Journal of Business Research xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Journal of Business Research

journal homepage: www.elsevier.com/locate/jbusres

Security in digital markets☆

Mariola Sánchez[a,b], Amparo Urbano[a,b,*]

[a] Universitat de Valencia, Edificio Departamental Oriental, Campus del Tarongers, 46022 - Valencia, Spain
[b] ERI-CES, Universitat de Valencia, c/Serpis 29, 46022 - Valencia, Spain

ARTICLE INFO

Keywords:
Digital markets
Privacy
Security
Signaling equilibrium

ABSTRACT

This paper contributes to the literature on security in digital markets. We analyze a two-period monopoly market in which consumers have privacy concerns. We make three assumptions about privacy: first, that it evolves over time; second, that it has a value that is unknown by all market participants in the first period; and third, that it may affect market participants' willingness to pay for products. The monopolist receives a noise signal about consumers' average privacy. This signal allows the monopolist to adjust the price in the second period and engage in price discrimination. The monopolist's price in period 2 acts as a signal to consumers about privacy. This signal, together with consumers' purchase experiences from the first period, determines demand. We address two scenarios: direct investment in security to improve consumers' experiences and investment in market signal precision.

1. Introduction

In the digital age, we live in an always-on world. Our commercial and private lives are migrating to online platforms at a frenetic pace thanks to technological advances and a vast array of apps. To speak of the intersection between technology and privacy is inevitable. Consequently, privacy has long been a moving target. For example, in October 2017, Amazon unveiled *Amazon key*, which lets deliverers into consumers' homes.[1] It has thus become a reality that corporations not only access our digital data but also gain a window into our very lives. To use this service, consumers must buy a camera and a digital key to enable delivery and guarantee security. Although this idea is original within the industry, it has become the target of hackers.[2] As a result, questions over security and trust in digital markets abound. Security in digital markets is therefore a fundamental consideration when consumers are concerned with privacy.

We contribute to the literature on security in such markets by analyzing the investment decisions of a two-period monopoly market in which consumers have privacy concerns. The value of privacy is unknown by all market participants in the first period and may affect their willingness to pay for the product. The monopolist receives a noise signal about consumers' average privacy. This signal enables the monopolist to adjust the price in the second period. The monopolist's price in this second period acts as a signal to consumers about their privacy. This signal, together with consumers' purchase experiences from the first period, determines demand.

Our setting is novel in that it considers the implications of firms' investment in security. We address two scenarios: direct investment in security to improve consumers' experiences and investment in market signal precision. Through direct investment, the firm shows that it cares about each consumer's individual experiences and thereby seeks to maximize consumers' maximum willingness to pay. Through investment in market signal precision, the firm tries to manipulate consumers' information and increase market demand.

2. Literature review

Issues with privacy and economics are nothing new. For a complete review of this field, see Acquisti, Taylor, and Wagman (2016). Theoretical research has analyzed price competition (Taylor & Wagman, 2014; Montes, SandZantman, & Valletti, 2015), price for information (Villas-Boas, 2004; Chen & Zhang, 2009), and exchange of consumer information (Taylor, 2004; Calzolari & Pavan, 2006).

Chellappa and Pavlou (2002) empirically linked trust to perceived

☆ The authors thank the Spanish Ministry of Economy, Industry and Competitiveness for providing financial support (BES-2014-069278). The authors acknowledge the financial support of the Ministry of Economics and Competition (project ECO2016-75575-R) and the Generalitat Valenciana (Excellence Program Prometeo 2014II/054 and ISIC 2012/021).

* Corresponding author at: Departamento de Analisis Economico, Edificio departamental oriental, Avenida de los Naranjos s/n, 46022 - Valencia, Spain.
E-mail addresses: mariola.sanchez@uv.es (M. Sánchez), amparo.urbano@uv.es (A. Urbano).

[1] https://www.youtube.com/watch?v=wn7DBdaUNLA.

[2] https://www.forbes.com/sites/kevinmurnane/2017/12/12/what-could-possibly-go-wrong-amazon-key/#187c99974119.

https://doi.org/10.1016/j.jbusres.2018.12.066
Received 11 June 2018; Received in revised form 20 December 2018; Accepted 23 December 2018

information security as an intuitive perception for assessing consumer's risk. In fact, consumers' attitudes toward online purchasing seem to depend heavily on privacy and security concerns, and consumers' trust decreases when these concerns increase (McCole, Ramsey, & Williams, 2010). Cases, Fournier, Dubois, and Tanner (2010) described the indirect process whereby privacy concerns influence attitudes toward email campaigns. Our model captures the idea of consumers' trust via market signals (prices) and consumers' experiences to analytically quantify perceived privacy concerns.

Studies have investigated privacy concerns and regulation as potentially costly factors that depend on consumers. Acquisti and Varian (2005) and Conitzer, Taylor, and Wagman (2012) studied models in which consumers accessed anonymizing technologies, showing that welfare can be non-monotonic in degree of privacy.

However, investment in information security has become a significant organizational asset for companies in recent years. Some research on investment in security has focused primarily on cost savings associated with preventing cybersecurity breaches (Anderson, 2001; Gordon & Loeb, 2006; Angst, Block, D'arcy, & Kelley, 2017). In this scenario, organizations must decide which information technology (IT) security measures to invest in (e.g., Fenz, Ekelhart, & Neubauer, 2011) and how to evaluate those investment decisions (Anderson, Böhme, Clayton, & Moore, 2008). Gordon and Loeb (2002) present a model that determines the optimal amount to invest to protect a given information set. In this study, we determine the optimal level of investment, but we also consider the effects of this investment on consumers' beliefs and demand.

Few studies have provided empirical insight into how organizations make decisions regarding IT security investment. Recent studies have identified the main components of the information security investment decision-making process (e.g., Dor & Elovici, 2016; Weishäupl, Yasasin, & Schryen, 2018). As far as we know, no study has considered security investment as a way for firms to increase profits when consumers have privacy concerns. We fill this gap in the literature.

The paper is organized as follows. Section 2 reviews the most relevant literature. The model is presented in Section 3. Section 4.1 describes the firm's investment in security in our model. Section 4.2 analyzes the firm's investment in the market precision of the signal. Section 5 provides some policy remarks.

3. Theoretical framework: the baseline model

Our model is a two-period signaling game in which a monopolist and a continuum of consumers use market signals to learn about consumers' privacy concerns. We apply the classical signaling game framework to analyze the information content of prices and the market performance under imperfect information and privacy concerns.

All the consumers know their willingness to pay for the product represented by θ_i. It is a way of expressing that the product is not new and that consumers are familiar with its quality and/or characteristics. We assume that individual i purchasing for the first time has some privacy concern but does not know the precise value of these concerns, represented by α_{it}, at the time of the purchase. Consumer i's demand is given by

$$E\{\theta_i - \alpha_{it} - p_t | \Omega_{it}\}, \tag{1}$$

where Ω_{it} is consumer i 's information for period t. The privacy concerns of individual i who decides to purchase a product in period ($t = 1,2$) is represented by an index α_{it}, which is equal to

$$\alpha_{it} = \tilde{x} + \tilde{\omega}_i + \tilde{v}_{it}. \tag{2}$$

Random variables $\tilde{x}$, $\tilde{\omega}_i$ and $\tilde{v}_{it}$ represent the population-average privacy in that specific product market, the individual i's persistent deviation from that population-average privacy, and individual i's specific time deviation, respectively. The random variables have the following distributions $\tilde{x} \sim N(\bar{x}, \sigma_x^2)$, $\tilde{\omega}_i \sim N(0, \sigma_\omega^2)$ and $\tilde{v}_{it} \sim N(0, \sigma_v^2)$. Therefore, $E\{\tilde{\omega}\} = E\{\tilde{v}_{it}\} = 0$. Thus, we also assume that all of them are normally and independently distributed. Normality has the inconvenient feature of an unbounded support, which allows for negative demand and prices. However, normality also has the highly desirable feature of implying the use of linear Bayesian updating rules by consumers, which simplifies our analysis considerably.

Variable $\tilde{x}$ refers to average privacy concerns in that specific market. With the vast amount of news about the sale of personal data collected on the Internet, what are society's general concerns regarding personal information? With this random variable, we capture the idea that privacy has long been a moving target and that it continues to be so.

Variable $\tilde{\omega}_i$ captures differences between consumers. Some consumers do not care about privacy, whereas others consider privacy vital. If such a consumer realizes that some private information has been used in a harmful way, this will increase the value of α_{it}, in turn reducing consumer's utility. Variable $\tilde{v}_{it}$ is an external shock, which avoids complete learning by any market agent.

The firm receives a private signal about consumers' privacy concerns after period 1 given the amount of data disclosed and/or the cookies that have been eliminated. Specifically,

$$z = \tilde{x} + \tilde{\varphi}, \tag{3}$$

where $\tilde{x}$ represents the same random variable showing, as above, the average privacy in the market and where $\tilde{\varphi}$ is an external shock that is distributed normally $\tilde{\varphi} \sim N(0, \sigma_\varphi^2)$.

Signal z represents important information for the monopolist's second period choice. This signal is observed after first-period sales. With this particular definition of z, we can now give a more complete interpretation of $\tilde{x}$ and the random variable $\tilde{\varphi}$. Here, $\tilde{x}$ is the portion of the mean effect on the population that is detectable through z. Therefore, if $\tilde{x}$ is independent and not correlated with $\tilde{\varphi}$, then z will signal the actual population-average privacy concerns. If $\tilde{\varphi}$ were correlated, then $\tilde{x}$ would be the ex-ante expectation rather than the average privacy concerns about using this specific channel. We also assume that the unit production cost in each period is common knowledge and is normalized to zero.

The timing of the game is as follows. The market for the product opens in period 1. The monopolist decides on a price strategy and announces the first-period price. In this first period, no information is generated by any player. The monopolist has no private information, and consumers do not learn either. Therefore, the information set Ω_{i1} consists of simple expectations: the monopolist has an expected demand and the consumers have an expected privacy concern. Consumer i observes the market price and decides how much of the product to purchase given her or his privacy concern expectations. Note that at the beginning of the first period, consumers are uncertain about their privacy concerns, and they need some experience to update their information. Because it is common knowledge that the monopolist will receive a private signal about the mean privacy at the end of period 1, the consumers and the monopolist receive some new information at the beginning of period 2. In period 2, the information set is Ω_{i2}. The firm learns both $z = \tilde{x} + \tilde{\varphi}$ (i.e., the private signal about the average privacy concerns) and the first-period purchases. Both constitute the monopolist's information set in period $t = 2$. The monopolist then sets and announces its period 2 price. Consumers learn about their real privacy concerns from their purchases in the first period and from the second-period price. They are able to make an inference on z from the market price. Finally, they make a decision. The consumers' information set consists of consumers' purchase experiences, α_{i1}, and the inference made on z once the second-period price has been announced.

3.1. Updating of beliefs

Given the above information, we first calculate several Bayesian updates for future references. Because all random variables are

normally distributed, the Bayesian updates are just regression equations. First, we have the consumer's updated random variable α_{i1} once z has been observed. By normality and the parameters of the corresponding distributions,

$$E\{\alpha_{i1}|z\} = \gamma_z z + \gamma_x \bar{x}, \tag{4}$$

where

$$\gamma_z = \frac{\sigma_x^2}{\sigma_z^2}, \qquad \gamma_x = 1 - \gamma_z = \frac{\sigma_z^2 - \sigma_x}{\sigma_z^2}. \tag{5}$$

Here, γ_z is the relative precision of signal z, and γ_x is the relative precision of the prior distribution of α_{i1}. The Bayesian updating of privacy concerns in period 2, conditional on z and α_{i1}, is given by

$$E\{\alpha_{i2}|\alpha_{i1}, z\} = \bar{x}\delta_x + \alpha_{i1}\delta_\alpha + z\delta_z, \tag{6}$$

where

$$\delta_\alpha = \frac{\sigma_x^2\sigma_\varphi^2 + \sigma_\omega^2\sigma_z^2}{\sigma_\alpha^2\sigma_z^2 - \sigma_x^4},$$

$$\delta_z = \frac{\sigma_x^2\sigma_v^2}{\sigma_\alpha^2\sigma_z^2 - \sigma_x^4},$$

and

$$\delta_x = 1 - \delta_\alpha - \delta_z.$$

In these equations, $\sigma_\alpha^2 = \sigma_x^2 + \sigma_\omega^2 + \sigma_\vartheta^2$ and $\sigma_z^2 = \sigma_x^2 + \sigma_\varphi^2$. Therefore, by Eq. (5),

$$\delta_z = \gamma_z(1 - \delta_\alpha), \tag{7}$$

$$\delta_x = (1 - \gamma_z)(1 - \delta_\alpha). \tag{8}$$

Note that in period 2, the consumers' posterior distribution of α_{i2} comes from the information obtained through the purchase in period 1 and the updating of α_{i1}. In other words, it comes from consumers' experiences in period 1 and the inference made on z from the second-period price. Here, δ_α is the relative precision of the experience in period 1, γ_z is the relative precision of the signal in period 2, and γ_x is the relative precision of the prior distribution of α_{i2}. Eqs. (7) and (8) show that beliefs depend on two key parameters: δ_α and γ_z. Parameter δ_α measures how much weight consumers place on their privacy concerns regarding their purchase experiences. Parameter γ_z is the precision of the monopolist's private information (i.e., the signal precision of z).

3.2. Equilibrium analysis under privacy concerns

In this section, we analyze how the monopolist sets prices in periods $t = 1,2$ given the information Ω_t that is available in each period.

In period 1, consumers have expected demands given their set of information in period $t = 1$. As specified above, no information has yet been given to either monopolist or the consumers. Thus, consumers' expected demands and the monopolist's expected profits are, respectively:

$$E[q_{i1}|\Omega_{i1}(\alpha_{i1})] = \theta_i - \bar{x} - p_1,$$

$$E[\Pi_1|\Omega_1(\alpha_1)] = (\theta_i - \bar{x} - p_1)p_1. \tag{9}$$

Now consider the equilibrium in period 2. In this equilibrium, the monopolist's second-period price is a linear function of the monopolist's private information. The first step when computing the perfect Bayesian equilibrium is to specify exactly what consumer i believes when he or she decides to purchase the product for any possible information set, Ω_{i2}. A consumer's information set at the beginning of period 2 consists of the consumer's own experience regarding α_{it} plus the commonly observed p_2, which might indicate the monopolist's observation of z. Suppose consumers make inferences on z from p_2 following Bayes according to the linear rule $z = a + bp_2$.

The expected demand in period 2 of consumer i is,

$$E[q_{i2}|\Omega_{i2}(\alpha_{i1}, p_2)] = \theta_i - E\{E\{\alpha_{i2}|\alpha_{i1}, z\}|\alpha_{i1}, p_2\} - p_2,$$

which specifies to,

$$E[q_{i2}|\Omega_{i2}(\alpha_{i1}, p_2)] = \theta_i - E\{\bar{x}\delta_x + \alpha_{i1}\delta_\alpha + z\delta_z|\alpha_{i1}, p_2\} - p_2,$$

and therefore,

$$E[q_{i2}|\Omega_{i2}(\alpha_{i1}, p_2)] = \theta_i - \{\bar{x}\delta_x + \alpha_{i1}\delta_\alpha + (a + bp_2)\delta_z\} - p_2.$$

After period 1, the monopolist gets some information about average privacy. The monopolist uses this information to set the second-period price. Therefore, the monopolist's second-period expected demand is

$$E[q_2|\Omega_2(\alpha_{i2}, z)] = (\theta_i - E\{\bar{x}\delta_x + \alpha_{i1}\delta_\alpha + z\delta_z|z\} - p_2),$$

Using the expectations already discussed and Eq.(8), the expected demand curve faced by the monopolist is

$$E[q_2|\Omega_2(\alpha_{i2}, z)] = (\theta_i - (\bar{x}\gamma_x + \delta_z(a + bp_2) + z\delta_\alpha\gamma_z) - p_2).$$

Thus, the monopolist's second-period expected profits are,

$$E[\Pi_2|\Omega_2(\alpha_{i2}, z)] = ((\theta_i - (\bar{x}\gamma_x + \delta_z(a + bp_2) + z\delta_\alpha\gamma_z) - p_2))p_2. \tag{10}$$

The equilibrium concept is a perfect Bayesian equilibrium, which specifies here as a *noisy signaling equilibrium*, and consists of the monopolist's price in each period given the information set Ω_t in periods $t = 1,2$, the consumers' expected demand from the consumers' utility maximization given the information set Ω_{it} in periods $t = 1,2$, and the posterior beliefs of both the consumers and the monopolist. In equilibrium, the posterior beliefs are consistent with Bayes' rule and equilibrium prices.

Definition 1. The tuple $(p_1^*(E[\Pi_1|\Omega_1(\alpha_1)]), p_2^*(E[\Pi_2|\Omega_2(\alpha_{i2}, z)]), z = a + bp_2)$ is a noisy signaling equilibrium if

1 Given $E[\Pi_1|\Omega_1(\alpha_1)]$ in period $t = 1$ and $E[\Pi_2|\Omega_2(\alpha_{i2}, z)]$ in t = 2, the firm's price strategy for the first period is

$$p_1^*(E[\Pi_1|\Omega_1(\alpha_1)]) = \arg\max_{p_1} \{(\theta_i - \bar{x} - p_1)p_1\}, \tag{11}$$

and the firm's price strategy for the second period is

$$p_2^*(E[\Pi_2|\Omega_2(\alpha_{i2}, z)]) = \arg\max_{p_2} E[q_2|\Omega_2(\alpha_{i2}, z)]p_2. \tag{12}$$

2 Given consumers' prior beliefs α_{it} and consumers' information set Ω_{it} in each period $t = 1,2$, consumers maximize their utility and decide how much to purchase once the monopolist's prices have been announced.

3 Consumers' posterior beliefs upon observing the second period price are computed by the Bayesian updating rule.Proposition 1 characterizes the noisy signaling equilibrium.

Proposition 1. *There exists a noisy signaling equilibrium. In equilibrium,*

1 *The firm sets the price in period t = 1*

$$p_1^* = \frac{\theta_i - \bar{x}}{2}.$$

2 *Since the ex-ante expected price in the second period is*

$$p_2^* = \frac{\theta_i - z\delta_\alpha\gamma_z - a\delta_z - \bar{x}\gamma_x}{2(1 + b\delta_z)}, \tag{13}$$

and in a linear equilibrium

$$a = \frac{\theta_i - \bar{x}\gamma_x}{\gamma_z}, \tag{14}$$

and

$$b = \frac{2}{(\delta_\alpha - 2)\gamma_z}, \tag{15}$$

then the second period expected price and profits are, respectively,

$$p_2 = \frac{1}{2}(2 - \delta_\alpha)(\theta_i - \bar{x}\gamma_x - z\gamma_z), \tag{16}$$

$$\Pi_2 = \frac{1}{4}(2 - \delta_\alpha)\delta_\alpha(\theta_i - \bar{x}\gamma_x - z\gamma_z)^2. \tag{17}$$

The second period price is indeed a linear function of signal z. As indicated above, the key parameters of the model are δ_α and γ_z. Some remarks should be made here. First, signaling distorts price upward on average. Second, the price in period 2 increases as long as the precision of the signal increases too. Thus, the derivative with respect to the precision of the signal z is positive: $\frac{\partial P_2^*}{\partial \gamma_z} > 0$. However, the opposite occurs when consumers' privacy experiences, δ_α, are considered. When consumers attach greater importance to their experiences, the price in period 2 is lower: $\frac{\partial P_2^*}{\partial \delta_\alpha} < 0$.

These remarks highlight two lines of action for the monopolist to increase profits. One option is for the monopolist to try to manipulate consumers' experiences in period 1. We address this option in the next section through investment in security in period 1. Alternatively, the monopolist could use market signal precision to manipulate consumers' beliefs. We address this possibility in Section 4.2.

4. Calculations: privacy and security

Many real-world examples show that security and privacy in the digital market are unresolved issues. Until recently, consumers paid for online security in the form of software and antivirus packages. These packages guaranteed them protection against viruses and other digital intrusions. Nowadays, privacy has become the responsibility of firms, which seek security in digital markets. Newspapers have reported the vulnerability, data hacking, and data theft of consumer information. The onus in terms of who must pay for security investment has shifted noticeably from consumers to firms in recent years.

Companies are aware that guaranteeing security, privacy, and trust is the key to success in digital markets. Firms like Apple and Facebook constantly publicize their efforts and commitment in this area.[3,4] Signaling this commitment has become a basic requirement.

4.1. Private investment

The following set-up presents a simple model of security investment by a monopolist. The monopolist may invest in privacy measures in the first period. The effect of this investment is reflected by consumer *i's* computation of expected privacy concerns in period 1 (α_{i1}), represented by the parameter s_1. This parameter affects the first-period utility of consumers' expected privacy concerns. However, while it does not directly affect consumer *i's* utility in the second period, it does affect second-period demand due to the inference by consumers. As in the baseline model, α_{it} is given by

$$\alpha_{i1} = \tilde{x} + \omega_i + \nu_{1t} - s_1,$$

where s_1 diminishes consumers' overall privacy concerns because of investment in security to protect consumers' personal data. The cost of that investment is $c\frac{s_1^2}{2}$, where $c > 0$. In this section, we assume that γ_z is fixed and is common knowledge. In other words, market signal precision is known by all the participants in the market.

The next step in our analysis is to adjust the period 2 expectations formulae to reflect the consumers' beliefs about privacy once the security investment s_1^e has been made. They become

$$E\{\alpha_{i1}|z\} = \gamma_z z + \gamma_x \bar{x} - s_1^e,$$

and

$$E\{\alpha_{i2}|\alpha_{i1}, z\} = \bar{x}\delta_x + (\alpha_{i1} + s_1^e)\delta_\alpha + z\delta_z. \tag{18}$$

Therefore, the new expected demand faced by the monopolist in period 2 is

$$E[q_2^s|\Omega_2(\alpha_{i2}, z)] = \theta_i - (\delta_\alpha(s_1^e - s_1) + z\delta_a\gamma_z + \delta_z(a + bp_2) + \bar{x}\gamma_x) - p_2,$$

and the monopolist's expected profits in period 2 are

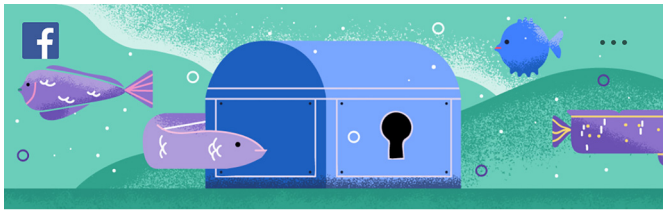
$$E[\Pi_2^s|\Omega_2(\alpha_{i2}, z)] = (\theta_i - (\delta_\alpha(s_1^e - s_1) + z\delta_a\gamma_z + \delta_z(a + bp_2) + \bar{x}\gamma_x) - p_2)p_2.$$

4.1.1. Results and discussion

With the new expectation formulae, the equilibrium when there is investment in security consists of the monopolist's price strategies in period $t = 1,2$, $p_1^{s*}(E\{\alpha_{i1}\})$ and $p_2^{s*}(E\{\alpha_{i2}|\alpha_{i1}, p_2^s\}, E\{\alpha_{i2}|\alpha_{i1}, z\})$, the optimal level of investment s_1, and the Bayesian beliefs, which take the following linear form $z = a + bp_2^s$.

Proposition 2. *There exists a noisy signaling equilibrium. In equilibrium,*

1 *The firm sets the price in period* $t = 1$



Nuestros equipos de seguridad trabajan 24 horas al día para proteger tu información

Mariola, queremos que sepas lo que hacemos para proteger tu información cada vez que usas Facebook. La seguridad de tu cuenta es importante para nosotros, por lo que nuestros equipos de seguridad encuentran y detectan los problemas antes de que afecten a tu cuenta. Te avisaremos si observamos algo inusual.

— El equipo de ayuda de Facebook

Más información sobre nuestras funciones de seguridad

Fig. 1. Example. Facebook's notification in a profile in Spanish. "Our security team works 24 hours a day in order to protect your information".

[3] https://www.apple.com/apples-commitment-to-customer-privacy/.

[4] This is an example of how Facebook reminds users of (i.e., sends signals) of its commitment to security. See Fig. 1.

Table 1
A numerical example.

	$\delta_\alpha = \gamma_z = 0.5$	$\delta_\alpha = 0.9;\gamma_z = 0.1$	$\delta_\alpha = 0.1;\gamma_z = 0.9$	$\delta_\alpha = 0.9;\gamma_z = 0.9$	$\delta_\alpha = 0.1;\gamma_z = 0.1$
Period 1					
p_1	2.08	2.08	2.08	2.08	2.08
CS_1	2.08	2.08	2.08	2.08	2.08
Π_1	4.33	4.33	4.33	4.33	4.33
Period 2					
p_2	3.21	2.30	4.16	2.41	3.97
CS_2	1.07	1.88	0.22	1.97	0.21
Π_2	3.43	4.33	0.91	4.74	0.83
Period 1(Security investment)					
p_1^s	3.44	3.55	2.75	3.56	2.75
CS_1^s	0.72	0.60	1.41	0.60	1.41
s_1^*	2.71	2.96	1.34	2.96	1.34
Π_1^s	9.97	10.49	7.11	10.49	7.11
$CS_T^{NI} = CS_1 + CS_2$	3.15	3.96	2.30	4.05	2.29
$CS_T^I = CS_1^s + CS_2$	1.79	2.48	1.63	2.57	1.62
$\Pi_T = \Pi_1 + \Pi_2$	7.76	8.66	5.24	9.07	5.16
$\Pi_T^s = \Pi_1^s + \Pi_2$	13.40	14.82	8.02	15.23	7.94
SW^{NI}	10.91	12.62	7.53	13.12	7.45
SW^I	15.20	17.30	9.65	17.80	9.56
$\%\triangle SW$	39.3%	37.1%	28.1%	35.7%	28.4%
$\%\frac{s_1}{\Pi_T^s}$	20.2%	20.0%	16.7%	19.5%	16.9%

$\theta_i = 5$; $\bar{x} = 0.84$; $z = 0.60$

$$p_1^{s*} = \frac{1}{2}(\theta_i - (\bar{x} - s_1)).$$

2 *Since the second period ex-ante expected price is*

$$p_2^{s*} = \frac{\theta_i - z\delta_\alpha\gamma_z - a\delta_z - \bar{x}\gamma_x}{2(1 + b\delta_z)}, \tag{19}$$

and in a linear equilibrium

$$a = \frac{\theta_i - \bar{x}\gamma_x}{\gamma_z}, \tag{20}$$

and

$$b = \frac{2}{(\delta_\alpha - 2)\gamma_z}, \tag{21}$$

then the second period expected price and expected profits are, respectively,

$$p_2^{s*} = \frac{1}{2}(2 - \delta_a)(\theta_i - \bar{x}\gamma_x - z\gamma_z), \tag{22}$$

$$\Pi_2^{s*} = \frac{1}{4}(2 - \delta_\alpha)\delta_\alpha(\theta_i - \bar{x}\gamma_x - z\gamma_z)^2. \tag{23}$$

3 *Using the expressions for a and b, the effect of the investment on consumers' beliefs about the general security in period 2 (δ_α), and the cost of privacy to the monopolist yields the following first-order condition for s_1, taking expectations over z:*

$$s_1^* = \frac{(2 - \delta_\alpha)\delta_\alpha(\theta_i - \bar{x})}{2c}. \tag{24}$$

At the equilibrium, beliefs are correct (i.e., $s_1 = s_1^e$), so it is optimal for the monopolist to invest the amount s_1^*, specified in Eq. (24), for a cost c. The optimal level of investment in period 1, s_1^*, is a decreasing function of cost.

The main findings of the model are the following:

1. The optimal level of investment increases with the consumers' experience, δ_α.
2. The expected price in period 1 is the only price affected by the firm's investment in period 1. It does not affect the expected price in period 2. Moreover, the expected price in the first period with investment in security is higher than the expected price without investment (see Section 4). Thus, $p_1^s > p_1$. The firm transfers the cost of security investment to consumers through price.

The interesting feature of this solution is that even though the security investment does not affect the consumer's second-period utility, the firm still makes the investment. This is because the marginal first-period investment affects each consumer's inference about the individual specific valuation, δ_α, which increases confidence and therefore second-period demand.

To illustrate our results, we provide a numerical example. It is not feasible to find real budgetary data on IT security investment, so we make some assumptions. We assume that the willingness to pay for a product is known to be 5 monetary units. We take the average privacy concern in the market $\bar{x} = 0.84$, from the estimated privacy parameter in Eastlick, Lotz, and Warrington (2006). Similarly, the realization of the firm's signal observation, z, is taken to be 0.60. Finally, we assign different values to the key parameters of the model δ_α (consumers' experiences) and γ_z (relative precision of signal z).

Table 1 first presents the scenario in which there is no investment in security, where CS_1 and CS_2, and Π_1 and Π_2, are the consumer surplus and the firm's profits in periods 1 and 2, respectively. Second, Table 1 presents the scenario in which there is investment in security in period 1. Finally, CS_T^{NI}, CS_T^I, SW_T^{NI} and SW_T^I show the sum of period 1 and period 2 consumer's surplus and social welfare with no investment in security (identified by superscript NI) and with investment in security (identified by the superscript I), respectively.

The following remarks derived from the data in Table 1 reinforce the model results:

1. The greater consumers' experience, δ_α, is, the higher the optimal investment in security s_1* will be.
2. Prices in period 1 are higher with security investment than without investment. This results in higher profits for the firm in period 1 and lower consumer surplus. Nevertheless, social welfare is still higher than without security investment.
3. Interestingly, the percentage of security investment is 16%–20% of the sum of period 1 and period 2 profits. This may seem a sizeable investment, but it is by no means unrealistic. Indeed, according to Karpersky,[5] an international company that specializes in IT security, almost a quarter (23 %) of IT budgets in large companies is spent on IT security, and this amount is expected to grow. Businesses are starting to view this investment as strategic. Our model shows the benefits of doing so.

4.2. Endogenous precision

In the previous section, we analyzed the level of investment that the monopolist must make to increase its expected profits. By achieving the optimal level of investment, the monopolist seeks to improve consumers' experiences in the first period by increasing consumers' confidence. Here, the approach is different. In this section, the monopolist sets a specific level of market signal precision, γ_z. The choice of signal precision allows the monopolist to manipulate the information received by consumers.

We now assume that the monopolist chooses the precision of its information (i.e., γ_z is endogenous). More specifically, we hold σ_x^2 constant and assume that the monopolist determines γ_z by an implicit choice of σ_φ^2, as Eq. (5) shows. The monopolist receives its private signal without any kind of noise. This could be the case if the firm conducted a prior market study or big data analysis. We determine the equilibrium level of γ_z under various specifications of the informational and regulatory environment. To focus on the optimal choice of γ_z, we assume that there is no period-one investment. For expositional clarity, we assume that γ_z is chosen at some initial time prior to the introduction of any specific good.

The cost of achieving precision γ_z is $c(\gamma_z)$. We assume that $c(\cdot)$ is increasing and convex such that $c(1) = c'(1) = \infty$ and $c(0) = c'(0) = 0$. Because $\gamma_z = 1$ corresponds to the situation in which the monopolist has perfect information about $\bar{x}$, it is natural to assume that the total and marginal cost of eliminating the last bit of uncertainty is infinite. Because $\gamma_z = 0$ corresponds to no information, it is reasonable to assume that the marginal cost of the first bit of information is zero. These assumptions yield interior solutions to the monopolist's choice of γ_z.

The monopolist's choice of precision is not observable by consumers. Therefore, consumers form some point expectation of γ_z, whose value will determine their point beliefs about the regression coefficients δ_α and δ_z. These coefficients generate consumers' predictions about the information quality of z. We denote consumers' (common) beliefs about the monopolist's information quality by γ_z^e. These beliefs translate into beliefs about the values of δ_α and δ_z, which we denote by δ_α^e and δ_z^e. They, in turn, determine the period-2 coefficients, a and b, of the consumers' period 2 inference rule, $z = a + bp_2$.

4.2.1. Results and discussion

The firm's expectation of α_{it} is conditional on z and depends on the true value of γ_z. Given consumer beliefs about γ_z and the resulting inference parameters, the expected demand function perceived by the monopolist in period 2 is

$$E[q_2^e|\Omega_2(\alpha_{i2}, z)] = \theta_i - (\delta_\alpha^e\gamma_z z + \delta_z^e(a + bp_2^e) + \bar{x}(1 - \delta_\alpha^e\gamma_z - \delta_z^e)) - p_2^e, \tag{25}$$

and given that the firm knows γ_z, then $E[\alpha_{i1}|z] = \gamma_z z + (1 - \gamma_z)\bar{x}$.

Solving for the profit-maximizing price and substituting into the profit function, period 2 expected profit conditional on z is given by

$$\Pi_2^e = \frac{(\theta_i + \bar{x}(\gamma_z\delta_\alpha^e + \delta_z^e - 1) - a\delta_z^e - z\gamma_z\delta_\alpha^e)^2}{4(1 + b\delta_\alpha^e)}. \tag{26}$$

Hence the firm chooses γ_z to maximize $E\{\Pi_2^e\} - c(\gamma_z)$, where the expectation is taken over z because γ_z is chosen ex ante.[6]

The first-order condition of the monopolist's problem is

$$c'(\gamma_z^e) = \frac{\gamma_z^e\sigma_z^2(\delta_\alpha^e)^2}{2(1 + b\delta_z^e)}. \tag{27}$$

Note that $c'(\gamma_z^e)$ is positive and is indeed the marginal profit of the information precision. It is simple to show that the second-order condition is satisfied. The optimal level of γ_z is

$$\gamma_z^* = \frac{2c(\gamma_z)}{(2 - \delta_\alpha^e)\delta_\alpha^e\sigma_z^2}. \tag{28}$$

The optimal value of the information precision is a negative function of consumers' experiences. In Bayes Nash equilibrium, consumers' beliefs are correct. This implies that $\gamma_z^e = \gamma_z$, $\delta_\alpha^e = \delta_\alpha$, and $\delta_z^e = \delta_z$, where γ_z^e denotes the equilibrium value of γ_z when the monopolist's choice of γ_z is unobservable. Thus,

Proposition 3. *At equilibrium, the optimal precision choice is*

$$\gamma_z^* = \frac{2c(\gamma_z)}{(2 - \delta_\alpha)\delta_\alpha\sigma_z^2}. \tag{29}$$

To interpret our results, we should note that Eq. (29) can be written as marginal revenues by equating marginal costs:

$$c'(\gamma_z) = \frac{1}{2}(2 - \delta_\alpha)\delta_\alpha\sigma_x^2. \tag{30}$$

Fig. 2 plots the monopolist's marginal revenues as a function of consumers' experiences (a) and as a function of the value of the signal's precision (b).

The monopolist finds it profitable to choose to invest in market signal precision because the monopolist's marginal revenue of doing so, given cost $c(\gamma_z)$, is positive.

Given the potential marginal revenue of investing in the signal's precision, an incentive to manipulate arises as follows:

1. First, as Fig. 2 (a) shows, the monopolist's marginal revenue, and therefore expected profits, increases with consumers' experience, δ_α.
2. Second, as Fig. 2 (b) shows, marginal revenue, and therefore expected profits, decreases with signal precision, γ_z.
3. The monopolist can signal a specific value of precision to make consumers believe that precision is worse than it really is. By doing so, the monopolist increases consumers' trust in the online market, thereby increasing consumers' market demand.

These results also show an interesting trade-off between the level of expected price and expected demand in period 2. This trade-off is due to the negative relationship between the market signal, γ_z, and the parameter that measures the weight of experience, δ_α. Whereas expected price increases with the market signal, the effect is the opposite with respect to the expected demand. If the monopolist manipulates the market signal precision, consumers will pay more attention to their own experience and less to the market signal. This shift in attention

[5] Full text available on https://www.kaspersky.com/about/press-releases.

[6] Note that z is squared in (26), so $E\{z^2\} = \bar{x}^2 + \sigma_z^2$.

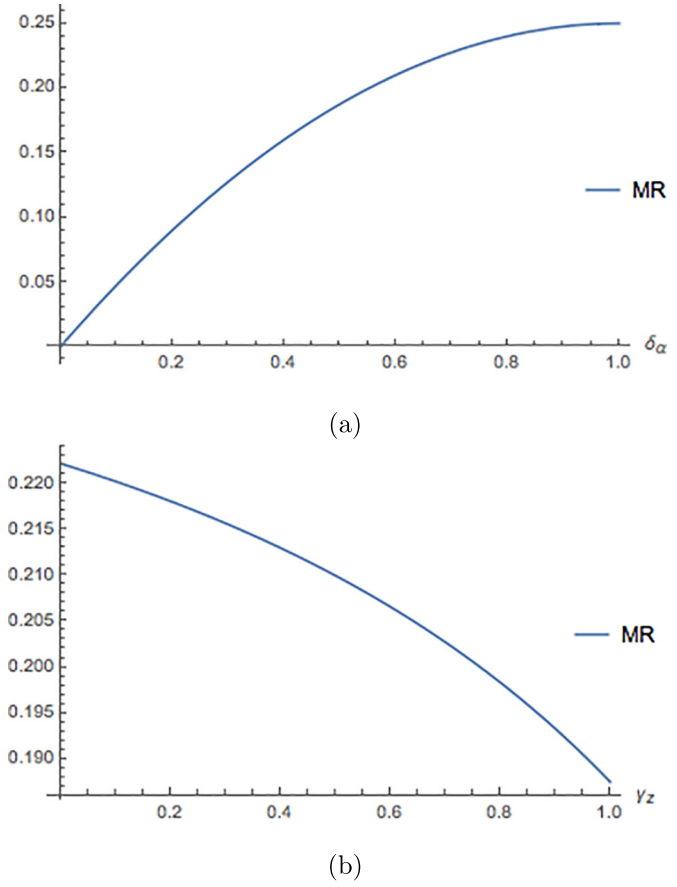


Fig. 2. Marginal revenues depending on γ_z and δ_α.

increases expected demand, q_2^e, for the monopolist and results in a lower expected price, p_2^e, than when there is an absence of manipulation. The optimal choice is the one that increases the monopolist's expected profits, so the demand effect dominates the price effect. According to our results, the monopolist has an incentive to create less confidence in the market signal (the public signal) and more in the consumers' individual experiences (the private signal).

5. Conclusions and policy remarks

Comparing the two investment approaches reveals several implications for consumers. First, the direct investment in security in period 1 results in a transfer of the cost directly to consumers through price. Second, investment in signal precision transfers the control of information in the market to the monopolist. This transfer influences both demand and expected prices. In this scenario, the monopolist obtains higher profits by increasing expected demand, which implies a lower price in period 2 (i.e., prices are lower than in the absence of investment in period $t = 2$). We therefore conclude that it would be preferable to grant the monopolist a certain power of information because doing so would result in lower prices.

The European Union addresses cybersecurity failures in systems and organizations as a key topic in the Horizon 2020 Project. The construction of the Digital Single Market requires the necessary tools to fight cybercrime and consistently guarantee cybersecurity. Recently, the General Affairs Council (GAC) announced its commitment to tightening cybersecurity. Incentivizing investment in cybersecurity is a precondition for the construction of the Digital Single Market.[7]

Subsidizing security costs to benefit from their economic effect on the market and consumers is still economically controversial. For example, in our model, the firm can take two directions in its investment efforts. Subsidizing the cost of security suggests the need for a clear economic policy on firms' behavior.

1. Investment in cybersecurity tools only makes sense if it is done continuously under strict regulation. If it lasts for only short periods and there is little control, traditional monopolies or oligopolies with significant market power will return and will transfer security costs back to consumers. The data in Table 1 indicate that a security investment of around 20% of profits resulted in an increase of almost 40% in prices in period 1.
2. If the subsidy helps firms maintain control of consumers' information, strategic advantages for the firm, such as big data analysis, may emerge. Security measures may lead to market manipulation and the abuse of position by firms.

References

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economics Literature, 54*(2), 442–492.
Acquisti, A., & Varian, H. R. (2005). Conditioning prices on purchase history. *Marketing Science, 24*(3), 367–381.
Anderson, R. (2001). Why information security is hard. *Annual Computer Security Applications Conference*.
Anderson, R., Böhme, R., Clayton, R., & Moore, T. (2008). *Security economics and the internal market. Study commissioned by ENISA*.
Angst, C. M., Block, E. S., D'arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of Healthcare data breaches. *Mis Quarterly, 41*(3).
Calzolari, G., & Pavan, A. (2006). On the optimality of privacy in sequential contracting. *Journal of Economic Theory, 2*(2), 168–204.
Cases, A. S., Fournier, C., Dubois, P. L., & Tanner, J. F., Jr. (2010). Web Site spill over to email campaigns: The role of privacy, trust and shoppers' attitudes. *Journal of Business Research, 63*(9-10), 993–999.
Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*(5/6), 358–368.
Chen, Y., & Zhang, Z. J. (2009). Dynamic targeted pricing with strategic consumers. *International Journal of Industrial Organization, 27*(1), 43–50.
Conitzer, V., Taylor, C. R., & Wagman, L. (2012). Hide and seek: Costly consumer privacy in a market with repeat purchases. *Marketing Science, 31*(2), 277–292.
Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers & Security, 63*, 1–13.
Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research, 59*(8), 877–886.
Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information security risk management: In which security solutions is it worth investing? *CAIS, 28*, 22.
Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438–457.
Gordon, L. A., & Loeb, M. P. (2006). Budgeting process for information security expenditures. *Communications of the ACM, 49*(1), 121–125.
McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research, 63*(9-10), 1018–1024.
Montes, R., SandZantman, W., & Valletti, T. M. (2015). *The value of personal information in markets with endogenous privacy*.
Taylor, C. R. (2004). Consumer privacy and the market for customer information. *The RAND Journal of Economics, 35*(4), 631–650.
Taylor, C., & Wagman, L. (2014). Consumer privacy in oligopolistic markets: Winners, losers, and welfare. *International Journal of Industrial Organization,* 80–84.
Villas-Boas, J. M. (2004). Price cycles in markets with customer recognition. *The RAND Journal of Economics, 35*(3), 486–501.
Weishäupl, E., Yasasin, E., & Schryen, G. (2018). An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security, 77*, 807–823.

[7] http://www.consilium.europa.eu/es/press/press-releases/2017/11/20/eu-to-beef-up-cybersecurity/pdf.