Journal Pre-proof

Does data protection legislation increase the quality of internet services?

Wing Man Wynne Lam, Bruce Lyons

PII: S0165-1765(20)30284-6
DOI: https://doi.org/10.1016/j.econlet.2020.109463
Reference: ECOLET 109463

To appear in: *Economics Letters*

Received date : 8 April 2020
Revised date : 1 August 2020
Accepted date : 1 August 2020

Please cite this article as: W.M.W. Lam and B. Lyons, Does data protection legislation increase the quality of internet services?. *Economics Letters* (2020), doi: https://doi.org/10.1016/j.econlet.2020.109463.

Highlights:

- Opt-in regulation (e.g. GDPR) changes the behaviour of loss averse consumers
- This changes investment incentives for firms
- Investment in data security increases under opt-in regulation
- The condition for investment in service quality also to increase is identified
- Most consumer types gain, even when service quality falls

*Title Page

Does Data Protection Legislation Increase the Quality of Internet Services?

Wing Man Wynne Lam[a], Bruce Lyons[b,*]

[a]Norwich Business School and Centre for Competition Policy, University of East Anglia, Norwich Research Park, NR4 7TJ, Norwich, United Kingdom
[b]School of Economics and Centre for Competition Policy, University of East Anglia, Norwich Research Park, NR4 7TJ, Norwich, United Kingdom

Abstract

Digital firms attract consumers and collect their data by offering service enhancements and data security. These require separate types of investment. In light of the GDPR, data collection now requires explicit consumer consent, i.e. opt-in. This changes the consumer default option and the data provision decision when consumers are loss averse. We examine the consequences for investment. We set out the conditions under which opt-in increases both types of investment and when security comes at the expense of service quality. We further find that most consumer types gain, even when service quality falls.

Keywords: Data protection; Loss aversion, Investment incentives, Regulation
JEL classification: L51, L86

*Corresponding Author
Email addresses: wing.m.lam@uea.ac.uk (Wing Man Wynne Lam), b.lyons@uea.ac.uk (Bruce Lyons)

1. Introduction

In digital markets, consumers typically enjoy a benefit from providing their personal data in the form of individualised value added services (e.g. individualised search results, information on products of personal interest, access to relevant social networks). At the same time, many consumers are concerned about the security of their personal data and its potential misuse (e.g. identity theft, hacking of credit card details, misuse for political purposes). Consequently, internet firms invest both in the quality of value added services to attract consumers and in data security to create the confidence for them to provide their data.

There are also wider public and political concerns about the use and misuse of personal data by firms. These concerns have resulted in the EU's General Data Protection Regulation (GDPR) of 2018 and the California Consumer Privacy Act of 2020. In particular, the GDPR grants consumers a right to determine how their own data is used and requires consumer consent before data collection, i.e. opt-in. The evidence suggests this has substantially reduced consumer willingness to provide their data for commercial use.[1]

While this may be partly due to increased privacy awareness, another plausible explanation is that these regulations shift consumers to a new reference point so they perceive gains and losses differently, which changes data provision decisions (Kahneman et al., 1991). Acquisti et al. (2013) find that the ratio between willingness-to-accept to give up privacy and willingness-to-pay to keep privacy is five. This cannot be explained by privacy awareness or traditionally rational consumers, but is exactly consistent with loss aversion.[2]

We examine the unintended side-effects of privacy legislation on business investment decisions when consumers are loss averse: how does a change from opt-out to opt-in affect a firm's investment incentives? In particular, does it reduce or enhance the quality of value-added services? What is the consequent effect on consumer welfare? These questions have not received much attention despite the legislative aim to protect personal data while allowing digital markets to flourish. The paper contributes to the literature on privacy protection; see Acquisti et al. (2016) for a survey. Recent contributions have focused on issues such as information disclosure (e.g. Ichihashi, 2020) and data ownership (e.g. Dosis and Sand-Zantman, 2019), whereas this paper focuses on the issue of multi-dimensional investments (see e.g. Lam, 2016, for a related discussion). Furthermore, by taking into account consumer loss aversion, which is largely missing in the literature of digital regulation, this paper contributes to the literature of behavioural industrial organization (see Heidhues and Köszegi, 2018, for a review).

[1]Six months after the GDPR enforcement deadline, a survey by Deloitte (2018) of 1,650 consumers in 11 countries found 23% had opted out of direct marketing, leaving 60% "still willing to share information on themselves in exchange for personalised benefits or discounts".

[2]Aridor et al. (2020) and Johnson et al. (2020) provide further evidence that consumers behave differently under opt-in and opt-out.

2. The Model and Analysis

Consider a monopolist providing a basic service worth v_0 to consumers. In addition, the provider offers an individualised service based on each consumer's data, if a consumer consents to data collection. We denote $u(e_v)$ as the value of the data service, which is increasing in the provider's investment in value enhancement, e_v. Consumers are differentiated in their valuation for the data service, $\theta \in [0,1]$ distributed according to $M(\theta)$, which is continuously differentiable on $[0,1]$. We assume that $\theta m(\theta)$ is increasing in θ. If a consumer consents to data collection, he/she may experience a loss when there is a breach or misuse of their data, denoted $b(e_c)$. We assume $b(e_c)$ is decreasing in the provider's quality of security control, e_c.[3]

Assumption 1. *$u'(e_v) > 0, u''(e_v) \leq 0; b'(e_c) < 0$.*

Denote the total value of the firm's services by u, which consists of the basic service and data service in the case of consent, and the potential risk of breach by b. In the case of dissent to data collection, we have $(u, b) = (v_0, 0)$ and in the case of consent to data collection, we have $(u, b) = (v_0 + \theta u(e_v), b(e_c))$.

Therefore, the utility of loss-neutral consumers is simply given by

$$U = u - b.$$

The utility of loss-averse consumers depends additionally on their reference point. Given a reference point (r_u, r_b), a consumer evaluates the service of the provider (u, b) as the consumption utility $u-b$ plus the gain-loss utility evaluated against the reference point. Specifically, his/her utility is given by

$$U = u - b - \lambda \max(r_u - u, 0) - \lambda \max(b - r_b, 0),$$

with $\lambda > 0$. Thus, a loss is more painful than an equal amount of gain in the sense that a consumer is loss-averse but not gain-loving.[4] We assume a consumer consents to data collection if he/she is indifferent.

For simplicity, we assume that the provider does not charge consumers a price but generates profits from other sources based on data collection, e.g. advertisements. We normalize the profit per consumer with data collection to one.[5] Hence, the provider chooses e_v and e_c to maximize demand net of costs, which are given by $C_v(e_v)$ and $C_c(e_c)$. Both are assumed to be increasing and convex.

[3] This assessment may be informed by past security breaches and disclosures, which depend on e_c. Deloitte (2018) found 17% of respondents would stop using a service in the event of a data breach. Furthermore, 70% of potential customers would be concerned about engaging with a brand with a history of a data compromise. Gordon et al. (2010) show that disclosure of security measures has real effects on the value of the firm.

[4] This follows Spiegler (2011).

[5] This is reasonable in our set-up as we do not model explicitly the advertising market and hence there is no difference for advertisers between consumers who opt-in and those who opt-out. Moreover, Aridor et al. (2020) show empirically that, overall, GDPR has little impact on ad revenue.

Assumption 2. $C_v'(e_v) > 0, C_v''(e_v) > 0; C_c'(e_c) > 0, C_c''(e_c) > 0.$

Although we make no assumption on the sign of $b''(e_c)$, we require that the second order conditions for the firm's optimisation problem are satisfied. A necessary condition for this is that the security cost function is more convex than the breach function.[6] Define $B(e_c) = \frac{-e_c b''(e_c)}{b'(e_c)}$ as the curvature of the breach function, and $G(e_c) = \frac{e_c C_c''(e_c)}{C_c'(e_c)} > 0$ as the curvature of the security cost function.

Assumption 3. $B(e_c) + G(e_c) > 0.$

Consider first a benchmark model where consumers are loss-neutral. The reference point has no effect and a consumer will opt-in for data collection (or not opt-out) if

$$v_0 + \theta u(e_v) - b(e_c) \geq v_0.$$

That is,

$$\theta \geq \frac{b(e_c)}{u(e_v)},$$

hence, demand (i.e. consumers providing data) is $1 - M\left(\frac{b(e_c)}{u(e_v)}\right)$.[7]

In the presence of loss aversion, as shown in Section 2.1 and 2.2, we can write the demand function as $1 - M\left(\alpha\frac{b(e_c)}{u(e_v)}\right)$, where $\alpha > 0$ varies according to the consumer reference point and $\alpha = 1$ in the absence of loss aversion. Hence, we define an α-problem for the service provider as

$$\max_{e_v, e_c} \pi(e_v, e_c) = 1 - M\left(\alpha\frac{b(e_c)}{u(e_v)}\right) - C_v(e_v) - C_c(e_c).$$

Writing $m\,(.)$ as the density of $M\left(\alpha\frac{b(e_c)}{u(e_v)}\right)$, the optimal investments satisfy

$$-\alpha\frac{b'(e_c)}{u(e_v)} m\,(.) = C_c'(e_c), \tag{1}$$

$$\alpha\frac{b(e_c)u'(e_v)}{u^2(e_v)} m\,(.) = C_v'(e_v), \tag{2}$$

which together imply

$$\frac{-b'(e_c)/b(e_c)}{C_c'(e_c)} = \frac{u'(e_v)/u(e_v)}{C_v'(e_v)}. \tag{3}$$

[6] That is, $\frac{b''(e_c)}{b'(e_c)} - \frac{C''(e_c)}{C'(e_c)} < 0$. The proof for sufficient second-order conditions is available upon request.

[7] To ensure an interior solution with the indifferent consumer located between 0 and 1, we require $\frac{-b'(e_c)/b(e_c)}{C_c'(e_c)} > \frac{1}{m(1)}$ for any e_c. See Equation (4).

Equation (3) defines a relationship between e_v and e_c that has to hold for the optimal investments. Note that the marginal consumer is given by $\hat{\theta} = \alpha \frac{b(e_c)}{u(e_v)}$, hence, $-\frac{b'(e_c)}{b(e_c)} = |\frac{d\hat{\theta}/de_c}{\hat{\theta}}|$ and $\frac{u'(e_v)}{u(e_v)} = |\frac{d\hat{\theta}/de_v}{\hat{\theta}}|$ are the marginal impacts of the two investments on the location of the marginal consumer. Altogether, Equation (3) can be interpreted as the ratio of the marginal benefit to the marginal cost for the two investments being equal. By assumption, the right hand side (the benefit/cost ratio for value enhancement) is decreasing in e_v. We further assume that the left hand side is monotone. We then have two situations:

1. If the left hand side is decreasing in e_c, then in equilibrium $de_c/de_v > 0$. In this case, the equilibrium investments are *complements*.
2. If the left hand side is increasing in e_c, then in equilibrium $de_c/de_v < 0$. In this case, the equilibrium investments are *substitutes*.

Which situation arises in equilibrium depends on the shape of the breach function $b(e_c)$. Define $\epsilon(e_c) = \frac{-e_c b'(e_c)}{b(e_c)} > 0$ as the elasticity of the breach function and we show that

Lemma 1. *Equilibrium investments are substitutes if and only if $\epsilon > B + G$ ("easy" security enhancement). They are complements if and only if $\epsilon < B + G$ ("difficult" security enhancement). They are independent if and only if $\epsilon = B + G$ (exact log-linearity in security).*

Proof. Equilibrium investments are substitutes if and only if the LHS of Equation (3) is increasing in e_c, i.e. if $\frac{dy}{de_c} > 0$, where

$$y = \frac{-b'(e_c)/b(e_c)}{C_c'(e_c)}.$$

Further define $\gamma(e_c) = \frac{e_c C_c'(e_c)}{C_c(e_c)}$ as the elasticity of cost of supplying security. Differentiating y with respect to e_c, we obtain

$$\frac{dy}{de_c} = \frac{C_c'(e_c)\frac{-b''(e_c)b(e_c)+(b'(e_c))^2}{b^2(e_c)} + \frac{b'(e_c)}{b(e_c)}C_c''(e_c)}{(C_c'(e_c))^2} = \frac{\epsilon(\epsilon - B - G)}{\gamma e_c C_c(e_c)}.$$

Given that $\epsilon > 0$ and $\gamma > 0$, we have $dy/de_c > 0$ if and only if $\epsilon > B + G$, $dy/de_c < 0$ if and only if $\epsilon < B+G$, and $dy/de_c = 0$ if and only if $\epsilon = B+G$. □

Intuitively, consider an exogenous increase in α, which we later interpret as a GDPR-type policy change. This directly increases the marginal benefit of both investments, i.e. the LHS of Equations (1) and (2), and raises the incentive for both types of investment. As e_c and e_v increase, the benefit/cost ratio of value enhancement decreases, but that of security control increases if the left hand side of Equation (3) is increasing. This makes it relatively more attractive to invest in security control rather than value enhancement. Therefore, the equilibrium investments become substitutes. This occurs when it is easy to enhance security substantially, i.e. when the breach function is sufficiently elastic. On the other hand, if the left hand side of Equation (3) is decreasing, then the benefit/cost ratio of both investments move in the same direction and then we have the equilibrium investments being complements.

Having established the independence of Lemma 1 from the distribution of θ, we simplify the presentation of our results by assuming a uniform distribution so demand is $1 - \alpha\frac{b(e_c)}{u(e_v)}$.

2.1. Opt-In with Loss-Averse Consumers

Now we consider opt-in when consumers are loss-averse. In this case, the default is no data collection where consumers obtain the value of v_0 and do not face any data breach risk, i.e. the reference point is $(r_u^{in}, r_b^{in}) = (v_0, 0)$. Thus, a consumer opts-in if

$$v_0 + \theta u(e_v) - b(e_c) - \lambda b(e_c) \geq v_0,$$

that is,

$$\theta \geq \frac{(1+\lambda)b(e_c)}{u(e_v)}.$$

Specifically, compared to the reference point, opt-in associates service value with a gain of $\theta u(e_v)$ and security risk with a loss of $b(e_c)$; hence, there is an additional gain-loss utility of $-\lambda b(e_c)$. The service provider then faces an α-problem with $\alpha = 1 + \lambda$ and we have the following result:

Proposition 1. *(Opt-in) Compared to the loss-neutral benchmark, the provider invests more in security. In the case of complements, the provider also invests more in value enhancement. In the case of substitutes, the provider invests less in value enhancement. In the case of independence, investment in value enhancement remains fixed.*

Proof. The equilibrium must satisfy Equations (1) and (2). Taking total differentiation with respect to α, we obtain

$$\begin{aligned} \tfrac{de_c}{d\alpha} \propto \quad & det \begin{bmatrix} \frac{b'}{u} & \alpha\frac{b'u'}{u^2} \\ -\frac{bu'}{u^2} & \alpha b\frac{u''u-2(u')^2}{u^3} - C_v'' \end{bmatrix} \\ = \quad & \alpha\tfrac{bb'}{u^3}\big(u'' - \tfrac{(u')^2}{u}\big) - \tfrac{b'}{u}C_v'', \end{aligned}$$

which is always positive. That is, $de_c/d\alpha > 0$. In the case of complements, Equation (3) implies that $de_v/d\alpha > 0$. In the case of substitutes, Equation (3) implies that the two terms must have different signs, so $de_v/d\alpha < 0$. In the case of independent investments, e_v remains unchanged with α. □

The intuition is that under opt-in, consumers overweigh the security risks or privacy concerns related to data collection. This added weight boosts the incentive to invest in security. In the case of substitutes, the effect highlighted under Lemma 1 then reduces the incentive for service quality improvement, but complementarity applies if it is sufficiently difficult to enhance security.

2.2. Opt-Out with Loss-Averse Consumers

Under opt-out, the default is with data collection where consumers obtain the value of $v_0 + \theta u(e_v)$ but face a data breach risk of $b(e_c)$, i.e. the reference point is $(r_u^{out}, r_b^{out}) = (v_0 + \theta u(e_v), b(e_c))$. Thus, a consumer does not opt-out if

$$v_0 + \theta u(e_v) - b(e_c) \geq v_0 - \lambda\theta u(e_v),$$

that is

$$\theta \geq \frac{b(e_c)}{(1+\lambda)u(e_v)}.$$

Specifically, opting-out is associated with a loss of the value of data service, $\theta u(e_v)$, and a gain of avoiding data risk, $b(e_c)$; hence, there is an additional gain-loss utility of $-\lambda\theta u(e_v)$. The service provider then faces an α-problem with $\alpha = \frac{1}{1+\lambda}$:

Proposition 2. *(Opt-out) Compared to the loss-neutral benchmark, the provider invests less in security. In the case of complements, the provider also invests less in value enhancement. In the case of substitutes, the provider invests more in value enhancement. In the case of independence, investment in value enhancement remains fixed.*

Proof. This follows similarly to the proof of Proposition 1. □

The intuition is similar to opt-in. Under opt-out, consumers under-weigh security relative to the loss of value added service. The firm invests less in security investment, but value enhancing investment may increase or decrease depending on the ease of security enhancement.

Finally, note that $\alpha = \frac{1}{1+\lambda} < 1$ under opt-out, and $\alpha = 1 + \lambda > 1$ under opt-in, so a GDPR-type regulation that changes the reference point is equivalent to an exogenous increase in α.

3. Welfare Implications of Investment Side-Effects of Opt-In Regulation

Regulating for opt-in hurts the service provider as the firm always prefers the default of an opt-out regime.[8] The impact on consumer welfare is more complex, depending on whether investments are complements or substitutes and how we view loss aversion in consumer welfare. We first consider the effect on data provision, before examining the welfare of individual consumers.

We can rank the indifferent consumer under each regime, taking into account the endogenous levels of investments. Opt-in has a direct effect on α, tending to increase $\hat{\theta}$ (i.e. reduce the number of consumers providing data), and indirect

[8]More formally, we can apply the envelope theorem to the profit function in the α-problem: $\frac{d\pi}{d\alpha} = -\frac{b(e_c)}{u(e_v)} < 0$.

effects through changed investments. Substituting the marginal consumer $\hat{\theta} = \frac{\alpha b(e_c)}{u(e_v)}$ into Equation (1), we have

$$\hat{\theta} m(\hat{\theta}) = \frac{1}{\frac{-b'(e_c)/b(e_c)}{C_c'(e_c)}}. \tag{4}$$

Write superscripts *out* for equilibrium opt-out values, *bm* for the benchmark, and *in* for opt-in; and subscripts *com* for $\hat{\theta}$ in the case of complements and *sub* for substitutes. The following Lemma summarises the net effect on $\hat{\theta}$, with the implication that a switch from opt-out to an opt-in regime decreases data provision when investments are complements, but increases it in the case of substitutes (because security is so much enhanced even though this is partly at the expense of a lower quality product).

Lemma 2. *For complements, the ranking of indifferent consumers is* $\theta^{out}_{com} = \frac{b(e_c^{out})}{(1+\lambda)u(e_v^{out})} < \theta^{bm}_{com} = \frac{b(e_c^{bm})}{u(e_v^{bm})} < \theta^{in}_{com} = \frac{(1+\lambda)b(e_c^{in})}{u(e_v^{in})}$*, so fewer consumers provide data under opt-in regulation. The ordering is reversed for substitutes:* $\theta^{in}_{sub} < \theta^{bm}_{sub} < \theta^{out}_{sub}$*, so more consumers provide data. For independent investments,* $\hat{\theta}$ *is unchanged by the default regime.*

Proof. e_c increases with α (see proof of Proposition 1), and $\frac{-b'(e_c)/b(e_c)}{C_c'(e_c)}$ is increasing in e_c for substitutes (Lemma 1), so $\hat{\theta}$ decreases with e_c (Equation 4). Thus, demand increases with α. For complements, $\frac{-b'(e_c)/b(e_c)}{C_c'(e_c)}$ is decreasing in e_c, so by similar reasoning $\hat{\theta}$ increases and demand falls with α. For independent investments, $\frac{-b'(e_c)/b(e_c)}{C_c'(e_c)}$ is constant, so the marginal consumer is invariant to the default. Lemma 2 follows from $\alpha^{out} = \frac{1}{1+\lambda}$ and $\alpha^{in} = 1 + \lambda$, so α increases with opt-in. $\square$

Next, consider consumer welfare. While loss aversion is a well-established 'bias' in positive economics, the normative implications of loss aversion remain controversial because it can be viewed either as a "mistake" in decision making (i.e. *ex post* experienced utility should be measured as if $\lambda = 0$), or as a "genuine" experience. In the latter case, we assume the extra burden of loss is felt *ex post* if it is the result of an active choice by the consumer (i.e. a change from the status quo).

Suppose loss aversion is a mistake. Define $\theta^{free} = \frac{b(e_c^{out})}{u(e_v^{out})}$ as the mistake-free marginal consumer under opt-out investments. θ^{free} provides our welfare benchmark to identify which consumers are better or worse off if they provide data.[9] On the other hand, suppose the loss is genuinely felt, active choice to opt-out under the initial regime incurs an additional loss of $\lambda\theta u(.)$, while active choice to opt-in under the regulated regime incurs an additional expected loss of $\lambda b(.)$.

[9] Note that $\theta^{out}_{com} < \theta^{free}$ and $\theta^{out}_{sub} < \theta^{free}$, so too many consumers provide data under the opt-out regime. However, our focus is on the direction of impact of regulation.

Proposition 3. *(Consumer welfare) a) In the case of loss aversion as a mistake, all consumers at least weakly gain from opt-in regulation with the exceptions of: i) consumers with* $\theta^{free} < \theta < \theta^{in}_{com}$ *if investments are complements - this set may be empty; or ii) consumers with very high* $\theta > \widetilde{\theta}_{sub} = \frac{b(e_c^{in})-b(e_c^{out})}{u(e_v^{in})-u(e_v^{out})}$ *if investments are substitutes. b) In the case of loss aversion as a genuine preference, all consumers gain from opt-in with the exceptions of: i) consumers with* $\theta^{free} < \theta < \widetilde{\theta}_{com} = \frac{(1+\lambda)b(e_c^{in})-b(e_c^{out})}{u(e_v^{in})-u(e_v^{out})}$ *if investments are complements - this set may be empty; or ii) consumers with very high* $\theta > \widetilde{\widetilde{\theta}}_{sub} = \frac{(1+\lambda)b(e_c^{in})-b(e_c^{out})}{u(e_v^{in})-u(e_v^{out})}$ *if investments are substitutes.*[10]

Proof. If loss aversion is experienced *ex post*, the consumer utility functions under opt-out and opt-in are given respectively by

$$U^{out} = \begin{cases} v_0 - \lambda\theta u(e_v^{out}), & \text{if } \theta < \theta^{out}_{com} \\ v_0 + \theta u(e_v^{out}) - b(e_c^{out}), & \text{if } \theta \geq \theta^{out}_{com}, \end{cases}$$

and

$$U^{in} = \begin{cases} v_0, & \text{if } \theta < \theta^{in}_{com} \\ v_0 + \theta u(e_v^{in}) - (1+\lambda) b(e_c^{in}), & \text{if } \theta \geq \theta^{in}_{com}. \end{cases}$$

Depending on whether θ^{free} is greater or smaller than θ^{in}_{com}, we have two cases when investments are complements, as illustrated by Figure 1. When we move from opt-out to opt-in, most consumers gain except the following two cases: First, in panel (a), when investments are complements and $\theta^{free} < \theta^{in}_{com}$, consumers with $\theta \in (\theta^{free}, \theta^{in}_{com})$ lose out as they no longer provide data and lose the value from data service, and consumers with $\theta \in [\theta^{in}_{com}, \widetilde{\theta}_{com})$ lose out due to the mental loss associated with potential security risk under opt-in. Second, in panel (c), when investments are substitutes, consumers with $\theta > \widetilde{\widetilde{\theta}}_{sub}$ lose out as the benefit of better security is not sufficient to compensate their loss of lower quality. For other consumers, they gain from avoiding the mental loss associated with opting out of data service (for consumers with low θ), better quality or enhanced security (for consumers with high θ).

If loss aversion is a mistake, the ex post consumer utility functions under opt-out and opt-in are given respectively by

$$U^{out} = \begin{cases} v_0, & \text{if } \theta < \theta^{out}_{com} \\ v_0 + \theta u(e_v^{out}) - b(e_c^{out}), & \text{if } \theta \geq \theta^{out}_{com}, \end{cases}$$

and

$$U^{in} = \begin{cases} v_0, & \text{if } \theta < \theta^{in}_{com} \\ v_0 + \theta u(e_v^{in}) - b(e_c^{in}), & \text{if } \theta \geq \theta^{in}_{com}. \end{cases}$$

A similar graph can be drawn for this case, except that the two utility functions overlap for consumers with $\theta < \theta^{out}_{com}$. Although the mental loss associated with

[10] Note that, although $\widetilde{\theta}_{com}$ and $\widetilde{\widetilde{\theta}}_{sub}$ take the same form, their values are different as the investments are different.

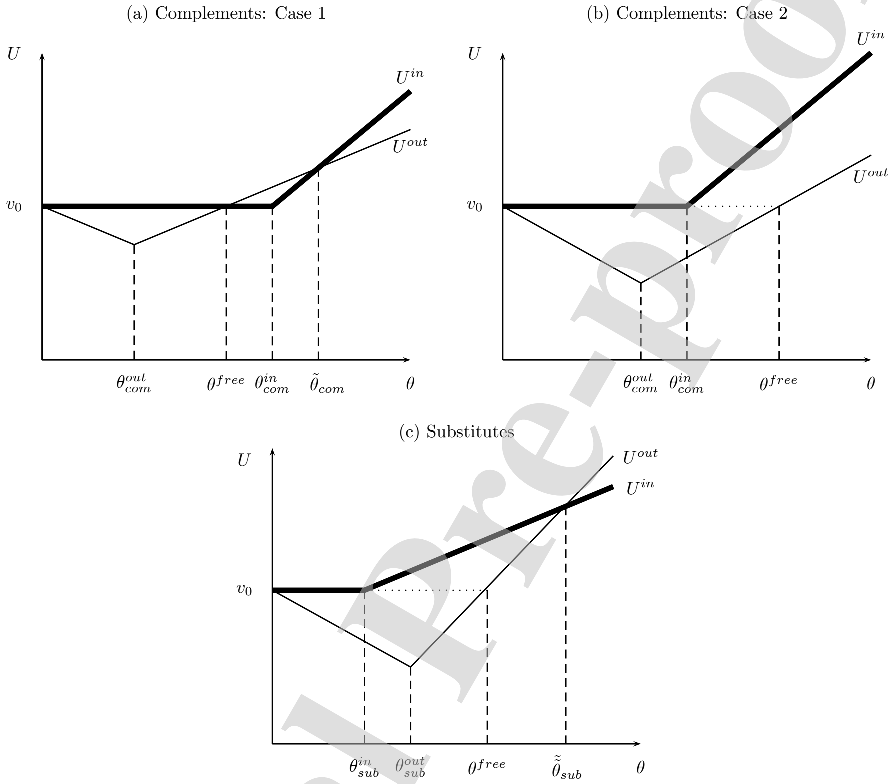

Figure 1: Loss Aversion as a Genuine Preference

λ is not genuinely felt and does not enter the utility functions, it does not affect the relative position of U^{in} and U^{out}. Hence, we still have the two groups of consumers who potentially lose out under opt-in, whereas the others gain. □

Put another way, although most consumers would gain from opt-in, the regulator needs to be cautious about two groups of consumers: conditional on investments being complements, possibly some of those who previously enjoyed enhanced services but who now choose not to opt-in, and some of those who still enjoy the service but suffer from the mental loss associated with the potential security risk; and, conditional on investments being substitutes, some consumers who put a very high value on quality, which now receives less investment.

4. Conclusion

The primary motive for data protection legislation has been privacy protection, but it remains important to examine the unintended consequences for business investment decisions and consumer welfare. We have developed a model of how an internet service provider's investment strategy responds to data protection legislation that requires consumers to opt-in. The change in default matters because of consumer loss-aversion. We find that investment in data security increases and we provide a sufficient condition for service quality also to be enhanced. We further find that most consumers gain from the investment side-effects of opt-in regulation while the service provider loses. Further work is needed on models with competitive entry and exit and with network externalities.

Acknowledgement

We thank Amelia Fletcher, Bob Sugden, conference and seminar participants in Norwich, Nottingham, Liège and Rhodes, and particularly Joe Harrington and the referee for their valuable comments. Bruce Lyons was supported in this research by the Economic and Social Research Council [grant number ES/P008976/1].

Acquisti, A., John, L. K., Loewenstein, G., 2013. What is privacy worth? The Journal of Legal Studies 42 (2), 249–274.

Acquisti, A., Taylor, C., Wagman, L., 2016. The economics of privacy. Journal of Economic Literature 54 (2), 442–92.

Aridor, G., Che, Y.-K., Salz, T., 2020. The economic consequences of data privacy regulation: empirical evidence from GDPR. NBER Working Paper No. 26900.

Deloitte, 2018. Almost a quarter of consumers have opted-out of direct marketing since GDPR. https://bit.ly/2nsEZDr (accessed 18/12/19).

Dosis, A., Sand-Zantman, W., 2019. The ownership of data. TSE Working Paper No. 19-1025.

Gordon, L. A., Loeb, M. P., Sohail, T., 2010. Market value of voluntary disclosures concerning information security. MIS quarterly 34 (3), 567–594.

Heidhues, P., Köszegi, B., 2018. Behavioral industrial organization. In: Bernheim, D., DellaVigna, S., Laibson, D. (Eds.), Handbook of Behavioral Economics: Foundations and Applications. Vol. 1. Ch. 6.

Ichihashi, S., 2020. Online privacy and information disclosure by consumers. American Economic Review 110 (2), 569–595.

Johnson, G., Shriver, S., Du, S., 2020. Consumer privacy choice in online advertising: Who opts out and at what cost to industry? Marketing Science 39 (1), 33–51.

Kahneman, D., Knetsch, J., Thaler, R., 1991. Anomalies: The endowment effect, loss aversion, and status quo bias. Journal of Economic Perspectives 5 (1), 193–206.

Lam, W., 2016. Attack-prevention and damage-control investments in cybersecurity. Information Economics and Policy 37, 42–51.

Spiegler, R., 2011. Bounded rationality and industrial organization. Oxford University Press.