delta - p\left(s^Y\right)\hat{\eta}\right] \mathrm{d}u - c\left(s^Y\right), \end{aligned}$$

$$\text{s.t. } \tau^Y = \frac{1}{2}\left[1 - \Delta + p\left(s^Y\right)\eta(1-\theta\phi)\right]. \tag{19}$$

This leads to the following second-best security investment when data is shared:

$$\tilde{s}^Y = \frac{\eta\left[3(1+\Delta-\eta) + (1+\Delta-2\eta)(2+\theta)\phi - 3\eta\phi^2\theta^2\right]}{4-\eta^2\left[3+\phi\left(4+\theta(2+3\phi\theta)\right)\right]}. \tag{20}$$

Algebraic comparison of (18) and (20) leads to the following result.

Proposition 3. Data privacy and cybersecurity are negatively related in the second-best, $\tilde{s}^Y > \tilde{s}^N$.

Proof. See Supplementary Calculations. ■

Data sharing exposes consumers to additional cyber-damages at the third party. The marginal social benefit of security investments is consequently higher when data is shared, resulting in a higher second-best level of security.

By comparing the second-best welfare levels arising under the investments in (18) and (20), we may also characterise the condition in terms of Δ that determines when the planner chooses data sharing.

Proposition 4. Data sharing increases social welfare if and only if $\Delta > \overline{\Delta}_W > 0$, and where $\overline{\Delta}_W$ is increasing in θ.

Proof. See Appendix C. ■

The precise expression for the data sharing threshold $\overline{\Delta}_W$ is provided in Appendix C. In order for data sharing to be preferred, the benefits must be sufficiently large to offset the increased cyber-risks and the costly cybersecurity investments that go along with such a policy.

Moreover, the presence of sophisticated consumers makes data sharing less desirable from a welfare perspective. Conditional on data being shared, an increase in sophisticated consumers reduces demand directly, but tends to increase demand indirectly via a lower price. Since the price adjustment does not fully compensate the increase in security risks, and in contrast to the outcome in the theoretical first-best where welfare under data sharing is independent of θ (see Appendix B), the former effect dominates here. As in the market equilibrium, the presence of sophisticated consumers therefore reduces the social planner's incentive to share data.

IV(i). *Comparison with the Market Equilibrium*

We first consider how the firm's cybersecurity investment decisions compare to the second-best. The following result shows that, for a given data sharing outcome, an individual consumer is left at excessive risk of cyber-attack.

Proposition 5. The data controller under-invests in cybersecurity relative to the second-best, $s^{N*} < \tilde{s}^N$ and $s^{Y*} < \tilde{s}^Y$.

Proof. See Supplementary Calculations. ■

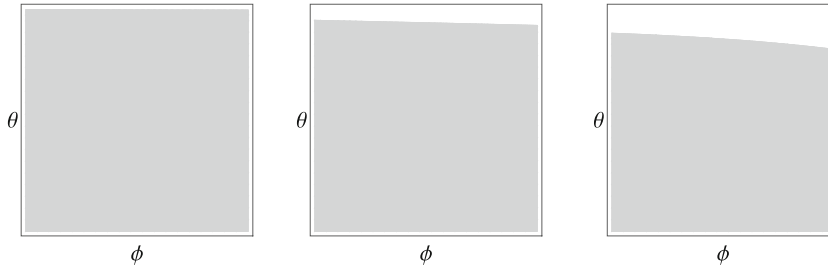
Compared to the firm, the social planner prefers to increase security investments in order to reduce the price and boost demand. Together with the fact that, when data is shared, the data controller is liable for only a portion of cyber-damages, this reduces privately-optimal incentives to invest in security below second-best levels.

Turning to the firm's data sharing decisions, the following result shows that the market equilibrium with liability for partial cyber-damages may be characterised by excessive or insufficient data privacy.

Proposition 6. Given liability for partial cyber-damages, the data controller may over- or under-share data relative to the second-best.

Proof. We provide numerical examples to prove that each case may arise. Given (15) and the expression for $\overline{\Delta}_W$ in Appendix C, when $\eta = \frac{1}{3}$, $\phi = \frac{2}{3}$ and $\theta = \frac{1}{10}$ we have over-sharing in the sense that $\overline{\Delta}_\pi = 0.02 < 0.13 = \overline{\Delta}_W$. Conversely, when $\eta = \frac{1}{3}$, $\phi = \frac{2}{3}$ and $\theta = \frac{99}{100}$, we have under-sharing because $\overline{\Delta}_\pi = 0.18 > 0.17 = \overline{\Delta}_W$. ■

The likelihood of over- and under-sharing is examined graphically in Figure 1. Over-sharing occurs whenever $\overline{\Delta}_\pi < \overline{\Delta}_W$, which is identified below by the shaded region. Two observations may be made about Figure 1. Firstly, over-sharing is less likely when the level of consumer sophistication is high. Although a higher θ discourages both the firm and the planner from sharing,



(a) $\eta = 0.01$ (b) $\eta = 0.15$ (c) $\eta = 0.35$

Figure 1
Over-Sharing Region for $\phi, \theta \in [0, 1]$

the effect on the firm is more pronounced. This is because naive consumers do not take the damages arising from follow-on attacks into account. The firm therefore exploits the presence of naive consumers by over-sharing data relative to the planner, who takes all cyber-risks into account.

Secondly, increasing η makes over-sharing less likely. The reason is that, although the firm is liable for only partial cyber-damages, the extent of its liability is increasing in η, which reduces its incentive to over-share.

V. REGULATION

Proposition 1 highlights the interdependence between firms' data privacy and cybersecurity strategies. Moreover, we have identified important market failures in both areas in the sense that firms under-invest in cybersecurity, Proposition 5, and choose levels of privacy that may exceed or fall short of socially desirable levels, Proposition 6. This section focuses on the appropriate regulatory responses to these market failures. In order to limit the number of cases for analysis, we will focus on the economically most relevant scenario, which is characterised by Assumption 1.

V(i). *Minimum Standard on Security*

Consider first a minimum standard on security when the data controller is liable for partial cyber-damages. This standard stipulates a minimum level of security $\hat{s}$ that the data controller must achieve, irrespective of whether data is shared or not. In the UK, for example, Cyber Essentials certification is a requirement for firms wishing to bid for Government contracts that involve sensitive data. Many tenders in the area of Defence, moreover, require the more comprehensive Cyber Essentials Plus standard to be met.

A first important question concerns the unintended side-effects that such a policy may have on data privacy. Letting $\overline{\delta}_{\pi}(\hat{s})$ denote the sharing threshold

in the presence of a minimum standard $\hat{s}$, such that the data controller shares data if and only if $\Delta > \overline{\delta}_{\pi}(\hat{s})$, we have the following result.

Proposition 7. $\overline{\delta}_{\pi}(\hat{s})$ is a continuous and weakly decreasing function of $\hat{s}$.

Proof. We divide the proof into three cases.

Case (i): $\hat{s} \leq s^{N*}$. Given that $s^{Y*} > s^{N*}$, the security standard has no impact on the market equilibrium. In this case, the sharing threshold in terms of Δ is given by $\overline{\Delta}_{\pi}$ in (15), which is independent of $\hat{s}$.

Case (ii): $\hat{s} \in (s^{N*}, s^{Y*}]$. Now the security standard has no effect on the firm's investment when it shares data. However, conditional on not sharing data, the standard forces the firm to invest more in security than it would otherwise have done. This lowers the no-sharing profit to

$$\pi^{N}(\hat{s}) = \frac{1}{4}\left[1 - p(\hat{s})\eta\right]^2 - c(\hat{s}), \tag{21}$$

which is independent of Δ but decreasing in $\hat{s}$ for all $\hat{s} > s^{N*}$. The data controller's profit when it shares data is given by (13), which is independent of $\hat{s}$ but increasing in Δ. It follows that the firm will now share data if and only if $\Delta > \overline{\Delta}_{\pi}'(\hat{s})$, and where this new sharing threshold is implicitly defined by the condition that

$$\pi^{Y*}\left(\overline{\Delta}_{\pi}'(\hat{s})\right) = \pi^{N}(\hat{s}).$$

Given that π^{Y*} is increasing in Δ, it follows immediately that $\overline{\Delta}_{\pi}'(\hat{s})$ is decreasing in $\hat{s}$ for $\hat{s} \in (s^{N*}, s^{Y*}]$. Moreover, $\overline{\Delta}_{\pi}'(\hat{s}) \to \overline{\Delta}_{\pi}$ as $\hat{s} \to s^{N*}$.

Case (iii): $\hat{s} > s^{Y*}$. Now the firm must increase its investment up to the minimum standard, regardless of its sharing decision. In the absence of data sharing, profits are given by (21). When data is shared, profits are equal to

$$\pi^{Y}(\hat{s}) = \frac{1}{4}\left[1 + \Delta - p(\hat{s})\eta(1 + \theta\phi)\right]^2 - c(\hat{s}), \tag{22}$$

which is decreasing in $\hat{s}$ for all $\hat{s} > s^{Y*}$. Comparing (21) and (22), the controller shares data if and only if $\Delta > \overline{\Delta}_{\pi}''(\hat{s}) := p(\hat{s})\eta\theta\phi$, which is clearly decreasing in $\hat{s}$. Again, $\overline{\Delta}_{\pi}''(\hat{s}) \to \overline{\Delta}_{\pi}'(\hat{s})$ as $\hat{s} \to s^{Y*}$. ■

Summarising the preceding analysis, we may write the sharing threshold $\overline{\delta}_{\pi}(\hat{s})$ that applies in the presence of a minimum security standard as follows:

$$\overline{\delta}_{\pi}(\hat{s}) = \begin{cases} \overline{\Delta}_{\pi} & \text{if } \hat{s} \leq s^{N*}, \\ \overline{\Delta}_{\pi}'(\hat{s}) & \text{if } \hat{s} \in (s^{N*}, s^{Y*}], \\ \overline{\Delta}_{\pi}''(\hat{s}) & \text{if } \hat{s} > s^{Y*}, \end{cases} \tag{23}$$

where $\overline{\Delta}_{\pi}$ is given in (15) and where both $\overline{\Delta}_{\pi}'(\hat{s})$ and $\overline{\Delta}_{\pi}''(\hat{s})$ are strictly decreasing in $\hat{s}$. This again demonstrates the interdependence between privacy and security. While a higher standard can improve cybersecurity, it can also exacerbate the privacy problem when the firm over-shares data.

To further explore this interdependence, we consider the welfare implications of the minimum security standard. Given the under-investment result in Proposition 5, it is clear that the marginal welfare impact of increasing $\hat{s}$ from the private optimum towards the second-best investment level is positive, provided the firm's data sharing decision remains unchanged.

Corollary 1, below, shows that the minimum security standard can achieve the second-best outcome in some cases when the firm over-shares data. Excessive data sharing is consistent with low levels of η and, for any level of η, a non-negligible degree of consumer naivety concerning data risks, see Figure 1. In terms of the latter, Deloitte [2020] found that the proportion of UK consumers who were 'very concerned' about the use of their data halved from 47% in 2018 to 24% in 2020.

Corollary 1. If:

(a) $\underline{\Delta}_{\pi} < \overline{\Delta}_{W} \leq \Delta$, the second-best is achieved by setting $\hat{s} = \tilde{s}^{Y}(\Delta)$,
(b) $\underline{\Delta}_{\pi} < \Delta \leq \overline{\Delta}_{W}$, the welfare under regulation is maximised by setting $\hat{s} = \tilde{s}^{Y}(\Delta)$ but the resulting welfare is lower than the second-best level,
(c) $\overline{\delta}_{\pi}(\tilde{s}^{N}) < \Delta \leq \overline{\Delta}_{\pi}$, the welfare under regulation is maximised by setting $\hat{s} > s^{N*}$ but the resulting welfare is lower than the second-best level,
(d) $\Delta \leq \overline{\delta}_{\pi}(\tilde{s}^{N})$ the second-best is achieved by setting $\hat{s} = \tilde{s}^{N}$.

The various possible outcomes follow directly from the properties of the sharing threshold in the presence of the minimum security standard. In particular, if, as in case (a), $\Delta > \overline{\Delta}_{W} > \overline{\Delta}_{\pi}$, the firm shares data regardless of the level of $\hat{s}$. Therefore the second-best is attainable by setting $\hat{s} = \tilde{s}^{Y}(\Delta)$, and where $\tilde{s}^{Y}(\Delta)$ is given in (20).

Similarly, in case (d), Δ is low enough for the second-best to be achieved by setting setting $\hat{s} = \tilde{s}^{N}$, see (18), at which level the firm, like the planner, chooses not to share data.

If $\overline{\Delta}_{\pi} < \Delta \leq \overline{\Delta}_{W}$, as in case (b), the welfare under regulation is maximised by setting $\hat{s} = \tilde{s}^{Y}(\Delta)$, although this does not achieve the second-best because the firm, unlike the planner, decides to share data.

Case (c) is an interesting case. The firm chooses not to share data at the privately-optimal security level s^{N*} and, holding fixed this data sharing choice,

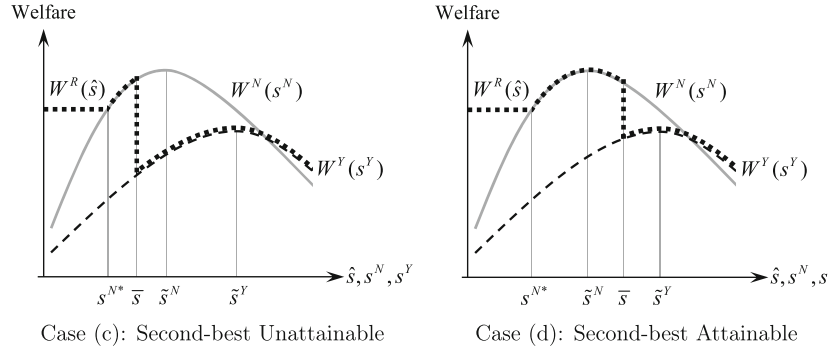


Figure 2
Welfare Effects of a Minimum Security Standard

welfare is improved by setting $\hat{s}$ above s^{N*}. However, increasing $\hat{s}$ now causes the firm to share data inefficiently. To see this, recall that $\tilde{s}^N > s^{N*}$ (Proposition 5). Given that $\overline{\delta}_\pi(\hat{s})$ is strictly decreasing in $\hat{s}$ for $\hat{s} > s^{N*}$, there exists an $\overline{s} \in (s^{N*}, \tilde{s}^N)$ such that $\overline{\delta}_\pi(\overline{s}) = \Delta$, and the firm shares data for all $\hat{s} > \overline{s}$. The second-best is unattainable in this case because the firm begins to share data before $\hat{s}$ reaches $\tilde{s}^N$.[11]

We contrast cases (c) and (d) graphically in Figure 2. This Figure depicts welfare under no sharing (the grey solid line), welfare under data sharing (the dashed black line) and welfare under regulation as a function of the security standard, which we denote by $W^R(\hat{s})$ (the bold dotted line). In the left panel, we have $\overline{s} < \tilde{s}^N$ and the second-best is unattainable due to inefficient data sharing. This represents case (c) of Corollary 1. In the right panel, $\overline{s} > \tilde{s}^N$ so that the second-best can be achieved by setting $\hat{s} = \tilde{s}^N$. This reflects the scenario in case (d) of Corollary 1.

In conclusion, a minimum security standard has unambiguously positive welfare implications if we hold constant the data sharing decision because it can correct the firm's tendency to under-invest. When the data sharing benefit is either very large or very small, this allows the second-best to be achieved. For intermediate values of Δ, the second-best is unattainable due to inefficient data sharing that is induced by the standard itself.

V(ii). *Disclosure and Consumer Education*

In this section, we explore the effectiveness of consumer policies in resolving privacy- and security-related market failures. By consumer policies we mean

[11] The participation constraints of the firm under security standard regulation for cases (a)–(d) are satisfied. See Supplementary Calculations.

measures that oblige the firm to increase its disclosure of specific data-related risks to its customers, as under the UK GDPR, or policies that educate consumers generally about cybersecurity, for example the 'International Computer Security Day' or the US 'National Cyber Security Awareness Month'. Increasing consumer awareness about their personal data is also a central recommendation of the Communications Consumer Panel [2011], for example.

These policies will not alter the behaviour of sophisticated consumers in our model, who already base their decisions on a correct assessment of all benefits and risks associated with submitting their personal data to the firm. However, they cause more consumers who would otherwise have remained naive to take data-risks into account. We may therefore capture disclosure and consumer education policies generally in our model by associating them with an increase in the consumer sophistication parameter θ.

This increase in θ entails a direct consumer benefit in terms of preventing the over-provision of data by naive customers, whose decision to submit data would otherwise have neglected important data risks. Nevertheless, this increase in consumer sophistication also affects the firm's data sharing decision, as shown in Proposition 2. As demonstrated below, consumer policies also exert a non-monotonic effect on the firm's security investment.

Proposition 8. Letting $\overline{\Delta}_\pi(\theta)$ denote the firm's sharing threshold as a function of θ, increasing θ:

(a) first increases then decreases investment if $0 = \overline{\Delta}_\pi(0) < \Delta \leq \overline{\Delta}_\pi(1)$;
(b) increases security investment if $\Delta > \overline{\Delta}_\pi(1)$.

Proof. From Proposition 2, the firm shares data whenever

$$\Delta > \overline{\Delta}_\pi = -(1-\hat{\eta}) + (1-\eta)\sqrt{\frac{2-\hat{\eta}^2}{2-\eta^2}},$$

which depends on θ via $\hat{\eta} = \eta(1+\theta\phi)$. From Lemma 1, the firm's security investment under data sharing increases with θ whenever

$$\Delta > \overline{\Delta}_I = \frac{\hat{\eta}(4-\hat{\eta})-2}{2+\hat{\eta}^2}.$$

We can show that $\overline{\Delta}_\pi \geq \overline{\Delta}_I$ for all θ, which is equivalent to

$$\frac{1-\eta}{\sqrt{2-\eta^2}} \geq \frac{\hat{\eta}}{2+\hat{\eta}^2}\sqrt{2-\hat{\eta}^2}.$$

The right-hand side is smaller than $\frac{1}{3}\sqrt{2-\eta^2}$, which follows from $\hat{\hat{\eta}} < 1$ and $\hat{\hat{\eta}} \geq \eta$. Hence, a sufficient condition for the above inequality to hold is

$$\frac{1-\eta}{2-\eta^2} \geq \frac{1}{3},$$

which is always satisfied for $\eta \leq \frac{1}{2}\left(3-\sqrt{5}\right)$. Therefore, whenever the firm is choosing to share data, its security investment is increasing in θ.

Recall from Proposition 2 that the sharing threshold $\overline{\Delta}_\pi$ is itself increasing in θ, and note that, when $\theta = 0$, we have $\overline{\Delta}_\pi = 0$.

In case (a), the firm chooses to share data for low levels of θ but switches to no sharing for θ sufficiently close to 1. For the interval of θ for which the firm is sharing data, security investments are increasing by the above arguments. However, as soon as θ causes the sharing threshold $\overline{\Delta}_\pi$ to exceed Δ, the firm's investment falls to $s^{N*} < s^{Y*}$, and where s^{N*} is independent of θ given (10).

In case (b), the firm shares data for any level of θ. Therefore, as θ increases, the firm invests more in security. ■

We again observe the interdependence between privacy and security: informing consumers about risks associated with data sharing mitigates any tendency on the part of the firm to over-share data, Proposition 2, but, according to the above result, may also imply a drop in security levels.

The issue is complicated by the fact that the social planner's investment decision under data sharing and their decision to share data similarly depend on θ, see (20) and Proposition 4. Since Proposition 5 shows that we have under-investment for all possible parameter values, it is clear that consumer policies can never achieve the second-best, however.

Nevertheless, it is important to consider the impact that consumer policies have on welfare in the market equilibrium, that is when investments are chosen by the firm. Letting $W^{Y*}(\theta)$ denote the equilibrium welfare level according to (19) when data is shared, and W^{N*} equilibrium welfare according to (17) when data is not shared, Figure 3 shows that the welfare effect of increasing θ depends crucially on the firm's data sharing choices.

Interestingly, panel (a) shows that equilibrium welfare is falling in θ when the firm's decision to share data remains unchanged. This is because consumers stop contributing data as they become aware of the risk of follow-on attacks, and this tendency for demand to drop is not fully offset by an increase in security investment. Panel (b) shows that, while welfare is again decreasing in θ when the firm shares data, welfare can jump upwards when higher θ causes the firm to stop sharing data. This is the case because deterring data sharing eliminates the risk of follow-on attacks.

In summary, the welfare-desirability of consumer policies rests crucially on their ability to affect the firm's data sharing decision.

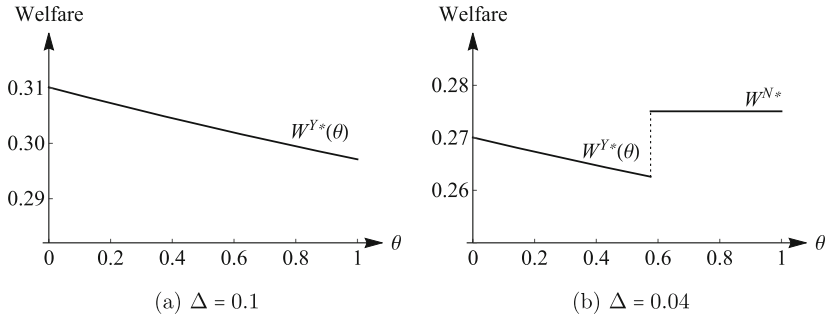


Figure 3
Effect of θ on Welfare ($\eta = 0.15$, $\phi = 0.5$)

V(iii). *Liability for Full Damages*

Another potential means of correcting the data controller's tendency to under-invest in cybersecurity is to impose a stricter liability rule. We therefore reconsider the market equilibrium when the data controller is liable for cyber-damages suffered not only by its own customers, but also by those of the third party. In practical terms, this ties in with Section 75 of the UK Consumer Credit Act 1974, for example, which makes the credit card company or trader fully liable for any misrepresentation or breach of contract. Similarly, the UK Network and Information Systems Regulations 2018 make operators of essential services responsible for security, even where delivery of a service has been delegated to a third party. As noted in Section II, however, there may be practical difficulties with enforcing such liability rules in the courts.

Conditional on data not being shared, both the social planner's problem and the market problem are unaffected by this change in the liability rule since, in the absence of data sharing, the question of who bears liability for cyber-attacks at the third party does not arise. The difference arises in the market problem and second-best welfare benchmark when data is shared.

Conditional on data being shared, the data controller's problem under full liability is

$$\max_{\tau^{YF}, s^{YF}} \pi^{YF} = \left[\tau^{YF} + \Delta - p(s^{YF})\hat{\eta}\right](1 - \tau^{YF}) - c(s^{YF}),$$

which leads to the following first-order conditions:

$$\tau^{YF} = \frac{1}{2}\left[1 - \Delta + p(s^{YF})\hat{\eta}\right] \tag{24}$$

and

$$\frac{\partial \pi^{YF}}{\partial s^{YF}} = -p'(s^{YF})\hat{\eta}(1-\tau^{YF}) - c'(s^{YF}) = 0. \tag{25}$$

Using (1), the equilibrium under data sharing is now

$$s^{YF*} = \frac{\hat{\eta}(1+\Delta-\hat{\eta})}{2-\hat{\eta}^2}, \tag{26}$$

and

$$\pi^{YF*} = \frac{(1+\Delta-\hat{\eta})^2}{2(2-\hat{\eta}^2)}. \tag{27}$$

By comparison with (12) and (13), equilibrium security investments and profits under full liability are equal to those under liability for partial damages when $\theta = 1$. Just as sophisticated consumers adjust their demand in response to the risks of follow-on attacks when they bear liability for the associated damages, so the data controller now internalises these risks when it is fully liable. It does so by investing more in security and by charging a higher price than it does under partial liability, compare (8) and (24).

In the social planner's problem, welfare given data sharing must be amended to reflect the fact that (a) follow-on cyber-damages no longer affect the demand of sophisticated consumers and (b) prices are now set according to (24). This implies that the social planner maximises

$$\begin{aligned} W^{YF} &= \int_{\tau^{YF}}^{1} \left[u + \Delta - p(s^{YF})\hat{\eta}\right] \mathrm{d}u - c(s^{YF}) \\ \text{s.t. } \tau^{YF} &= \frac{1}{2}\left[1 - \Delta + p(s^{YF})\hat{\eta}\right], \end{aligned} \tag{28}$$

which leads to the following second-best investment levels and welfare when data is shared:

$$\tilde{s}^{YF} = \frac{3\hat{\eta}(1+\Delta-\hat{\eta})}{4-3\hat{\eta}^2} \tag{29}$$

and

$$\tilde{W}^{YF} = \frac{3(1+\Delta-\hat{\eta})^2}{8-6\hat{\eta}^2}. \tag{30}$$

The following result compares market outcomes under full liability to the second-best.

Proposition 9. Given liability for full cyber-damages, the data controller under-invests in cybersecurity, conditional on data being shared, and chooses excessive data privacy.

Proof. Algebraic comparison of (26) and (30) reveals that $s^{YF*} < \tilde{s}^{YF}$. In terms of data privacy, the firm now shares data whenever, $\pi^{YF*} > \pi^{N*}$, see (11) and (27), which occurs whenever $\Delta > \overline{\overline{\Delta}}_{\pi}$, where

$$\overline{\overline{\Delta}}_{\pi} := -(1-\hat{\eta}) + (1-\eta)\sqrt{\frac{2-\hat{\eta}^2}{2-\eta^2}} > 0. \tag{31}$$

The planner shares data whenever $\tilde{W}^{YF} > \tilde{W}^{N}$, which, using (30) and Appendix C, requires $\Delta > \overline{\overline{\Delta}}_{W}$, where

$$\overline{\overline{\Delta}}_{W} := -(1-\hat{\eta}) + (1-\eta)\sqrt{\frac{4-3\hat{\eta}^2}{4-3\eta^2}} > 0. \tag{32}$$

Algebraic comparison of (31) and (32) reveals that $\overline{\overline{\Delta}}_{\pi} > \overline{\overline{\Delta}}_{W}$, implying that the firm under-shares data. See Supplementary Calculations. ■

Since equilibrium profits and investments under full liability are equivalent to those under liability for partial damages when $\theta = 1$, and since $\overline{\Delta}_{\pi}$ is increasing in θ and $\overline{\overline{\Delta}}_{\pi}$ is invariant to θ, it follows immediately that $\overline{\overline{\Delta}}_{\pi} > \overline{\Delta}_{\pi}$ for all $\theta < 1$. Therefore $\overline{\overline{\Delta}}_{\pi} > \overline{\Delta}_{I}$, see Lemma 1 and, consequently, $s^{YF*} > s^{Y*}$ for all $\theta < 1$.

It follows that this change in the liability rule promotes cybersecurity investments. Nonetheless, according to Proposition 9, these never reach the level associated with the second-best. The social planner still prefers a higher level of security due to the difference between the value of security investment to the average and the marginal consumers. Moreover, relative to the liability for partial damages case, a new problem is introduced in the sense that the firm is now certain to choose socially excessive levels of data privacy.

It is therefore interesting to compare equilibrium welfare levels under these alternative liability rules. In Figure 4, welfare under full liability is represented by the grey line, while the dashed black line indicates welfare under liability for partial damages. In panel (a), Δ is high enough to ensure that the firm shares data, irrespective of the liability rule and the level of θ. Welfare is higher under liability for partial damages than under full liability for all $\theta < 1$, because the higher price associated with the full liability rule, which tends to reduce demand and overall welfare, is not sufficiently offset by an increase in cybersecurity investment.

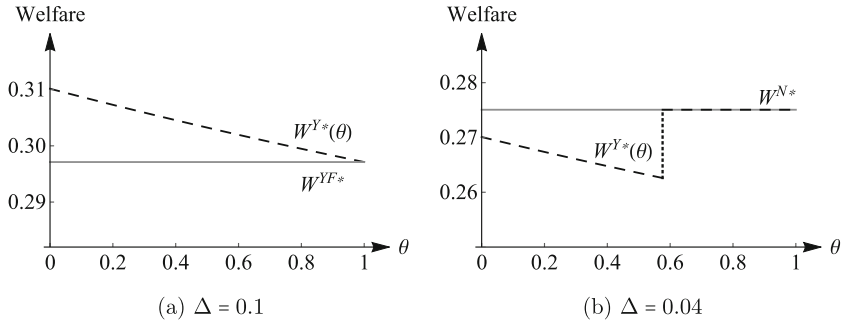


Figure 4
Welfare Comparison of Liability Rules ($\eta = 0.15$, $\phi = 0.5$)

Panel (b) makes clear that the data sharing decision also matters. In particular, full liability may be preferred when it deters the firm from sharing data. When $\eta = 0.15$ and $\phi = 0.5$, we have $\overline{\overline{\Delta}}_{\pi} = 0.07 > 0.04 = \Delta$, so the firm does not share data under full liability and welfare is equal to W^{N*} for all θ. When liable for partial damages, the firm shares data for all $\theta < 0.58$ and, in the range of θ where the firm shares data, full liability generates higher welfare. For higher values of θ, the firm would not share data under either liability rule, and welfare levels are consequently identical.

V(iv). *Consumer Mitigation Strategies*

Suppose that consumers can, at a private cost to themselves, undertake mitigation strategies that reduce the damage they suffer as a result of a cyber-breach at the third party when the data controller is liable for partial cyber-damages. This may be achieved by changing passwords, spending time to monitor user accounts, and using private browsing modes and ad blockers, for example.

These mitigation strategies do not affect the equilibrium when the data controller does not share data because, in that case, consumers face no risk of follow-on damages and therefore have no incentive to invest in mitigation. However, the availability of mitigation strategies does affect the equilibrium when the controller shares data, as shown below.

Suppose that every consumer can reduce the damage of follow-on attacks by the endogenous amount m, at a private cost equal to

$$e(u, m) = \frac{\overline{e}}{2u} m^2.$$

This cost is increasing in $\overline{e} > 0$, a parameter capturing the opportunity cost of effort, and in the magnitude of the selected damage reduction m, but decreasing in the consumer's product valuation u.

The optimal amount of damage reduction m^* therefore satisfies

$$m^* = \arg\max_m \left[u - \tau^{YM} - p(s^{YM})(\phi\eta - m) - e(u,m)\right] = \frac{p(s^{YM})u}{\bar{e}}, \tag{33}$$

where s^{YM} is the security investment chosen by the data controller in the presence of consumer mitigation strategies. The optimal mitigation effort is guaranteed to lie below $\phi\eta$ for all s^{YM} and u if $\bar{e} \geq \frac{1}{\phi\eta}$.

Using (33), a sophisticated consumer now joins the service if and only if

$$u \geq \tau^{YM} + A,$$

where

$$A = \frac{p(s^{YM})\phi\eta - \frac{\tau^{YM}p^2(s^{YM})}{2\bar{e}}}{1 + \frac{p^2(s^{YM})}{2\bar{e}}}. \tag{34}$$

Since naive consumers do not anticipate follow-on damages, they do not invest in mitigation and submit data whenever $u \geq \tau^{YM}$. This means that the data controller's optimization problem in the presence of consumer mitigation strategies, and conditional on data being shared, is given by

$$\begin{aligned}\max_{\tau^{YM},s^{YM}} \pi^{YM} = {} & \theta\left[\tau^{YM} - p(s^{YM})\eta + \Delta\right]\left[1 - \tau^{YM} - A\right] \\ & + (1-\theta)\left[\tau^{YM} - p(s^{YM})\eta + \Delta\right](1 - \tau^{YM}) - c(s^{YM}).\end{aligned} \tag{35}$$

We can show that:

Proposition 10. The availability of consumer mitigation strategies reduces security investments if η is small enough.

Proof. Using (35), the optimal investment level is determined by

$$\begin{aligned}\frac{\partial \pi^{YM}}{\partial s^{YM}} = {} & -p'(s^{YM})\eta(1 - \tau^{YM} - \theta A) \\ & - \frac{\partial A}{\partial s^{YM}}\theta\left[\tau^{YM} - p(s^{YM})\eta + \Delta\right] - c'(s^{YM}) = 0.\end{aligned} \tag{36}$$

Comparing (9) and (36) and evaluating at $\tau^{YM} = \tau^{Y^*}$ and $s^{YM} = s^{Y^*}$, we have $A < p(s^{Y^*})\phi\eta$. Demand is larger in the presence of mitigation strategies, which tends to increase the incentive to invest in security via the total demand effect. On the other hand, $-\frac{\partial A}{\partial s^{YM}} < -p'(s^{Y^*})\phi\eta$, so that the demand responsiveness effect is weaker in the presence of mitigation strategies, which reduces the incentive to invest in security. Notice, however, that the difference in the total demand effects with and without mitigation is of second order, whereas the difference in the demand responsiveness effects is of first order.

On balance, therefore, these effects imply a lower incentive to invest for small η. In addition, it is straightforward to show that the optimal price is higher with mitigation, and we can show that

$$\frac{\partial}{\partial \tau^{YM}}\left(\frac{\partial \pi^{YM}}{\partial s^{YM}}\right) < 0$$

if η is small enough. In particular, we have

$$\begin{aligned}\frac{\partial}{\partial \tau^{YM}}\left(\frac{\partial \pi^{YM}}{\partial s^{YM}}\right) = &\left[p'(s^{YM})\eta - \theta\frac{\partial A}{\partial s^{YM}}\right] + p'(s^{YM})\theta\eta\frac{\partial A}{\partial \tau^{YM}} \\ &- \theta(\tau^{YM} - p(s^{YM})\eta + \Delta)\frac{\partial}{\partial \tau^{YM}}\left(\frac{\partial A}{\partial s^{YM}}\right).\end{aligned}$$

The terms in square brackets are clearly negative. The remaining terms are negative when

$$\frac{\tau^{YM} - p(s^{YM})\eta + \Delta}{1 + \frac{p^2(s^{YM})}{2e}} > \frac{p(s^{YM})\eta}{2}.$$

Notice that $\tau^{YM} - p(s^{YM})\eta + \Delta$ is the margin, which must be strictly positive for the firm to be active in the market. It follows that η small is a sufficient condition for the above condition to be satisfied. In that case, the price effect is weaker in the presence of mitigation strategies, and the incentives to invest in security is consequently lower. It follows that the availability of mitigation strategies weakens the firm's incentives to invest in security when η is small. ■

It is interesting to consider whether this reduction in security investments necessarily implies a fall in equilibrium welfare levels. Conditional on data being shared, welfare in the presence of consumer mitigation strategies is given by

$$\begin{aligned}W^{YM} &= \theta\int_{\tau^{YM*}+A^*}^{1}\left[u + \Delta - p\left(s^{YM}\right)(\hat{\eta} - m^*) - e(m^*)\right]\mathrm{d}u \\ &\quad + (1-\theta)\int_{\tau^{YM*}}^{1}\left[u + \Delta - p\left(s^{YM}\right)\hat{\eta}\right]\mathrm{d}u - c\left(s^{YM}\right), \\ \text{s.t. } A^* &= \frac{p(s^{YM})\phi\eta - \frac{\tau^{YM*}p^2(s^{YM})}{2\bar{e}}}{1 + \frac{p^2(s^{YM})}{2\bar{e}}}, \\ \tau^{YM*} &= \arg\max_{\tau^{YM}} \pi^{YM}, \\ m^* &= \frac{p(s^{YM})u}{\bar{e}}. \end{aligned} \tag{37}$$

Given the complexity of both the welfare and profit expressions, we consider two scenarios to illustrate the contrasting effects that consumer mitigation strategies may exert on welfare. When $\eta = 0.15$, $\phi = \theta = 0.8$, $\overline{e} = 5$ and $\Delta = 1$, the optimal security investments with and without consumer mitigation are given by $s^{YM*} = 0.20 < 0.22 = s^{Y*}$. Equilibrium welfare levels with and without mitigation, as calculated using (37) and (19), respectively, are equal to $W^{YM*} = 1.19 > 1.18 = W^{Y*}$. In this case, the mitigation activities of consumers enhance welfare.

If $\eta = 0.35$, $\phi = \theta = 0.8$, $\overline{e} = 5$ and $\Delta = 1$, optimal security investments are equal to $s^{YM*} = 0.47 < 0.49 = s^{Y*}$. Now, equilibrium welfare levels are given by $W^{YM*} = 0.945 < 0.947 = W^{Y*}$, so that the mitigation activities of consumers reduce welfare.[12] Placing greater control for the prevention of cyber-damages in the hands of consumers is therefore not unambiguously welfare-improving. In particular, cases exist in which the crowding out of the firm's security investments that goes along with consumers' mitigation efforts leads to lower welfare in equilibrium.

V(v). *Policy Discussion*

It follows from the preceding analysis that a minimum standard on security, disclosure and consumer education policies, liability rules and consumer mitigation strategies offer only partial solutions to the market failures we have identified with respect to data privacy and cybersecurity. In terms of a minimum security standard, the second-best may be unattainable because of the effect the standard exerts on the firm's decision to share data. Disclosure and consumer education policies tend to reduce welfare unless they deter data sharing. Similarly, moving to a setting in which the data controller is liable for all cyber-damages improves welfare relative to the liability for partial damages case only if it deters the firm from sharing data. Finally, the presence of consumer mitigation strategies reduces the firm's incentive to invest in security and may also lead to lower welfare.

Whenever unilateral policies fail to achieve the second-best or, even worse, exert a detrimental impact on welfare, a co-ordinated regulatory approach that jointly oversees data privacy and cybersecurity is needed.

This represents a departure from the existing regulatory framework in the UK, which takes interactions between privacy and security into account only in a more limited sense. In particular, the UK GDPR and Data Protection Act 2018 require controllers to ensure 'appropriate security' when transferring or otherwise processing personal data. Firms are expected to adhere to the security principle by putting in place measures that balance the risks of data

[12] In both cases, it may be verified that equilibrium profits are consistent with the firm deciding to share data.

sharing against the cost and state of the art of available security measures (Article 32(1) UK GDPR).[13]

Although reports suggest that this approach has increased investment in cybersecurity (RSM UK Consulting [2020]), it is also true that firms tend to underestimate the cyber-risks they are exposed to, which reduces their incentive to invest.[14] Moreover, as we have shown, even when firms assess risks accurately and are fully liable for cyber-damages, they under-invest in security.

A more prescriptive UK GDPR that not only defines the limits within which firms may lawfully share data but also specifies more directly the necessary security precautions that must accompany specific types of data sharing is one possible direction that future regulation might take to address these shortcomings. More generally, our results emphasise that joint control over a firm's data sharing and security investment choices is often necessary in order for the second-best to be achieved.[15]

VI. CONCLUSION

This paper studies firms' interdependent decision making in the areas of data privacy and cybersecurity. We find that, provided the damage of an individual cyber-attack is not too large, the relationship between privacy and security is negative in both the market equilibrium and the second-best in the sense that optimal security investments are higher when data is shared.

Nonetheless, our analysis also highlights important market failures with respect to both privacy and security. With respect to the former, we find that, when the data controller is liable for partial cyber-damages, it over-shares data relative to the second-best whenever the consumer population displays a non-negligible degree of naivety concerning cyber-risks. In terms of the latter, the controller under-invests in cyber-defences, irrespective of whether data is shared or not.

We study a number of regulatory interventions that may correct these market failures. In each case, the interdependence between privacy and security is crucial to understanding the welfare properties of the remedy under consideration. For example, while a minimum security standard unambiguously improves welfare when it obliges firms to invest more in security for a given sharing decision, it may fail to achieve the second-best because of inefficient data sharing that is induced by the standard itself. Similarly, the effect of

[13] Similar requirements are contained in the Network and Information Systems Regulations 2018 and the Privacy and Electronic Communications Regulations 2003.

[14] According to HM Government [2020], 63% of respondents identified difficulties in quantifying the benefits of cybersecurity as a factor behind low incentives to invest in security.

[15] Interviews conducted with businesses, regulators, law enforcement and legal advisers as part of Lam and Seifert [2021] support the conclusion that greater co-ordination and pooling of competencies would help to close gaps in regulation.

consumer policies and stricter liability rules depends crucially on the impact that these policies exert on data sharing.

These results suggest that stricter oversight of firms' cybersecurity choices than is currently the case under the UK GDPR may be appropriate. In particular, the reliance of the current approach on self-regulation, as part of which firms themselves assess the appropriate level of cybersecurity given the extent of their data sharing, may need to be replaced with a more prescriptive approach that specifies required security measures for different types of data sharing.

There are several important directions for future research. Firstly, we may endogenize the incentives of hackers in order to study the interactions between both sides of the security ecosystem. Secondly, our analysis highlights conflicting direct and indirect effects of data sharing on investment incentives. An empirical exploration of the extent to which privacy regulations may have unintended side effects on welfare remains an important open question.[16]

APPENDIX A

INTERIOR SOLUTIONS

When data is not shared, the restriction on η in Section II is sufficient to ensure interior solutions. When data is shared, we must restrict Δ to ensure that investments in the market equilibrium and second-best are between 0 and 1. Moreover, in order for demand to be interior, we require prices to be positive, irrespective of whether the investment level is chosen by the firm or the planner.

Substituting (20) into (8), in order for the market price in the second-best to be positive when data is shared, we require

$$\Delta < \overline{\delta}_1 := \frac{2 - \eta\left[\eta\left(3 + \phi(3 - \phi\theta(1-\theta))\right) - 2(1 - \phi\theta)\right]}{2 - \eta^2\phi(1+2\theta)(1+\phi\theta)}.$$

In order for the second-best investment in (20) to lie below 1, we require

$$\Delta < \overline{\delta}_2 := \frac{4}{\eta(3 + \phi(2+\theta))} - 1.$$

A general ranking of these two thresholds is not possible. For instance, when $\eta = 0.1$, $\phi = 0.5$ and $\theta = 0.1$, we have $\overline{\delta}_1 = 1.1 < 8.9 = \overline{\delta}_2$. When $\eta = 0.38$, $\phi = 0.95$ and $\theta = 0.4$, however, we have $\overline{\delta}_1 = 1.00 > 0.99 = \overline{\delta}_2$.

We therefore assume that $\Delta < \min\left\{\overline{\delta}_1, \overline{\delta}_2\right\}$. This condition is sufficient to ensure that all prices and investments under data sharing are interior.[17] These conditions

[16] Price effects associated with data privacy regulation have been discussed, albeit informally, in Yaraghi [2018] and McQuinn and Castro [2019].

[17] The same method may also be used to derive the thresholds that apply when the data controller is liable for full cyber-damages, see Supplementary Calculations.

are checked systematically in the Supplementary Calculations. It may also be verified that $\max\{\overline{\Delta}_\pi, \overline{\Delta}_W\} < \min\left\{\overline{\delta}_1, \overline{\delta}_2\right\}$, so that this restriction on Δ does not constrain the firm's or the planner's data sharing behaviour.

APPENDIX B

THEORETICAL FIRST-BEST

We show that the theoretical first-best in which the planner decides which consumers should submit data, whether or not this data should be shared between firms and the level of cybersecurity is unobtainable in the absence of price regulation. The first-best is consequently less relevant as a welfare benchmark for our regulatory analysis.

If data is not shared, the planner would like to direct all consumers with valuation $u > p\left(s^N\right)\eta$ to submit data. At the associated, optimal security investment level $\tilde{s}^N_{FB}$, first-best social welfare is equal to

$$\tilde{W}^N_{FB} = \int_{p(\tilde{s}^N_{FB})\eta}^{1} \left[u - p\left(\tilde{s}^N_{FB}\right)\eta\right] \mathrm{d}u - c\left(\tilde{s}^N_{FB}\right).$$

Supposing that the regulator can impose both the no-sharing decision and the investment level $\tilde{s}^N_{FB}$ to be implemented by the firm, in the absence of price regulation, the firm would set its optimal price to satisfy

$$\tau^{N*} = \frac{1}{2}\left[1 + p\left(\tilde{s}^N_{FB}\right)\eta\right].$$

Consumers with valuation $u > \tau^{N*}$ will submit data. Relative to the first-best, we have too few consumers joining whenever $\tau^{N*} > p\left(\tilde{s}^N_{FB}\right)\eta$, which must hold if the firm is to earn positive revenue, see (4). Hence the first-best is not attainable in the absence of data sharing if the price is unregulated.

Similarly, when data is shared, the planner would like to direct all consumers whose participation increases total welfare, that is all consumers with valuation $u > p(s^Y)\hat{\eta} - \Delta$, to submit data. At the associated, optimal security investment level $\tilde{s}^Y_{FB}$, first-best welfare is equal to

$$\tilde{W}^Y_{FB} = \int_{p(\tilde{s}^Y_{FB})\hat{\eta}-\Delta}^{1} \left[u + \Delta - p\left(\tilde{s}^Y_{FB}\right)\hat{\eta}\right] \mathrm{d}u - c\left(\tilde{s}^Y_{FB}\right). \tag{38}$$

If the regulator imposes the sharing decision and the optimal investment level $\tilde{s}^Y_{FB}$, the firm would optimally set price

$$\tau^{Y*} = \frac{1}{2}\left[1 - \Delta + p\left(\tilde{s}^Y_{FB}\right)\eta(1 - \phi\theta)\right].$$

At this price, sophisticated consumers with $u > \tau^{Y*} + p(\tilde{s}^Y_{FB})\phi\,\eta$ and naive consumers with $u > \tau^{Y*}$ will join. Total demand under market-determined prices is therefore equal to

$$\frac{1}{2}\left[1 + \Delta - p\left(\tilde{s}^Y_{FB}\right)\eta(1 + \phi\theta)\right].$$

This demand falls below demand in the first-best whenever

$$\frac{1}{2}\left[1+\Delta-p\left(\tilde{s}_{FB}^{Y}\right)\eta\left(1+\phi(2-\theta)\right)\right]>0. \tag{39}$$

Substituting in the first-best security level that maximises (38), namely

$$\tilde{s}_{FB}^{Y}=\frac{\hat{\eta}(1+\Delta-\hat{\eta})}{1-\hat{\eta}^{2}},$$

into (39) shows that this condition is always satisfied (see Supplementary Calculations). Again, we cannot attain the first-best outcome in the absence of price regulation.

APPENDIX C

PROOF OF PROPOSITION 4

Second-best welfare under no-sharing when investments are chosen according to (18) is given by

$$\tilde{W}^{N}=\frac{3(1-\eta)^{2}}{8-6\eta^{2}}.$$

The corresponding welfare level when data is shared and investments satisfy (20) are

$$\tilde{W}^{Y}=\frac{\left\{\begin{array}{c}3(1+\Delta-\eta)^{2}-2\eta\phi(1+\Delta-\eta)(2+\theta)\\+\eta^{2}\phi^{2}\left[(1+\Delta)^{2}(1+\theta)+\theta^{2}(1-2\Delta(2+\Delta))\right]\end{array}\right\}}{8-\eta^{2}\left[6+2\phi(4+\theta(2+3\phi\theta))\right]}.$$

Data sharing is preferred whenever $\tilde{W}^{Y}>\tilde{W}^{N}$, which occurs whenever $\Delta>\overline{\Delta}_{W}$, where

$$\overline{\Delta}_{W}:=-1+\frac{\eta\left[3+\phi(2+\theta)\right]}{3+\eta^{2}\phi^{2}(1-\theta)(1+2\theta)}+\left[\frac{\left(4-\eta^{2}(3+\phi(4+\theta(2+3\theta\phi)))\right)\left(9(1-\eta)^{2}+\eta^{2}\phi^{2}(7-6\eta)(1-\theta)(1+2\theta)\right)}{(4-3\eta^{2})(3+\eta^{2}\phi^{2}(1+\theta-2\theta^{2}))^{2}}\right]^{\frac{1}{2}}.$$

REFERENCES

Acquisti, A.; Taylor, C. and Wagman, L., 2016, 'The Economics of Privacy,' *Journal of Economic Literature*, 54, pp. 442–492.

Anderson, R. and Murdoch, S. J., 2010, 'Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication,' in Sion, R. (ed.), *Financial Cryptography and Data Security. FC 2010*. Lecture Notes in Computer Science, Vol. 6052 (Springer, Berlin, Germany).

Argenziano, R. and Bonatti, A., 2021, *Data Linkages and Privacy Regulation*, Working Paper.
BBC, 2019, *Equifax to Pay up to $700m to Settle Data Breach*, July 22, 2019.
Bergemann, D. and Bonatti, A., 2019, 'Markets for Information: An Introduction,' *Annual Review of Economics*, 11, pp. 85–107.
Calzolari, G. and Pavan, A., 2006, 'On the Optimality of Privacy in Sequential Contracting,' *Journal of Economic Theory*, 130, pp. 168–204.
Choi, J. P.; Fershtman, C. and Gandal, N., 2010, 'Network Security: Vulnerability and Disclosure Policy.' *The Journal of Industrial Economics*, 58, pp. 868–894.
Communications Consumer Panel, 2011, *Online Personal Data: The Consumer Perspective*, Communications Consumer Panel Research Report, *https://www.communicationsconsumerpanel.org.uk/Onlinepersonaldatafinal240511.pdf*.
Competition and Markets Authority, 2021, *A Joined-up Approach to Digital Regulation*, Press Release, March 10, 2021.
Deloitte, 2020, *Digital Consumer Trends 2020*, *https://www2.deloitte.com/uk/en/pages/technology-media-and-telecommunications/articles/digital-consumer-trends-data-privacy.html*.
DMA, 2018, *Data Privacy: What the Consumer Really Thinks*, *https://dma.org.uk/uploads/misc/5a857c4fdf846-data-privacy-what-the-consumer-really-thinks-final_5a857c4fdf799.pdf*.
Farrer & Co., 2020, *Art Heist: Constable painting the Subject of £2.4 million Online Fraud*, *https://www.farrer.co.uk/news-and-insights/art-heist-constable-painting-the-subject-of-2.4-million-online-fraud/*.
Financial Times, 2018, *Facebook Reveals Cyber Attack Affecting up to 50m Users*, September 28, 2018.
Financial Times, 2019, *Facebook Seeks to Knit Instagram and WhatsApp With Core App*, January 31, 2019.
Gordon, L. A. and Loeb, M. P., 2002, 'The Economics of Information Security Investment,' *ACM Transactions on Information and System Security*, 5, pp. 438–457.
Guardian, 2018, *Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, March 17, 2018.
HM Government, 2015, *New £5000 Government Grant for Small Businesses to Boost Cyber Security*, Press Release, July 16, 2015.
HM Government, 2016, *Making Cyberspace "Cyber Safe"—New Government Initiative for Cyber Startups Will Drive Innovation*, Press Release, January 26, 2016.
HM Government, 2020, *Cyber Security Incentives & Regulation Review: Summary of Responses to the Call for Evidence*, Policy Paper, *https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence/cyber-security-incentives-regulation-review-summary-of-responses-to-the-call-for-evidence*.
Ichihashi, S., 2020, 'Online Privacy and Information Disclosure by Consumers,' *American Economic Review*, 110, pp. 569–95.
Business Insider, 2019, *Zoom is Being Sued for Allegedly Handing over Data to Facebook*, March 31, 2020.
Jullien, B.; Lefouili, Y. and Riordan, M. H., 2020, *Privacy Protection, Security, and Consumer Retention*, TSE Working Paper, 18–947.
Lam, W. M. W., 2016, 'Attack-Prevention and Damage-control Investments in Cybersecurity,' *Information Economics and Policy*, 37, pp. 42–51.
Lam, W. M. W. and Seifert, J., 2021, *Regulatory Interactions and the Design of Optimal Cybersecurity Policies*, Report prepared for ESRC Discribe Hub+. *https://static1.squarespace.com/static/5f8ebbc01b92bb238509b354/t/618cf3a82f816f66d11dd4cc/1636627370520/Lam+Seifert+Final+Project+Report.pdf*.

Lamoreaux, N.R., 2019, 'The Problem of Bigness: From Standard Oil to Google,' *Journal of Economic Perspectives*, 33, pp. 94–117.
Li, W. C. Y.; Nirei, M. and Yamana, K., 2019, 'Value of Data: There's No Such Thing as a Free Lunch in the Digital Economy,' *RIETI Discussion Paper Series*, 19-E-022.
Mann, C. L., 2015, 'Information Lost,' in Goldfarb, A.; Greenstein, S. M. and Tucker, C. E. (eds.), *Economic Analysis of the Digital Economy* (NBER, Chicago, U.S.A.), *https://www.nber.org/system/files/chapters/c12990/c12990.pdf*.
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*.
McQuinn, A. and Castro, D., 2019, *A Grand Bargain on Data Privacy Legislation for America*, Information Technology & Innovation Foundation Report, *http://www2.itif.org/2019-grand-bargain-privacy.pdf*.
National Infrastructure Commission, 2019, *Strategic Investment and Public Confidence*, *https://www.nic.org.uk/wp-content/uploads/NIC-Strategic-Investment-Public-Confidence-October-2019.pdf*.
OnAudience, 2018, *Global Data Market Size 2017–2019*, *https://www.onaudience.com/files/OnAudience.com_Global_Data_Market_Size_2017-2019.pdf*.
Raul, A. and Mohan, V., 2018, 'United States,' in Raul, A. (ed.), *Privacy, Data Protection and Cybersecurity Law Review* (Law Business Research, London, UK).
RSM UK Consulting, 2020, *Impact of the GDPR on Cyber Security Outcomes*, Final Report, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/906691/Impact_of_GDPR_on_cyber_security_outcomes.pdf*.
Statista, 2018, *Forecast of Big Data Market Size, Based on Revenue, From 2011 to 2027*, *https://www.statista.com/statistics/254266/global-big-data-market-forecast/*.
Taylor, C., 2004, 'Consumer Privacy and the Market for Customer Information,' *The RAND Journal of Economics*, 35, pp. 631–650.
New York Times, 2018, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, December 18, 2018.
Yaraghi, N., 2018, *A Case Against the General Data Protection Regulation*, *https://www.brookings.edu/blog/techtank/2018/06/11/a-case-against-the-general-data-protection-regulation/*.

SUPPORTING INFORMATION

Additional supporting information maybe found in the online version of this article at *http://wileyonlinelibrary.com/journal/joie* or via the Journal's website, *http://www.jindec.org.*