Privacy Protection*

Bruno Jullien†, Yassine Lefouili‡and Michael Riordan§

May 30, 2016

Very preliminary version, please do not circulate

Abstract

We study the incentives of a website to sell its customers' personal information. Third parties buying that information can bring either benefits or harm to consumers, who learn their vulnerability to malicious third parties through experience. The cost of selling information is the risk that bad experience leads consumers to end their relationship with the website. The privacy policy is not contractible but the website may decide to be cautious by not selling personal information or may spend resources to screen harmful third parties from access to customer information. We characterize the equilibrium and its welfare properties. We then discuss implications for policy rules.

Keywords: Privacy, learning, reputation, security, Internet.

*We acknowledge financial support from the Orange/IDEI partnership and the Digital Society Initiative.

†Toulouse School of Economics, University of Toulouse Capitole. E-mail: bruno.jullien@tse-fr.eu

‡Toulouse School of Economics, University of Toulouse Capitole. E-mail: yassine.lefouili@tse-fr.eu

§Columbia University. E-mail: mhr21@columbia.edu.

1 Introduction

Should firms' privacy policy be regulated? The optimistic view contends that market forces have a disciplining effect on firms: those who would not adopt a privacy policy in line with consumer preferences would make less profits. The other polar view is that regulation is necessary: public authorities should define privacy rules that firms must comply with.

This paper contributes to the current debate on regulation of privacy by investigating whether a repeated interaction between a website and its customers could generate incentives to protect their personal data. We build a two-period model in which consumers learn about the value of visiting the website, and this learning process can be altered by the website's actions. We use this model to study the website's incentives to protect its customers' personal data under a *laissez-faire* policy and compare them to the corresponding social incentives.

More precisely, we consider a website that offers a service for free to consumers and derives revenues from banner advertising (or another activity that does not raise privacy concerns). In addition to this source of revenue, the website can also sell the information acquired on its customers to a third party. Third parties can be either *good* or *malicious*. A good third party uses a customer's information to offer her a service that yields a positive utility, while a malicious third party generates a negative utility in case of intrusion, which happens with a probability θ that captures consumer vulnerability. Before selling the information, the website can decide to inspect the third party and find out its type.

We assume that each consumer can be either highly vulnerable ($\theta = \theta_h$) or weakly vulnerable ($\theta = \theta_l$), and that this characteristic is unknown to all. The website interacts with consumers over two periods. At the end of the first period, a consumer revises her beliefs about her vulnerability according to whether it experienced an interaction with a good third party, an intrusion by a malicious third party, or nothing.

We define the degree of precaution as the probability that an uninspected third party is denied access to customer information, and the level of inspection as the inspection cost below which the website inspects the third party to find out its nature. This two elements constitute the website's strategy.

We fully characterize the equilibrium when the website cannot commit to its strategy. It turns out that the website would like to commit to a lower degree of precaution than the equilibrium one if it were able to do so. Moreover, we establish that the website would benefit from committing to a reduction (resp. increase) of the level of inspection if the value of information (to a third party) is small (resp. large) enough.

We also show that the short-term (i.e. first-period) consumer surplus increases with the degree of precaution if a consumer's expected utility from interacting with a third party is negative, while the long-term consumer utility decreases with the degree of precaution. Moreover, the short-term consumer utility increases with the inspection level, while the long-

term utility increases (resp. decreases) with the inspection level if the value of information is small (resp. large) enough. As a result, if the value of information is sufficiently small, there is a conflict of interest between the website and the consumers regarding the level of inspection.

Finally, we study the effect of an opt-out policy. More specifically, we allow consumers to refuse that the website sells their information and assume that the website always prefers that consumers do not opt out. We suppose that consumers do not find it optimal to opt out in the first period. However, after revising their beliefs at the end of that period, they can choose to opt out in the second period. We investigate how this affects the website's equilibrium strategy. In particular, in the scenario in which any intrusion in the first period triggers an opt in the second period, we show that imposing an opt-out policy on websites eliminates their incentives to inspect third parties but raises the degree of precaution they choose.

TO BE COMPLETED

2 Baseline model

We consider a website facing a population of unit mass of consumers for two periods: today (period 0) and tomorrow (period 1). The service offered to consumers is free and the website obtains an exogenous revenue a per consumer derived from activities that do not raise any privacy concerns (e.g. banner advertising). Moreover, during period 0, the website acquires information on the consumer and may sell it to a third party. We will develop alternative interpretations for this information, but to fix ideas, let us think of the information as being the consumer's address (and of course the fact that she consumes the service). A third party may then buy this information and contact the consumer to offer a service of positive value U_G. The problem is that the third party may also be malicious and use instead the information in other ways that cause damages with probability θ to consumers, generating a utility $U_B << 0$. To be more precise, a third party arrives with probability β. It is non-malicious (G) with probability λ and malicious (B) with probability $1-\lambda$. With some probability α, the third party obtains the consumer's information from other sources and doesn't need to buy it from the website.[1] With probability $1-\alpha$, the third party has to buy it if it wants to get access to it. Before selling the information, the website can decide to inspect the third party and find out its type (with certainty). The cost of inspection is a random variable z with cumulative distribution function F.

Each consumer may be highly vulnerable to intrusion, denoted $\theta = \theta_h$, or weakly vulnerable, denoted $\theta = \theta_l$. The parameter θ is unknown to all and we denote by r_0 the ex-ante probability of being weakly vulnerable. As we will see, vulnerability may have different interpretations depending on the context. A consumer obtains a direct utility u from the service

[1] Later on, we may assume that α depends on the type.

offered by the website. For now we assume that u is homogenous within the population and large enough for all consumers to participate in period 0.

The non-malicious party obtains a value v_0 when using the information while the malicious party obtains value $\tilde{v}_0$ from a successful intrusion. We assume that the parameters of the model are such that:

i) it is never optimal for the website to set a price above v_0, i.e the proportion of malicious parties is sufficiently low;

ii) the value $\tilde{v}_0$ is such that the malicious party is willing to pay v_0.

With these assumptions, the strategy of the website has only two components. First, the website decides to inspect or not (depending on the realization of z). If the website inspects, it sells the information at price v_0 if the third party's type is G and does not sell it if it is B. If it doesn't inspect, the website decides to sell the information at price v_0 or not. Notice that the website will consider inspecting the third party only if it intends not to sell the information to a malicious third party.

During period 0, the consumer observes whether she is contacted by a non-malicious third party (event G), whether it is subject to intrusion by a malicious third party (event B) or whether nothing happens (event $\emptyset$). In this model, nothing happens when there is no third party (which happens with probability $1-\beta$) but also when access to information is denied or when it is obtained by a malicious party but intrusion fails. This implies that the consumer learns about its vulnerability θ by observing the realized event. At the end of the period, the consumer hence revises its beliefs about θ based on new information. Let us denote by r_1 the updated probability that $\theta = \theta_l$.

In this model, vulnerability can be interpreted in two ways. One interpretation is that some consumers are not interesting targets for a malicious third party so that it renounces to intrude after observing the individual's characteristics. This may be the case for instance if third parties generate intrusive advertising. Another interpretation is that some consumers are better protected against aggressive intrusion, for instance because they have a better antivirus, so that intrusion by malicious third-parties is more likely to fail.

Period 1 is a summary for all future interactions. We capture the future by the probability that the consumer returns to the website in period 1, and the period 1's value of the consumer for the website. The probability to retain the consumer depends on her revised beliefs r_1 and is denoted $Q(r_1)$, assumed to be increasing in r_1. The discounted value of the website from a consumer's future participation is denoted V_1. As a simplification, we assume that value V_1 does not depend on r_1.

For the purpose of evaluating welfare, we define $U_1(r_1)$ as the expected discounted surplus of consumers at the end of the period for posterior beliefs r_1, and assume that it is increasing in r_1. This function reflects the future utility accounting for optimal adjustment of future

behavior (in particular choice of participation) to the information received during the current period. As a general property of decision with acquisition of information, we impose that U_1 is convex.[2]

A special case of particular interest is the scenario in which the situation in period 0 is repeated in period 1, where the value of access by a non-malicious party is v_1 and the consumer's utility is a random variable $\tilde{u}_1$. Then it is immediate that the website does not inspect in period 1 and sells the information at price v_1 (as there is no future in the relationship with consumers). The value V_1 is then equal to $\delta^F (a + v_1)$ where δ^F is the discount factor of the firm, while the retention rate is

$$Q(r_1) = \Pr\{\tilde{u}_1 + M_1(r_1) > 0\},$$

where

$$M_1(r_1) \equiv \beta(1-\alpha)\lambda U_G + \beta(1-\alpha)(1-\lambda)(r_1\theta_l + (1-r_1)\theta_h) U_B$$

is the consumer benefit from second-period matching, increasing in r_1. The expected future utility depends on the posterior r_1 at the end of the period and is given by

$$U_1(r_1) = \delta^C \int_{-M_1(r_1)}^{+\infty} (1 - G(s))\, ds.$$

where δ^C is the consumers' discount factor.

3 Preliminaries

3.1 Strategies

In this model a strategy for the website consists of a mapping $\phi(z)$ between the inspection cost z and the binary decision to inspect or not, as well as the probability X of not selling the information in case there is no inspection. Without loss of generality, we assume that the probability X does not depend on z.

Moreover, it is immediate that if the website is indifferent between inspecting or not at cost z, it strictly prefers to inspect at any cost strictly below z. Hence there must exist a critical level Z (potentially zero) such that the website inspects if $z < Z$ and not if $z > Z$. Thus we may characterize an equilibrium by a pair

$$(X, Z) \in [0,1] \times \mathbb{R}_+.$$

[2] See Blakwell's analysis of information.

We will say that we have a pure-strategy equilibrium if $X \in \{0,1\}$ and a mixed-strategy equilibrium otherwise.

As we can see, the privacy policy has two dimensions. When the website chooses $X = 1$, it blocks by default the access to consumer information and sells it only if the third party is identified as non-malicious. When it chooses $X = 0$, the default is to sell the information and access is denied only if the third party is identified as malicious. We will refer to X as the (degree of) *precaution*. Moreover, we will say that the policy $X = 1$ captures a *strong privacy* (protection) and the policy $X = 0$ is referred to as *weak privacy* (protection).

Under strong privacy, the consumer cannot be exposed to malicious content and inspection is a way to raise the value. The variable Z determines the benefits from allowing access to non-malicious parties and is referred to as the *level of inspection*. On the contrary, in the case of a weakly protective policy, inspection avoids malicious parties and thus determines the level of protection against malicious parties.

If in addition to $X = 1$, there is no inspection, we will say the the website adopts a *full privacy* policy, meaning that it never sell the information. On the opposite, if the website always sells the information ($X = Z = 0$) we say that the website has a *no privacy* policy.

3.2 Outcomes

If the website adopts a strategy (X, Z), the probability that a malicious third-party acquires customer information is given by

$$\pi_M(X,Z) = \beta\,(1-\lambda)\,\{\alpha + (1-\alpha)\,(1-X)\,[1-F(Z]]\}$$

and the probability that no third-party acquires customer information is

$$\pi_N(X,Z) = 1-\beta+\beta\,(1-\alpha)\,\{(1-\lambda)\,F(Z) + X\,[1-F(Z)]\}$$

We can now compute the probability of a given event observed by the customer and determine how that probability depends on the degree of precaution X and the intensity of inspection Z.

From the viewpoint of the website and consumers what matters is the distribution of outcome observed by the consumer. We will say that an intrusion occurs if outcome G or B is observed, while there is no intrusion if nothing happens, event $\emptyset$. Once the third-party has obtained the information, intrusiveness is measured by the joint probability of outcomes G and B. For type $t = h, l$, we then define *intrusiveness* as:

$$\gamma_t = \lambda + (1-\lambda)\,\theta_t$$

and denote $E(\gamma)$ the expected value of γ.

An intrusion may yield a good or a bad outcome, but reveals that the third-party had access to the information. The probability of a good outcome (event G) is

$$p_G(X,Z) = 1 - \pi_M(X,Z) - \pi_N(X,Z) = \beta\lambda\{1-(1-\alpha)X(1-F(Z))\}$$

which is decreasing in X but increasing in Z except under weak privacy:

$$\frac{\partial p_G}{\partial X} < 0 \leq \frac{\partial p_G}{\partial Z}. \tag{1}$$

The probability of a bad outcome (event B) is

$$p_B(\theta,X,Z) = \pi_M(X,Z)\theta = \beta(1-\lambda)\{\alpha+(1-\alpha)(1-X)(1-F(Z))\}\theta$$

which decreases with X and decreases with Z except under strong privacy

$$\frac{\partial p_B}{\partial X} < 0;\ \frac{\partial p_B}{\partial Z} \leq 0 \tag{2}$$

Finally, no intrusion occurs if no third-party obtained the information or if it is malicious but the consumer is not vulnerable. Thus the probability that no intrusion is observed is $p_\emptyset(\theta,X,Z) = (1-\theta)\pi_M(X,Z) + \pi_N(X,Z)$, which can be written

$$p_\emptyset(\theta,X,Z) = 1-\beta\gamma+\beta(1-\alpha)[(1-\lambda)\theta F(Z) + [\lambda+(1-\lambda)\theta]X(1-F(Z))]. \tag{3}$$

We then have

$$\frac{\partial p_\emptyset}{\partial X} = \beta(1-\alpha)[1-F(Z)]\gamma > 0$$

and

$$\frac{\partial p_\emptyset}{\partial Z} = \beta(1-\alpha)[(1-\lambda)\theta - \gamma X]f(Z)$$

Increasing X reduces the chance of an intrusion while the effect of inspection depends on the level of protection of privacy and is negative if X is larger than $(1-\lambda)\theta/\gamma$.

3.3 Beliefs

Denote by r_G, r_B and $r_\emptyset$ the updated probability at the beginning of period 1 that $\theta = \theta_l$ after the events G, B and $\emptyset$ respectively. A consumer who transacts with the platform updates her beliefs as follows:

$$r_G = r_0$$

$$r_B = \frac{r_0\theta_l}{E(\theta)}$$

where $E(\theta) = r_0\theta_l + (1 - r_0)\theta_h$.

Notice that r_G and r_B are not affected by the strategy of the website. This is because this strategy affects the likelihood of non-malicious and malicious use of the information, but not the outcome that follows access to the information. But the likelihood that the consumer is not affected by the third-party depends on the strategy;

$$r_\emptyset = \Phi(X, Z) \equiv \frac{p_\emptyset(\theta_l, X, Z)}{p_\emptyset(E(\theta), X, Z)} r_0, \tag{4}$$

where $p_\emptyset(\theta, X, Z)$ is given by equation (3). Observing no intrusion is a good news in our model in the sense that

$$r_B < r_G < r_\emptyset.$$

This is because no intrusion raises the possibility that some malicious party obtained the information and failed to exploit due to small vulnerability of the consumer.

The following lemma shows how the posterior beliefs when no intrusion occurs depends on the degree of precaution and the level of inspection:

Lemma 1 *i)* $\Phi(X, Z)$ *is decreasing in* X.

ii) There exists $X_\infty \in (0, 1)$ *such that* $\Phi(X, Z)$ *is increasing in* Z *for any* $X > X_\infty$, *decreasing in* Z *for any* $X < X_\infty$, *and constant in* Z *for* $X = X_\infty$.

iii) $\lim_{Z \to +\infty} \Phi(X, Z) = \Phi_\infty$ *for all* $X \in [0, 1]$ *where* Φ_∞ *is the constant value taken by* $\Phi(X, Z)$ *when* $X = X_\infty$.

Proof. i) $\Phi(X, Z)$ is a rational fraction in X. Therefore, it is monotonic in X (for a given Z) and the sign of $\frac{\partial \Phi}{\partial X}$ is the same as the sign of the determinant

$$\begin{vmatrix} \beta(1-\alpha)[\lambda + (1-\lambda)\theta_l](1 - F(Z)) & 1 - \beta[\lambda + (1-\lambda)\theta_l] + \beta(1-\alpha)(1-\lambda)\theta_l F(Z) \\ \beta(1-\alpha)[\lambda + (1-\lambda)E(\theta)](1 - F(Z)) & 1 - \beta[\lambda + (1-\lambda)E(\theta)] + \beta(1-\alpha)(1-\lambda)E(\theta)F(Z) \end{vmatrix}$$

which is the same as the sign of

$$\begin{vmatrix} [\lambda + (1-\lambda)\theta_l] & 1 - \beta[\lambda + (1-\lambda)\theta_l] + \beta(1-\alpha)(1-\lambda)\theta_l F(Z) \\ [\lambda + (1-\lambda)E(\theta)] & 1 - \beta[\lambda + (1-\lambda)E(\theta)] + \beta(1-\alpha)(1-\lambda)E(\theta)F(Z) \end{vmatrix}$$

The latter is equal to

$$(1-\lambda)(\theta_l - E(\theta))(1 - \beta(1-\alpha)F(Z)) < 0$$

Therefore, $\Phi(X, Z)$ is decreasing in X.

ii) $\Phi(X,Z)$ is a rational fraction in Z. Therefore, it is monotonic in Z (for a given X) and the sign of $\frac{\partial \Phi}{\partial Z}$ is the same as the sign of the determinant

$$\begin{vmatrix} \beta(1-\alpha)\left[(1-\lambda)\theta_l - [\lambda+(1-\lambda)\theta_l]X\right] & 1-\beta[\lambda+(1-\lambda)\theta_l]+\beta(1-\alpha)[\lambda+(1-\lambda)\theta_l]X \\ \beta(1-\alpha)\left[(1-\lambda)E(\theta) - [\lambda+(1-\lambda)E(\theta)]X\right] & 1-\beta[\lambda+(1-\lambda)E(\theta)]+\beta(1-\alpha)[\lambda+(1-\lambda)E(\theta)]X \end{vmatrix}$$

which is the same as the sign of

$$\begin{vmatrix} \left[(1-\lambda)\theta_l - [\lambda+(1-\lambda)\theta_l]X\right] & 1-\beta[\lambda+(1-\lambda)\theta_l]+\beta(1-\alpha)[\lambda+(1-\lambda)\theta_l]X \\ \left[(1-\lambda)E(\theta) - [\lambda+(1-\lambda)E(\theta)]X\right] & 1-\beta[\lambda+(1-\lambda)E(\theta)]+\beta(1-\alpha)[\lambda+(1-\lambda)E(\theta)]X \end{vmatrix}$$

Straightforward computations show that the latter is equal to

$$(1-\lambda)(E(\theta)-\theta_l)\{[1-\beta\lambda(1-\alpha)]X-(1-\beta\lambda)\}.$$

Therefore, denoting

$$X_\infty \equiv \frac{1-\beta\lambda}{1-\beta\lambda(1-\alpha)}$$

$\Phi(X,Z)$ is increasing in Z for any $X > X_\infty$, decreasing in Z for any $X < X_\infty$, and constant in Z for $X = X_\infty$.

iii) From $\Phi(X,Z) \equiv \frac{p_\emptyset(\theta_l,X,Z)}{p_\emptyset(E(\theta),X,Z)} r_0$ and the expression of $p_\emptyset$ it folllows that

$$\lim_{Z\to+\infty} \Phi(X,Z) = \frac{1-\beta(\lambda+\alpha(1-\lambda)\theta_l)}{1-\beta(\lambda+\alpha(1-\lambda)E(\theta))}$$

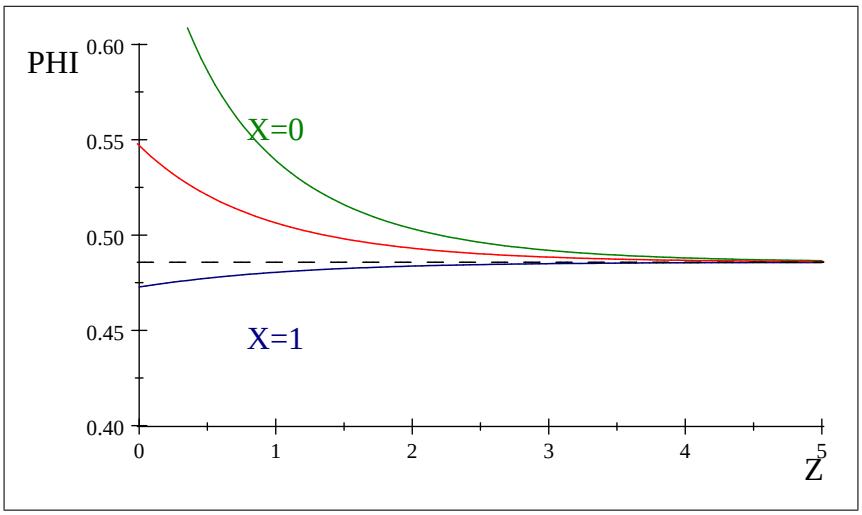
for all $Z \geq 0$. Since this limit does not depend on X, and $\Phi(X_\infty, Z) = \Phi_\infty$ for all $Z \geq 0$ (and therefore for $Z \longrightarrow +\infty$), it must hold that $\lim_{Z\to+\infty} \Phi(X,Z) = \Phi_\infty$ for all $X \in [0,1]$. ■

The posterior $\Phi(X,Z)$ decreases in X as increasing X reduces the likelihood that no intrusion is triggered by low vulnerability relative to no access to the information. Moreover when all third-parties are inspected, X becomes irrelevant and doesn't affect the posterior Φ_∞.The effect of Z depends on the degree of protection of privacy. Under high protection, more inspection reduces foreclosure of the good third-party so that the signal becomes more informative about vulnerability and Φ increases. Under weak protection, it reduces access by malicious third-party and thus the signal becomes less informative about vulnerability.

Combining these properties we see that

$$r_0 < \Phi(1,0) < \Phi(X,Z) < \Phi_\infty < \Phi\left(X',Z'\right) < \Phi(0,0)$$

for any $Z, Z' > 0$ and any $X, X' \in [0,1]$ such that $X' < X_\infty < X$. These properties are illustrated in the following figure.



Posterior with no intrusion

4 Scenario with no inspection

In this section, we consider the case in which the website cannot inspect the third party in order to determine its type, i.e., Z is necessarily zero. This may happen because a technology to distinguish bad third parties from good ones is not available (or is prohibitively costly).

We first derive the equilibrium degree of precaution for any parameter values. Then we compare this equilibrium value with the one chosen by a website that can commit to a given degree of precaution. Finally, we investigate whether the firm's choice exhibits under- or over-protection from a social standpoint.

4.1 Equilibrium analysis

With no inspection, privacy policy reduces to the decision to sell or not the information. The platforms prefers to grant access to customer information rather than denying it to any third party if

$$Q\left(r_{\emptyset}\right)V_1 \leq v_0 + \left[\lambda Q\left(r_G\right) + \left(1-\lambda\right)\left(E(\theta)Q\left(r_B\right) + \left(1-E(\theta)\right)Q\left(r_{\emptyset}\right)\right]V_1.$$

For what follows, a useful interpretation of the equilibrium condition is the following. Starting from full privacy, the benefit of selling the information is twofold. First, this raises the probability that a good party buys the information, which yields an expected gain $B_G\left(r_{\emptyset}\right)$ given by:

$$B_G\left(r_{\emptyset}\right) = \lambda\left[v_0 + Q\left(r_G\right)V_1 - Q\left(r_{\emptyset}\right)V_1\right] \tag{5}$$

Second, this also raises the probability that a malicious party buys with an expected cost

$-B_B(r_\emptyset)$ where

$$B_B(r_\emptyset) = (1-\lambda)\left[E(\theta)Q(r_\emptyset)V_1 - E(\theta)Q(r_B)V_1 - v_0\right] \tag{6}$$

is the expected gain from foreclosing malicious parties.

The net benefit from selling the information is then

$$B_G(r_\emptyset) - B_B(r_\emptyset) = v_0 - \left[\left(\lambda + (1-\lambda)E(\theta)\right)Q(r_\emptyset) - \lambda Q(r_G) - (1-\lambda)E(\theta)Q(r_B)\right]V_1 \tag{7}$$

and it must be non-negative for the website to choose privacy.

Hence, an equilibrium in which the platforms adopts a full privacy policy ($X = 1$, $r_\emptyset = \phi(1,0)$) exists if and only if

$$\frac{v_0}{V_1} \leq \psi^f \equiv \left(\lambda + (1-\lambda)E(\theta)\right)Q(\Phi(1,0)) - \lambda Q(r_G) - (1-\lambda)E(\theta)Q(r_B) \tag{8}$$

Similarly, an equilibrium with no privacy ($X = 0$, $r_\emptyset = \phi(0,0)$) exists if and only if

$$\frac{v_0}{V_1} \geq \psi^n \equiv \left(\lambda + (1-\lambda)E(\theta)\right)Q(\Phi(0,0)) - \lambda Q(r_G) - (1-\lambda)E(\theta)Q(r_B) \tag{9}$$

Notice that, because $\Phi(0,0) > \Phi(1,0)$, privacy is more attractive when consumers expect no privacy than when they expect full privacy. As a result, we have $\psi^n < \psi^f$ and there is a range of values, $\psi^n < v_0/V_1 < \psi^f$ for which no pure strategy equilibrium exists. In this range, the website randomizes between selling and not selling customer information in equilibrium and the level of privacy X^0 is such that $B_B = B_G$ when $r_\emptyset = \phi\left(X^0, 0\right)$:

$$\frac{v_0}{V_1} = \left(\lambda + (1-\lambda)E(\theta)\right)Q(\Phi(X^*,0)) - \lambda Q(r_G) - (1-\lambda)E(\theta)Q(r_B) \tag{10}$$

Therefore, we get the following equilibrium characterization:

Proposition 1 *For any parameter values, there exists a unique equilibrium. More precisely, there exist positive thresholds $\psi^f < \psi^n$ such that:*

- *The website provides full privacy ($X^0 = 1$) if $v_0 \leq \psi^f V_1$.*
- *The website's policy is random ($X^0 \in (0,1)$) if $\psi^f V_1 < v_0 < \psi^n V_1$.*
- *The website provides no privacy ($X^0 = 0$) if $v_0 \geq \psi^n V_1$.*

Proof. The pure strategy equilibria are described above. We have an equilibrium with random sale $X \in (0,1)$ if and only if the platform is indifferent between denying access to customer information and selling it. This writes

$$Q(r_\emptyset)V_1 = v_0 + \left[\lambda Q(r_G) + (1-\lambda)\left(E(\theta)Q(r_B) + (1-E(\theta))Q(r_\emptyset)\right]V_1$$

with $r_\emptyset = \Phi(X, 0)$, which is the same as condition (10). Since $\Phi(X, 0)$ is decreasing in X, the latter can only hold when $\psi^n < \frac{v_0}{V_1} < \psi^f$. Conversely, whenever this double inequality holds, there exists a unique $X \in (0, 1)$ such that (10) is satisfied. ■

Moreover, from (10) and the fact that $\Phi(X, 0)$ is decreasing in X it follows that the equilibrium degree of precaution X^0 is non-increasing in v_0 and non-decreasing in V_1.

4.2 Commitment

Let us now investigate how the equilibrium degree of precaution derived in the previous subsection compares to the one chosen by a website that can publicly commit to a given strategy.

For given beliefs $r_\emptyset$, a website choosing a precaution level X makes an expected profit

$$\Pi(r_\emptyset, X) = \beta(1-\alpha)(1-X)v_0 + \{p_G(X, 0)Q(r_0) + p_B(E(\theta), X, 0)Q(r_B) + p_\emptyset(E(\theta), X, 0)Q(r_\emptyset)\}V_1$$

The difference between the case where X is unobservable and the case where it is observed by consumers is that in the latter case, the website can affect the posterior beliefs by its choice of privacy policy. Since the profit is increasing in consumer beliefs $r_\emptyset$:

$$\frac{\partial \Pi}{\partial r_\emptyset} = p_\emptyset(E(\theta), X, 0)Q'(r_\emptyset)V_1 > 0,$$

the website will change X in a direction that raises $r_\emptyset$. This is achieved by raising the informativeness of he signal, that is, by selling the information to the malicious party more often. This leads the following result:

Proposition 2 *If the website is able to commit to its strategy, it chooses a weaker privacy policy (i.e., lower X) than in the equilibrium with no commitment.*

Proof. As $r_\emptyset = \Phi(X, 0)$ is decreasing in X, the marginal gain of the website from increasing X is lower when it can commit to its strategy.

$$\frac{\partial \Pi(r_\emptyset, X)}{\partial X} + \frac{\partial \Pi(r_\emptyset, X)}{\partial r_\emptyset}\frac{\partial \Phi(X, 0)}{\partial X} < \frac{\partial \Pi(r_\emptyset, X)}{\partial X}$$

This implies that a full privacy equilibrium exists for a smaller range of values v_0/V_1 while a no-privacy equilibrium exists for a wider range. Consider an interior equilibrium level X^0 with no commitment, then for any $X > X^0$we have

$$\Pi\left(\Phi\left(X^0, 0\right), X^0\right) > \Pi\left(\Phi\left(X^0, 0\right), X\right) > \Pi\left(\Phi(X, 0), X\right)$$

therefore the website chooses $X \leq X^0$. Moreover at X^0, $\frac{\partial \Pi}{\partial X} + \frac{\partial \Pi}{\partial r_\emptyset}\frac{\partial \Phi}{\partial X} = \frac{\partial \Pi}{\partial r_\emptyset}\frac{\partial \Phi}{\partial X} < 0$ so that the website chooses $X < X^0$. ■

Thus, a website is too cautious in protecting consumers from a profit-maximizing perspective when it cannot commit to its privacy policy. The reason is that the website would like consumers to interpret no intrusion as a stronger signal.

4.3 Welfare analysis

We now perform a welfare analysis. For this purpose, let us first derive consumer welfare.

We decompose consumer utility into two components: the utility from current period (period 0) consumption $STU(X)$ and the expected utility from future (period 1) consumption $LTU(r_\emptyset, X)$.

Privacy policy then affects the value of $r_\emptyset$ and the probabilities of each event. We separate the two effects for clarity and thus have two arguments in LTU. Consumer utility can be written as

$$U(r_\emptyset, X) = STU(X) + LTU(r_\emptyset, X)$$

where the short-term and long-term utilities are given by

$$STU(X) = \beta\left[\alpha + (1-\alpha)(1-X)\right]\left[\lambda U_G + (1-\lambda)E(\theta)U_B\right]$$

and

$$LTU(r_\emptyset, X) = p_G(X,0)U_1(r_G) + p_B(E(\theta),X,0)U_1(r_B) + p_\emptyset(E(\theta),X,0)U_1(r_\emptyset)$$

First, note that consumers benefit in period 1 from the belief-improving effect of a less cautious strategy: decreasing X raises posteriors $r_\emptyset = \Phi(X,0)$ and thus indirectly LTU, but of course it also alters the distribution of the posteriors.

$$\begin{aligned}\frac{\partial LTU}{\partial X} &= \frac{\partial LTU}{\partial r_\emptyset}\frac{\partial LTU}{\partial X} + \frac{\partial p_G}{\partial X}U_1(r_G) + \frac{\partial p_B}{\partial X}U_1(r_B) + \frac{\partial p_\emptyset(E(\theta),X,0)}{\partial X}\int_{-M_1(r_\emptyset)}^{+\infty}(1-G(s))\,ds \\ &= \underbrace{p_\emptyset U_1'(r_\emptyset)\frac{\partial \Phi}{\partial X}}_{<0} + \underbrace{\frac{\partial p_G}{\partial X}\left(U_1(r_G)-U_1(r_\emptyset)\right) + \frac{\partial p_B}{\partial X}\left(U_1(r_B)-U_1(r_\emptyset)\right)}_{>0}\end{aligned}$$

since $\frac{\partial p_G(X,0)}{\partial X}$ and $\frac{\partial p_B(E(\theta),X,0)}{\partial X}$ are negative and $U(r_B) < U_1(r_G) < U_1(r_\emptyset)$. Thus, the overall long-term effect of lowering the degree of precaution on consumers is *a priori* ambiguous. However, this long-term effect can be rewritten as

Lemma 2 *The long-term effect of precaution on utility is*

$$\frac{\partial LTU}{\partial X} = \frac{\partial p_G}{\partial X}\left(U_1(r_G) - U_1(r_\emptyset) + U_1'(r_\emptyset)(r_\emptyset - r_G)\right) + \frac{\partial p_B}{\partial X}\left(U_1(r_B) - U_1(r_\emptyset) + + U_1'(r_\emptyset)(r_\emptyset - r_B)\right).$$

Proof. Direct computation of derivatives shows that

$$r_{\emptyset} = \frac{p_{\emptyset}(\theta_l, X, 0)}{p_{\emptyset}(E(\theta), X, 0)} \Longrightarrow p_{\emptyset}\frac{\partial r_{\emptyset}}{\partial X} = \frac{\partial p_{\emptyset}(\theta_l, X, Z)}{\partial X} r_0 - \frac{\partial p_{\emptyset}(E(\theta), X, Z)}{\partial X} r_{\emptyset}$$

Using

$$\frac{\partial p_{\emptyset}(\theta, X, 0)}{\partial X} = -\frac{\partial p_G(X, 0)}{\partial X} - \frac{\partial p_B(\theta, X, 0)}{\partial X}$$

and

$$\frac{\partial p_B(\theta_l, X, 0)}{\partial X} r_0 = \frac{\partial p_B(E(\theta), X, 0)}{\partial X} \frac{\theta_l}{E(\theta)} r_0 = \frac{\partial p_B(E(\theta), X, 0)}{\partial X} r_B$$

we obtain

$$p_{\emptyset}\frac{\partial r_{\emptyset}}{\partial X} = \frac{\partial p_G(X, 0)}{\partial X}(r_{\emptyset} - r_G) + \frac{\partial p_B(E(\theta), X, 0)}{\partial X}(r_{\emptyset} - r_G)$$

which yields the result. ■

Let us now consider the effect of the degree of precaution on the short-term utility:

$$\frac{\partial STU}{\partial X} = -\beta(1-\alpha)[\lambda U_G + (1-\lambda)E(\theta)U_B]$$

If the expected matching value (with the prior beliefs) is negative, i.e., $\lambda U_G + (1-\lambda)E(\theta)U_B < 0$, consumers are positively affected in period 0 by a stronger privacy policy, which may create a tension between the short-term and long-term effects of more/less precaution on consumers. Indeed, recall that the future utility is convex in the posterior, implying that $U_1(r) - U_1(r_{\emptyset}) + U_1'(r_{\emptyset})(r_{\emptyset} - r) > 0$. Given that p_G and p_B decreases in X, the long-run effect is always negative. This is summarized in the next proposition.

Proposition 3 *A stronger privacy policy increases (decreases) the short-run consumer surplus if the expected matching value $\lambda U_G + (1-\lambda)E(\theta)U_B$ is negative (positive). The effect on consumers' long-run utility is negative.*

The result on the long-term utility is due to the fact that that more precaution reduces the informational content of the market signal about vulnerability and thus prevent optimal adjustment of future behavior. The proposition, combined with our result on the comparison between the equilibrium strategy and the website's optimal strategy when it can commit, yields the following:

Corollary 1 *If the expected matching value is negative and consumers are impatient (U_1 is small), then the website and the consumers have conflicting views regarding the privacy level. Otherwise, consumers may prefer a weaker privacy policy.*

5 Scenario with inspection

We now investigate the general case where the website may inspect or not the third party. The first question we address is the extent to which the possibility to inspect affects the previous equilibria. To analyze this issue, we first notice that the previous analysis of the choice of X still holds provided that $r_\emptyset$ is set at its equilibrium value, $r_\emptyset = \Phi(X, Z)$. Thus the website chooses $X = 1$ if

$$\frac{v_0}{V_1} < [\lambda + (1-\lambda) E(\theta)] Q(r_\emptyset) - \lambda Q(r_G) - (1-\lambda) E(\theta) Q(r_B)$$

Consider now the inspection decision. An inspection raises the probability to sell to a good third party from $1 - X$ to one with a benefit $XB_G(r_\emptyset)$ where $B_G(r_\emptyset)$ is the benefit from selling to a good third party, defined in (5). It also reduces the probability to sell to a malicious party from $1 - X$ to zero with a benefit $(1 - X) B_B(r_\emptyset)$ where $B_B(r_\emptyset)$ is the benefit from denying,access to a malicious third-party, defined in (6). The total benefit is then the sum $XB_G + (1 - X) B_B$,and some inspection occurs when it is positive. The main difference between inspection and precaution is that the former allows to combine the two benefits B_G and B_B while the latter requires to balance these benefits.

It follows from this reasoning that the previous equilibria with no inspection remain equilibria when inspection is allowed if $XB_G(r_\emptyset) + (1 - X) B_B(r_\emptyset)$ is non-positive. We then find the following characterization.

Proposition 4 *There is some inspection* $(Z^* > 0)$ *if* $\underline{\psi}^i V_1 < v_0 < \bar{\psi}^i V_1$ *where*

i) $\underline{\psi}^i = \psi^f = \bar{\psi}^i$ *if* $Q(\Phi(1,0)) \geq \frac{Q(r_G) - E(\theta) Q(r_B)}{1 - E(\theta)}$, *which implies that inspection never happens;*

ii) $\underline{\psi}^i < \psi^f < \bar{\psi}^i < \psi^n$ *if* $Q(\Phi(0,0)) > \frac{Q(r_G) - E(\theta) Q(r_B)}{1 - E(\theta)} > Q(\Phi(1,0))$;

iii) $\underline{\psi}^i < \psi^f < \psi^n < \bar{\psi}^i$ *if* $Q(\Phi(0,0)) \leq \frac{Q(r_G) - E(\theta) Q(r_B)}{1 - E(\theta)}$.

Proof. See Appendix. ■

Inspection occurs under strong privacy if $B_G(r_\emptyset) > 0$ while it occurs under weak privacy if $B_B(r_\emptyset) > 0$. While the benefit $B_G(r_\emptyset)$ increases with v_0, the benefit $B_B(r_\emptyset)$ decreases with v_0. Hence, inspection occurs only for some intermediate range of values v_0 of the information.

When the posterior $r_\emptyset$ is large for any strategy, the website abandons strong privacy at levels of v_0 such that $B_G(r_\emptyset) = B_B(r_\emptyset) < 0$ so that the benefit of inspection is negative for all values of v_0. Screening is not useful in this case.

Let us now on assume that some inspection may occur.

Under this assumption, it remains to determine the equilibrium for $v_0 \in \left(\underline{\psi}^i, \bar{\psi}^i\right)$. This equilibrium must be such that the following two conditions are verified, with $r^*_\emptyset = \Phi(X^*, Z^*)$:

$$\begin{aligned} Z^* &= X^* B_G\left(r^*_\emptyset\right) + (1 - X^*) B_B\left(r^*_\emptyset\right) > 0; \\ X^* &\in \arg\max_X X\left(B_G\left(r^*_\emptyset\right) - B_B\left(r^*_\emptyset\right)\right) \end{aligned}$$

The first condition just equates the cost of inspection with the expected benefit from inspection while the second condition is the same as the one discussed above. For clarity, we first analyze case iii) of Proposition 4 and then extend the analysis to case ii).

Let us assume that $\underline{\psi}^i < \psi^f < \psi^n < \underline{\psi}^i$. In this case there is no mixed strategy equilibrium with no inspection and the two boundaries of the interval are determined as the values at which the website starts to inspect in a pure strategy equilibrium. Intuitively, we expect that strong privacy ($X = 1$) will continue to prevail at the the right of $\underline{\psi}^i$ and weak privacy will continue to prevail at the left of $\bar{\psi}^i$.

Moreover, we have seen that because $\Phi(1, Z) < \Phi(0, Z)$, strong precaution is more attractive to the website when the consumers expect weak precaution to prevail. For this reason, we do not expect equilibria with different levels of precaution to coexist. This suggest that a random strategy emerges for intermediates value of the information. The next proposition confirms these intuitions.

For what follows we need a regularity condition.

Condition 1 (C1) *For* $X < X_\infty$, $\lambda(1-\lambda)[1 - E(\theta)] V_1 Q'(\Phi(X, Z)) \frac{\partial \Phi(X,Z)}{\partial Z} > -1$.

This property states that the future gains from no intrusion do not decline too fast with inspection. It ensures enough regularity for the threshold v_w to be well defined in the next proposition.

Proposition 5 *Assume* $\underline{\psi}^i < \psi^f < \psi^n < \bar{\psi}^i$ *and C*1. *Then for* $v_0 \in \left(\underline{\psi}^i, \bar{\psi}^i\right)$ *there exists a unique equilibrium. There exists two increasing functions* $v_s(V_1)$ *and* $v_w(V_1)$ *such that*

i) the website chooses strong privacy if $v_0 \leq v_s(V_1)$, *weak privacy if* $v_0 \geq v_w(V_1)$ *and a random privacy policy if* $v_0 \in (v_s(V_1), v_w(V_1))$;

ii) $\psi^f V_1 < v_s(V_1) < v_w(V_1) < \psi^n V_1$;

iii) $v_s(V_1)/V_1$ *is increasing in* V_1 *while* $v_w(V_1)/V_1$ *is decreasing in* V_1.

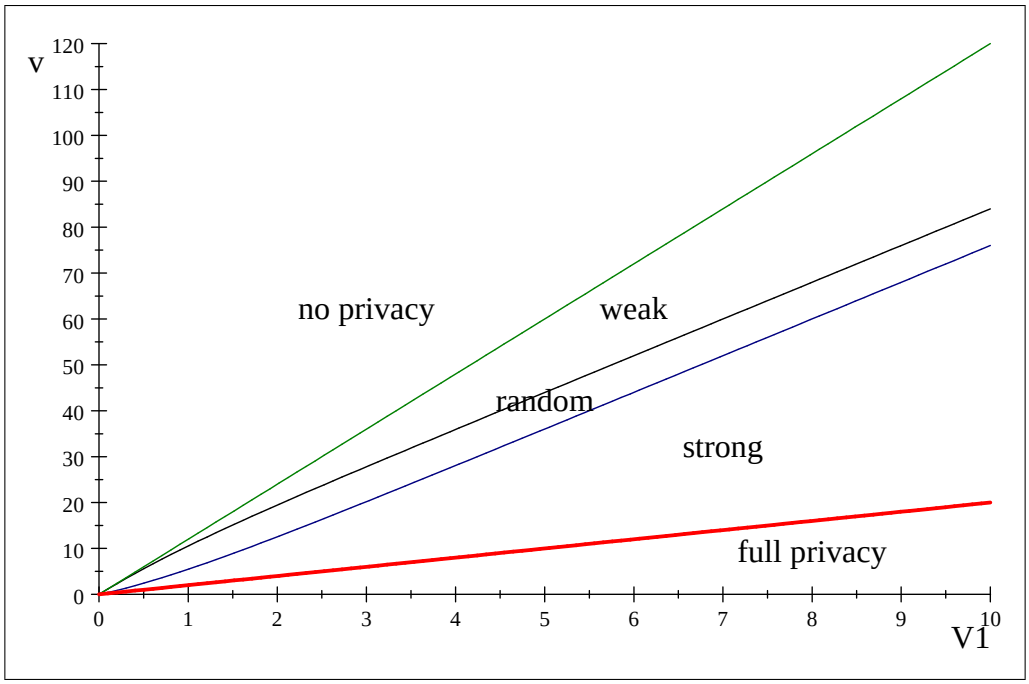
Proof. See Appendix ■

In an equilibrium in which the platform uses a strong privacy strategy ($X^* = 1$) with threshold $Z^* > 0$, the website inspects the third party and provides access to good third parties if $z \leq Z$, while it denies access to both types if $z > Z$. Thus, it does not sell the

information unless it is confident that the third party is good. The platform gains from denying access to information to third parties if no intrusion is interpreted by the consumer as sufficiently good news on her type. In that case, the retention rate would be higher than the average retention rate under access. Unsurprisingly, the strong privacy equilibrium exists if the monetary gain from selling the information is not too large. In this equilibrium, the website is willing to sacrifice short-run profits to convince the consumer to return to the website. Increasing Z reduces the probability that a good party fails to obtain the information, which raises the informativeness of no news. This in turn reduces the website's benefits from inspection, which explains the uniqueness result in the range $v_0 < v_s$.

In an equilibrium in which the platform uses a weak privacy strategy ($X^* = 0$) with threshold $Z^* > 0$, the platform inspects the third party and provides access to G if $z \leq Z^*$, while it provides access to both types if $z > Z^*$. In the weak privacy equilibrium, the value of information is too large for the platform to accept foregoing it without due knowledge that the third party is malicious. In this case, increasing Z decreases the probability that a malicious party obtains the information, which reduces the informativeness of no news. This in turn reduces the website's benefits from inspection, which explains the uniqueness result in the range $v_0 > v_w$.

We present the ranges of equilibria in the next graph.



In the mixed strategy range we have

$$B_B^* = B_G^* = (1-\lambda)\,\lambda\left[Q\left(r_G\right) - E\left(\theta\right)Q\left(r_B\right) - \left(1-E\left(\theta\right)\right)Q\left(r_\emptyset^*\right)\right]V_1 > 0$$

and at the level of inspection Z^*, the website is indifferent between inspecting, selling to all third parties, or not selling to any third party. As we have seen, that indifference between selling and not selling is compatible with only one posterior $r_\emptyset$. This implies in particular that

$$\Phi\left(X^*, Z^*\right) = \Phi\left(X^0, 0\right).$$

Hence, the posteriors are not affected in this range by the ability to inspect the third party.

We conclude this section by noticing that the analysis is similar for the case where $\bar{\psi}^i < \psi^n$.

Proposition 6 *Assume $\underline{\psi}^i < \psi^f < \bar{\psi}^i < \psi^n$. Then, for $v_0 \in \left(\underline{\psi}^i, \bar{\psi}^i\right)$, there exists a unique equilibrium. Moreover, there exists an increasing function $v_s\left(V_1\right)$ such that*

i) the website chooses strong privacy if $v_0 \leq v_s\left(V_1\right)$, and a random policy if $v_0 \in \left(v_s\left(V_1\right), \bar{\psi}^i V_1\right)$;

ii) $\psi^f V_1 < v_s\left(V_1\right) < \bar{\psi}^i V_1$;

iii) $v_s\left(V_1\right)/V_1$ is increasing in V_1

The analysis is the same as before except that there is no weak privacy regime with inspection, and the transition between inspection and no inspection is made in the mixed strategy regime.

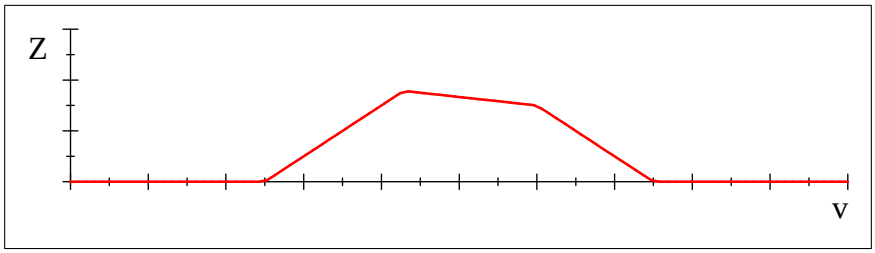
6 Comparative statics

Let us first perform some comparative static on the equilibrium. We first consider an increase in the value of v_0. Notice that such an increase could be triggered by a tax on information levied by the government, as well as by a technological improvement in the treatment of information or any other market development. Intuitively, increasing the price of information should reduce the level of precaution X but the the impact on the level of inspection is ambiguous. Indeed, inspection allows to restrict sales to good third parties which induces a short-term revenue loss that depends on the price v_0 but also on the level of precaution. With strong privacy, raising v_0 makes inspection more attractive as it generates more sales. In contrast, with weak privacy, raising v_0 renders inspection less attractive at it reduces the probability to sell. The next proposition shows that the random privacy region is similar to the weak privacy regime in this respect.

Proposition 7 *The equilibrium level of precaution X^* is non-increasing in the price of information v_0. The level of inspection Z^* is increasing in v_0 in the range of strong precaution $v_0 \in \left(\underline{\psi}^i, v_s(V_1)\right)$ and decreasing in v_0 in the range of random and weak privacy $v_0 \in \left(v_s(V_1), \bar{\psi}^i\right)$.*

Proof. To be completed. ■

Hence, we find a non-monotonic effect of the price v_0 on the level of inspection.



Level of inspection

An implication of these comparative statics that we highlight below is that the posterior belief after no intrusion $r_\emptyset^*$ is non-decreasing in v_0: in any case, increasing v_0 makes no intrusion a better news about the potential risk of successful malicious intrusion.

Let $p_B^* = p_B(X^*, Z^*)$ (resp. $p_G^* = p_G(X^*, Z^*)$) be the equilibrium probability that the malicious type buys the information from the website (conditional on needing it). It follows from the above comparative statics and (2) that:

Corollary 2 *The posterior $r_\emptyset^*$ and the probability p_B^* that the bad party buys the information are non-decreasing in v_0*

7 Welfare analysis

Let us now turn to the analysis of profit and welfare.

First, consider the profit of the firm and as in the case with no inspection. Let us evaluate what the website would find it optimal to do if it could commit to X or to Z. The profit is now given by

$$\Pi(r_\emptyset, X, Z) = \beta(1-\alpha)(1-X)v_0 + \{p_G(X,Z)Q(r_0) + p_B(E(\theta), X, Z)Q(r_B) + p_\emptyset(E(\theta), X, Z)Q(r_\emptyset)\}V_1.$$

The website can control all the elements of profit except for the beliefs $r_\emptyset$. Since

$$\frac{\partial \Pi}{\partial r_\emptyset} = p_\emptyset(E(\theta), X, Z)Q'(r_\emptyset)V_1 > 0,$$

we reach the same conclusion as before: the website would like to commit to change the policy in the direction that would raise the consumers' posterior beliefs when no intrusion occurs. Clearly, this means decreasing X as $\Phi(X, Z)$ is decreasing in X. The conclusion regarding Z is more ambiguous as the sign of the slope of Φ with respect to Z depends on X.

Proposition 8 *The website would benefit from committing to a marginal reduction of the level X of precaution (starting from X^*). There exists v_∞ such that the website would benefit from committing to a marginal reduction (resp. increase) of the level Z of inspection if $v_0 > v_\infty$ (resp. $v_0 < v_\infty$).*

Proof. The first part of the proposition follows from $\frac{\partial \Phi(X,Z)}{\partial X} < 0$ while the second part follows from the fact that $\frac{\partial \Phi(X,Z)}{\partial Z} > 0$ for $X > X_\infty$ and $\frac{\partial \Phi(X,Z)}{\partial Z} < 0$ for $X < X_\infty$. As X^* is decreasing in v_0 in the random policy range, there exists v_∞ such that $X^* = X_\infty$ which determines a threshold of the information value below which raising inspection raises posterior belief $r^*_\emptyset$. ■

Consumer utility is again given by

$$U(r_\emptyset, X, Z) = STU(X, Z) + LTU(r_\emptyset, X, Z)$$

where the short-term (i.e., period 0) utility is given by

$$STU(X, Z) = p_G(X, Z)\, U_G + p_B(E(\theta), X, Z)\, U_B,$$

and the long-term (i.e., period 1) utility is given by

$$LTU(r_\emptyset, X, Z) = p_G(X, Z)\, U_1(r_G) + p_B(E(\theta), X, Z)\, U_1(r_B) + p_\emptyset(E(\theta), X, Z)\, U_1(r_\emptyset)$$

In this context, a public policy intervention may aim at fostering precaution (X) or inspection (Z). For instance, a penalty for selling to malicious third parties would reduce the value of non-discriminating sales and thus reduce X and most likely increase Z. The impact of a tax on sales of customer information has the same effect as reducing v_0: it reduces X and may reduce or increase Z depending on the level of precaution. Similarly, any rule that forces third parties to be more transparent or that generates information about third parties would reduce the inspection cost, which, in our model amounts to shifting the distribution of the inspection cost toward lower values.

Regarding the level of precaution, we notice that the analysis is the same as before, adjusting for the fact that $Z > 0$. The reason is that the level of precaution matters only if there is no inspection. In particular the sign of the effect of X on p_G, p_B and $r_\emptyset$ is the same for all levels of inspection. We then have

$$\frac{\partial STU(X,Z)}{\partial X} = -\beta\left(1-\alpha\right)\left(1-F\left(Z\right)\right)\left(\lambda U_G + \left(1-\lambda\right)E\left(\theta\right)U_B\right)$$

which is positive if intrusions are on average detrimental to consumers. Let us now consider the effect of inspection on consumer utility. As we have seen, inspection raises the probability p_G and reduces the probability p_B.It is then immediate that inspection always raises the consumer surplus with no less good outcome and no more bad outcomes:

$$\frac{\partial STU(X,Z)}{\partial Z} > 0.$$

The effects on long-term consumer utility can be decomposed as before. For precaution, we have

$$\frac{\partial LTU}{\partial X} = \underbrace{p_\emptyset U_1'\left(r_\emptyset\right)\frac{\partial r_\emptyset}{\partial X}}_{<0} + \underbrace{\frac{\partial p_G}{\partial X}\left(U_1\left(r_G\right)-U_1\left(r_\emptyset\right)\right)+\frac{\partial p_B}{\partial X}\left(U_1\left(r_B\right)-U_1\left(r_\emptyset\right)\right)}_{>0}$$

where $\frac{\partial p_G}{\partial X}$ and $\frac{\partial p_B}{\partial X}$ are negative.

Furthermore, the effect of inspection on the long-term utility is now

$$\frac{\partial LTU}{\partial Z} = \underbrace{p_\emptyset U_1'\left(r_\emptyset\right)\frac{\partial r_\emptyset}{\partial Z}}_{>0 \ for \ X>X_\infty} + \underbrace{\frac{\partial p_G}{\partial Z}\left(U_1\left(r_G\right)-U_1\left(r_\emptyset\right)\right)}_{<0} + \underbrace{\frac{\partial p_B}{\partial Z}\left(U_1\left(r_B\right)-U_1\left(r_\emptyset\right)\right)}_{>0}$$

where $\frac{\partial p_G}{\partial Z}$ is positive while $\frac{\partial p_B}{\partial Z}$ is negative. The overall effect is ambiguous. However, as before we have the following lemma:

Lemma 3 *The slopes of the long-term utility are given by*

$$\begin{aligned}
\frac{\partial LTU}{\partial X} &= \frac{\partial p_G}{\partial X}\left(U_1\left(r_G\right)-U_1\left(r_\emptyset\right)+U_1'\left(r_\emptyset\right)\left(r_\emptyset-r_G\right)\right)+\frac{\partial p_B}{\partial X}\left(U_1\left(r_B\right)-U_1\left(r_\emptyset\right)+U_1'\left(r_\emptyset\right)\left(r_\emptyset-r_B\right)\right), \\
\frac{\partial LTU}{\partial Z} &= \frac{\partial p_G}{\partial Z}\left(U_1\left(r_G\right)-U_1\left(r_\emptyset\right)+U_1'\left(r_\emptyset\right)\left(r_\emptyset-r_G\right)\right)+\frac{\partial p_B}{\partial Z}\left(U_1\left(r_B\right)-U_1\left(r_\emptyset\right)+U_1'\left(r_\emptyset\right)\left(r_\emptyset-r_B\right)\right)
\end{aligned}$$

Proof. The proof is the same as for lemma 2. ■

The previous decomposition still holds with inspection. Thus, regarding the effect of precaution, we find the same conclusions as in the case without inspection.

The conclusions regarding the level of inspection are more ambiguous as the sign of the long-term effect depends on the level of precaution. We summarize these conclusions below.

Proposition 9 *Short-term consumer utility increases (resp. decreases) with precaution X if the expected matching value $\lambda U_G+\left(1-\lambda\right)E\left(\theta\right)U_B$ is negative (resp. positive) while long-term consumer utility decreases with X.*

The short-term consumer utility increases with the level of inspection Z, while the long-term utility increases (resp. decreases) with Z if $X > X_\infty$ (resp. $X < X_\infty$), that is, if $v_0 < v_\infty$ (resp. $v_0 > v_\infty$).

Therefore, we get the following two results regarding the (mis)aligment of the website's and consumers' preferences:

Corollary 3 *If intrusions are on average beneficial or consumers are sufficiently patient then both the website and consumers would benefit from a lower degree of precaution. Otherwise, the website would benefit from a lower degree of precaution while consumers would prefer a higher degree of precaution.*

Corollary 4 *- If the value of information is low enough, both the website and consumers are better off with more inspection.*

- If the value of information is high enough and consumers are sufficiently patient, both the website and consumers are better off with less inspection.

- If the value of information is high enough and consumers are sufficiently impatient, the website would prefer to inspect less while consumers would be better off with more inspection.

8 Opt-out

An alternative policy to protect consumers is to give them control rights over their personal data. A consumer would like to choose which third party can access her personal data and for what purpose. However, contracts are typically incomplete due to private information and lack of verifiability. Here, we assume that whether information is sold or not is verifiable (by courts), but not the nature of the third-party buying this information nor its usage. We allow consumers to opt out, which means they can prevent any resale of information and enforce full privacy. We assume that in the first-period consumers do not find optimal to opt out but that they may decide to do so after revising their beliefs about their vulnerability. Thus, at the end of the period consumers has three options: they may stop their relationship with the website, they may stay and opt in, or they may stay and opt out.

A consumer's choice between opting in and opting out is governed by her beliefs about vulnerability. Let $\bar{r}$ be the posterior beliefs at which the consumer is indifferent between opting in and opting out. When opt out is possible, a consumer chooses to opt out if her posterior belief r_1 is less than $\bar{r}$. In the case of opt out, the retention rate is clearly independent of the posterior r_1. Assuming that the opportunity cost of maintaining the activity on the website is independent of the benefits/costs from resale of personal data, the probability to retain a consumer who prefers to opt out is then $\bar{Q} = Q(\bar{r})$. As a consequence, the retention rate is given by

$$Q^o(r_1) = \max\left\{Q(r_1), \bar{Q}\right\}.$$

Allowing the consumer to opt out thus raises the retention rate. The cost for the website is that it deprives it from the possibility to sell personal data to third parties and, therefore, reduces the expected revenue per consumer. Denoting $\bar{V}_1 < V_1$ the value for the website of a consumer who chooses to opt out, the retention value of a consumer is[3]

$$V_1^o(r_1) = \begin{cases} \bar{V}_1 & \text{if} \quad r_1 < \bar{r}; \\ V_1 & \text{if} \quad r_1 \geq \bar{r}. \end{cases}$$

For now, we assume that:

Assumption $Q(r_B)V_1 > \bar{Q}\bar{V}_1$.

This implies that the website always prefers that consumers do not opt out. Intuitively, under this assumption, we expect that allowing the consumers to opt out makes the website more cautious and raises the level of privacy. As we shall see this conclusion is not so obvious because of the possibility to inspect.

Example

As an illustration, consider the repeated two-period model presented in the first section. The consumer benefit from second-period matching is

$$M_1(r_1) \equiv \beta\,(1-\alpha)\,\lambda U_G + \beta(1-\alpha)\,(1-\lambda)\,(r\theta_l + (1-r)\,\theta_h)\,U_B$$

We then have

$$\bar{r} \equiv \frac{\lambda U_G + (1-\lambda)\,\theta_h U_B}{(\theta_h - \theta_l)\,(1-\lambda)\,U_B}$$

the (unique) solution to $M_1(r_1) = 0$. Consumers opt out in the second period if and only if $M(r_1) < 0$, which is equivalent to $r_1 < \bar{r}$. Moreover $\bar{Q} \equiv 1 - G(0)$. The website's second-period profit per retained consumer is given by $V_1 = a + v_0$ if consumers do not opt out and $\bar{V}_1 = a$ if consumers opt out.

As a preliminary remark, note that in situations where $\bar{r} < r_B$, the equilibrium is not affected by the possibility of opting out as consumers never choose this option. Similarly, in the case where $\bar{r} > \Phi\,(0,0)$, consumers always opt out in the second period. Therefore, the website sells the information to all third parties in the first period, i.e. chooses the no-privacy strategy $(X, Z) = (0, 0)$. We thus restrict attention to the other cases:

Assumption $r_B < \bar{r} < \Phi\,(0,0)$.

[3]Notice also that the expected future utility of a consumer for $r_1 > \bar{r}$ is $U_1\,(\bar{r})$.

Under this assumption, some consumers will opt out in equilibrium (after a bad outcome). But it cannot be the case that all consumers opt out because this would imply $(X, Z) = 0$ and $r_\emptyset = \Phi(0,0) > \bar{r}$. Thus, in equilibrium, consumers should not opt out with positive probability, denoted $P_\emptyset$, if there is no intrusion (by either a good or a malicious third party). As we shall see, this probability may be smaller than 1. We can then distinguish several equilibria depending on whether consumers opt out or not after a good outcome is observed

8.1 Equilibrium with opt out after any intrusion

We first investigate the existence of an equilibrium where the consumers opt out when they observe a good outcome. This is the case when

$$r_0 < \bar{r} < \Phi(0,0).$$

When this holds we observe that both a good outcome and a bad outcome trigger opt-out so that the continuation profit of the website is the same for any intrusion. It is then immediate that the website would not gain from inspecting in this case:

Lemma 4 *When $r_0 < \bar{r}$, the website never inspects: $Z^{**} = 0$*

Proof. Recall that $P_\emptyset > 0$ is the probability that a consumer opts in if there is no intrusion. Following the same reasoning as before, the benefit B_B from selling the information to a good third party or the benefit B_B fromnot not selling it to a bad third party are

$$\bar{B}_G(r_\emptyset) = \lambda \left[v_0 + P_\emptyset \bar{Q} \bar{V}_1 - P_\emptyset Q(r_\emptyset) V_1 \right]$$

$$\bar{B}_B(r_\emptyset) = (1-\lambda) \left[E(\theta) P_\emptyset Q(r_\emptyset) V_1 - E(\theta) \bar{Q} \bar{V}_1 - v_0 \right]$$

Inspection is only profitable if $B_B > 0$ which writes as $P_\emptyset E(\theta) \left(Q(r_\emptyset) V_1 - \bar{Q} \bar{V}_1 \right) > v_0$. However, in this case $B_G < 0$ and selling to a good third party is not profitable. Thus, the website would be better off not selling at all. ■

The equilibrium characterization then follows from the analysis of the model without inspection, where $Q(r_B) V_1$ and $Q(r_G) V_1$ should be replaced with $\bar{Q} \bar{V}_1$. The net benefit from selling is

$$\bar{B}_G(r_\emptyset) - \bar{B}_B(r_\emptyset) = v_0 - (\lambda + (1-\lambda) E(\theta)) \left[Q(r_\emptyset) V_1 - \bar{Q} \bar{V}_1 \right] P_\emptyset$$

and it must be negative for the website to choose privacy:

$$\bar{X}^* = 1 \Longrightarrow \bar{B}_G(r_\emptyset) - \bar{B}_B(r_\emptyset) \leq 0.$$

The reasoning in the section on the equilibrium with no intrusion then applies with the caveat that it is possible that $P_\emptyset < 1$. Indeed, an equilibrium requires that $r_\emptyset \geq \bar{r}$ because some consumers must opt in. This condition is trivially verified if $\bar{r} \leq \Phi(1,0)$, in which case we can replicate the proof of Proposition 1.

Defining

$$\begin{aligned} \bar{v}^f &= (\lambda + (1-\lambda) E(\theta)) \left[Q(\Phi(1,0)) V_1 - \bar{Q}\bar{V}_1 \right] \\ \bar{v}^n &= (\lambda + (1-\lambda) E(\theta)) \left[Q(\Phi(1,0)) V_1 - \bar{Q}\bar{V}_1 \right] \end{aligned}$$

we have:

Proposition 10 *Suppose that $r_0 < \bar{r} \leq \Phi(1,0)$. For any parameter values, there exists a unique equilibrium, such that:*

- *The website provides full privacy ($X^{**} = 1$) if $v_0 \leq \bar{v}^f$.*
- *The website's policy is random ($X^{**} \in (0,1)$) if $\bar{v}^f < v_0 < \bar{v}^n$.*
- *The website provides no privacy ($X^{**} = 0$) if $v_0 \geq \bar{v}^n$.*

Proof. As $r_\emptyset \geq \Phi(1,0) \geq \bar{r}$, it suffices to replace $Q(r_G) V_1$ and $Q(r_B) V_1$ by $\bar{Q}\bar{V}_1$ in the proof of proposition 1. ■

Notice that $\bar{v}^f$ and $\bar{v}^n$ are higher than $\psi^f V_1$ and $\psi^n V_1$ respectively. Moreover, it is easy to see that $X^{**} > X^0$ in the range of random policy. The effect of the opt-out policy is then twofold:

i) It eliminates the incentives to inspect;

ii) It raises the incentives to protect with higher levels of precaution.

In the range where $\bar{r} > \Phi(1,0)$, the previous analysis must be amended because X cannot be too small. Let us define $\bar{X}$ as the solution of

$$\Phi\left(\bar{X}, 0\right) = \bar{r}.$$

Then in any equilibrium we must have $X \leq \bar{X}$. Notice that the equilibrium is such that X decreases in v_0. As for large values of v_0 we have $X = 0$, there must exist some critical level $\bar{v}^o$ such that $X < \bar{X}$ if $v > \bar{v}^o$. In this range, the equilibrium is as above. However, for lower values of v_0, the equilibrium must involve $X = \bar{X}$ and consumers randomize between opting in and opting out.

Proposition 11 *Suppose that $\Phi(1,0) < \bar{r} < \Phi(0,0)$. For any parameter values, there exists a unique equilibrium, such that:*

- *The website's policy is random ($X^{**} \in \left(\bar{X}, 1\right)$) if $v_0 < \bar{v}^n$.*
- *The website provides no privacy ($X^{**} = 0$) if $v_0 \geq \bar{v}^n$.*

Proof. The result is the same as before when $v_0 \geq \bar{v}^o$ where $\bar{v}^o$ is defined by

$$\bar{v}^o = \lambda + (1-\lambda) E(\theta) \left[Q\left(\Phi\left(\bar{X}, 0\right)\right) V_1 - \bar{Q}\bar{V}_1 \right]$$

For smaller values of v_0, we have $X = \bar{X}$, $r_\emptyset = \bar{r}$, and

$$P_\emptyset = \frac{v_0}{\bar{v}^o} < 1.$$

It then suffices to replace $Q(r_G) V_1$ and $Q(r_B) V_1$ by $\bar{Q}\bar{V}_1$ in the proof of proposition 1. ■

8.2 Equilibrium with opt out after bad outcome

The other case of interest is when $r_B < \bar{r} < r_0$.[4] In this case, consumers opt out only after experiencing an intrusion by a malicious third party. We then notice that as far as the firm's profit is concerned, the only change introduced by an option to opt out is that the future revenue of the website when the outcome is bad is reduced from $Q(r_B) V_1$ to $\bar{Q}\bar{V}_1$.

Thus, allowing opt-out is equivalent to reducing the posterior belief after a bad outcome. More formally:

Proposition 12 *Suppose that $r_B < \bar{r} < r_0$ and define $\bar{r}_B < r_B$ as the solution of $Q(\bar{r}_B) V_1 = \bar{Q}\bar{V}_1$. Then all the results of Proposition 4, Proposition 5, Proposition 6 hold replacing r_B by $\bar{r}_B$.*

Proof. Follows immediately from the reasoning above. ■

TO BE COMPLETED

[4] Note however that our assumption that consumers do not find it optimal to opt out in the first period imposes a lower bound on $\bar{r}$. However, it is easily checked that this lower bound is less than r_0 both when consumers are myopic (i.e. they only take into account their first-period expected when they decide whether to opt out in the first period) or forward-looking.

A Appendix

Proof of proposition 4. Consider the case where $X^0 = 1$. Then, there is no inspection if $B_G \leq 0$ or

$$\frac{v_0}{V_1} \leq Q\left(\Phi\left(1,0\right)\right) - Q\left(r_G\right).$$

This is an equilibrium if in addition $v_0 \leq \psi^f$. Notice that $Q\left(\Phi\left(1,0\right)\right) - Q\left(r_\emptyset\right) \geq \psi^f$ if

$$\left(1 - E(\theta)\right) Q\left(\Phi(1,0)\right) - Q\left(r_G\right) + E(\theta) Q\left(r_B\right) \geq 0$$

Similarly for $X^0 = 0$, there is no inspection if $B_B \leq 0$ or if

$$\frac{v_0}{V_1} \geq E(\theta)\left(Q\left(\Phi\left(0,0\right)\right) - Q\left(r_B\right)\right).$$

We have $E(\theta)\left(Q\left(\Phi\left(0,0\right)\right) - Q\left(r_B\right)\right) \leq \psi^n$ if

$$\left(1 - E(\theta)\right) Q\left(\Phi(0,0)\right) - Q\left(r_G\right) + E(\theta) Q\left(r_B\right) \geq 0$$

Now suppose that X^0 is interior. Then the equilibrium condition (10) implies that

$$B_G = -\left(1-\lambda\right)\lambda\left[\left(1 - E\left(\theta\right)\right) Q\left(\Phi(X^0,0)\right) - Q\left(r_G\right) + E(\theta) Q\left(r_B\right)\right] V_1$$

and

$$B_B = -\left(1-\lambda\right)\lambda\left[\left(1 - E\left(\theta\right) Q\left(\Phi(X^0,0)\right) - Q\left(r_G\right) + E(\theta) Q\left(r_B\right)\right)\right] V_1$$

Thus we have $B_G + B_B \leq 0$ if

$$\left(1 - E\left(\theta\right)\right) Q\left(\Phi(X^0,0)\right) - Q\left(r_G\right) + E(\theta) Q\left(r_B\right) \geq 0$$

Notice that $\left(1 - E\left(\theta\right)\right) Q\left(\Phi(X^0,0)\right) + Q\left(r_G\right) - E(\theta) Q\left(r_B\right)$ decreases in X^0.Therefore we can distinguish 3 cases.

1- If $\left(1 - E(\theta)\right) Q\left(\Phi(1,0)\right) \geq Q\left(r_G\right) - E(\theta) Q\left(r_B\right)$ then this holds for all X and thus $Z = 0$ for all X^0.

2- If $\left(1 - E(\theta)\right) Q\left(\Phi(0,0)\right) \leq Q\left(r_G\right) - E(\theta) Q\left(r_B\right)$ then this holds for all X and thus $Z = 0$ only for $\frac{v_0}{V_1} \leq \underline{\psi}^i = Q\left(\Phi\left(1,0\right)\right) - Q\left(r_G\right) \leq \psi^f$ and $\frac{v_0}{V_1} \geq \bar{\psi}^i = E(\theta)\left(Q\left(\Phi\left(0,0\right)\right) - Q\left(r_B\right)\right) \geq \psi^n$.

3- If $\left(1 - E(\theta)\right) Q\left(\Phi(1,0)\right) < Q\left(r_G\right) - E(\theta) Q\left(r_B\right) < \left(1 - E(\theta)\right) Q\left(\Phi(0,0)\right)$, there exists a critical value $\bar{X}^i > 0$ such that

$$Q\left(\Phi(\bar{X}^i,0)\right) = \frac{Q\left(r_G\right) - E(\theta) Q\left(r_B\right)}{1 - E(\theta)}$$

Moreover, $E(\theta)\left(Q\left(\Phi\left(0,0\right)\right)-Q\left(r_B\right)\right)<\psi^n$. We then define

$$\bar{\psi}^i=\left[\lambda+\left(1-\lambda\right)E(\theta)\right]Q\left(\Phi(\bar{X}^i,0)\right)-\lambda Q\left(r_G\right)-\left(1-\lambda\right)E(\theta)Q\left(r_B\right)$$

and $\underline{\psi}^i=Q\left(\Phi\left(1,0\right)\right)-Q\left(r_\emptyset\right)<\psi^f$.

In any case, some inspection occurs for $\underline{\psi}^i<\frac{v_0}{V_1}<\bar{\psi}^i$ and $\underline{\psi}^i<\psi^f<\bar{\psi}^i<\psi^n$.

It remains to show that the equilibrium is unique in the range $v_0\notin\left(\underline{\psi}^i,\bar{\psi}^i\right)$. An equilibrium with inspection has $r_\emptyset=\Phi\left(X,Z\right)$ and may be of three types:

i) $X=1$: Then we must have $B_G>0$ which is not possible because

$$B_G<\lambda\left[v_0+Q\left(r_G\right)V_1-Q\left(\Phi\left(1,0\right)\right)V_1\right]\leq 0$$

for $v_0\geq\underline{\psi}^i$;

ii) $X=0$: Then we must have $B_B>0$ which is not possible because

$$B_B<\left(1-\lambda\right)\left[E(\theta)Q\left(\Phi\left(0,0\right)\right)V_1-E(\theta)Q\left(r_B\right)V_1-v_0\right]\leq 0$$

for $v_0\leq\bar{\psi}^i$;

iii) $0<X<1$: Then we must have $B_B=B_G$ which implies that equation (10) holds and thus $\Phi\left(X,Z\right)=\Phi\left(X^0,0\right)$, implying that $B_B=B_G\leq 0$, which contradicts $Z>0$. ■

Proof of Proposition 5. We have $\underline{\psi}^i=Q\left(\Phi\left(1,0\right)\right)-Q\left(r_G\right)$ and $\bar{\psi}^i=E(\theta)\left(Q\left(\Phi\left(0,0\right)\right)-Q\left(r_B\right)\right)$.

Suppose that $v_0\in\left(\underline{\psi}^i,\bar{\psi}^i\right)$.

Strong privacy regime

$X^*=1$ is an equilibrium if and only if

$$\left(\lambda+\left(1-\lambda\right)E(\theta)\right)Q\left(r_\emptyset^*\right)-\lambda Q\left(r_G\right)-\left(1-\lambda\right)E(\theta)Q\left(r_B\right)\geq\frac{v_0}{V_1}. \tag{11}$$

where $r_\emptyset^*=\Phi\left(1,Z^*\right)$ and $B_G\left(r_\emptyset^*\right)=Z^*$, which reduces to

$$V_1\left[Q\left(\Phi\left(1,Z^*\right)\right)-Q\left(r_G\right)\right]+\frac{Z^*}{\lambda}=v_0\ . \tag{12}$$

As the left-hand side of (12) is increasing in Z and less than v_0 at $Z=0$ for $v_0>\underline{\psi}^iV_1$, there exists a unique solution $Z_1\left(v_0,V_1\right)>0$ to (12). An equilibrium with $X^*=1$, $Z^*>0$ exists if and only if (denoting $\rho_1=\Phi\left(1,Z_1\right)$)

$$\left(\lambda+\left(1-\lambda\right)E(\theta)\right)Q\left(\rho_1\right)-\lambda Q\left(r_G\right)-\left(1-\lambda\right)E(\theta)Q\left(r_B\right)\geq Q\left(\rho_1\right)-Q\left(r_G\right)+\frac{Z_1}{\lambda V_1}. \tag{13}$$

which can be rewritten

$$\frac{Z_1}{\lambda V_1} + (1-\lambda)(1-E(\theta))\,Q(\rho_1) \leq (1-\lambda)\left(Q(r_G) - E(\theta)Q(r_B)\right).$$

The left-hand side is increasing in v_0 and decreasing in V_1 while the right-hand side is independent of v_0 and V_1. Therefore, there exists a threshold $\nu_s(V_1) > 0$ increasing in V_1 such that a strong privacy equilibrium exists if $v_0 \leq v_s(V_1)$. Notice that at $v_0 > \underline{\psi}^i V_1$,condition (11) is strict, which shows that $v_s(V_1) > \underline{\psi}^i V_1$.

To show that $\frac{v_s}{V_1}$ is nondecreasing with V_1,we notice that at $v_0 = v_s$, $Z = Z_s \equiv Z_1(v_s(V_1), V_1)$ and.:

$$\frac{v_s(V_1)}{V_1} = (\lambda + (1-\lambda)E(\theta))\,Q(\Phi(1, Z_s)) - \lambda Q(r_G) - (1-\lambda)E(\theta)Q(r_B) \tag{14}$$

and

$$Q(\Phi(1, Z_s)) - Q(r_G) + \frac{Z_s}{\lambda V_1} = \frac{v_s(V_1)}{V_1}. \tag{15}$$

This implies

$$\frac{Z_s}{\lambda V_1} + (1-\lambda)(1-E(\theta))\,Q(\Phi(1, Z_s)) = (1-\lambda)\left(Q(r_G) - E(\theta)Q(r_B)\right)$$

When V_1 increases, it must be the case that Z_s/V_1 decreases and Z_s increases (otherwise the LHS is monotonic in V_1). But then, it follows that $v_s(V_1)/V_1$ also increases with V_1 from equation (14).Finally, notice that equation (14) implies that $v_s(V_1) > \psi^f V_1$ because $\Phi(1, Z_s) > \Phi(1, 0)$.

Weak privacy regime

$X^* = 0$ is an equilibrium if and only if

$$[\lambda + (1-\lambda)E(\theta)]\,Q(r_\emptyset) - \lambda Q(r_G) - (1-\lambda)E(\theta)Q(r_B) \leq \frac{v_0}{V_1}. \tag{16}$$

where $r^*_\emptyset = \Phi(0, Z^*)$ and $B_B\left(r^*_\emptyset\right) = Z^*$, which reduces to

$$v_0 = E(\theta)\left(Q(\Phi(0, Z^*)) - Q(r_B)\right)V_1 - \frac{Z^*}{1-\lambda}. \tag{17}$$

Note that the RHS is decreasing in Z. If $\bar{\psi}^i = E(\theta)\left(Q(\Phi(0,0)) - Q(r_B)\right) > \psi^n$, it is larger than v_0 at $Z = 0$ and there exists a unique solution $Z_0(v_0, V_1) > 0$ to (17). Notice that Z_0 is decreasing in v_0 and increasing in V_1. A weak privacy equilibrium exists if and only if (denoting $\rho_0 = \Phi(0, Z_0)$)

$$(\lambda + (1-\lambda)\, E(\theta))\, Q(\rho_0) - \lambda Q(r_G) - (1-\lambda)\, E(\theta) Q(r_B) \leq E(\theta)\,(Q(\rho_0) - Q(r_B)) - \frac{Z_0}{(1-\lambda)\, V_1}$$

which is the same as

$$\lambda Q(r_G) - \lambda E(\theta)\, Q(r_B) - \lambda\,(1 - E(\theta))\, Q(\rho_0) - \frac{Z_0}{(1-\lambda)\, V_1} \geq 0.$$

The LHS is decreasing in Z_0 under condition C1 and, therefore, it is increasing in v_0. Thus, there exists a value of v_0, which we denote $v_w(V_1)$, where the inequality binds, and an equilibrium with weak privacy exists if and only if $v_0 \geq v_w(V_1)$. Moreover $Z_w \equiv Z_0(v_w(V_1), V_1)$ is increasing in V_1 and so $\Phi(0, Z_w)$ decreases with V_1.

At the threshold

$$\frac{v_w(V_1)}{V_1} = E(\theta)\,(Q(\Phi(0, Z_w)) - Q(r_B)) + \lambda\,(1 - E(\theta))\, Q(\Phi(0, Z_w)) - \lambda Q(r_G) + \lambda E(\theta)\, Q(r_B)$$

or

$$\frac{v_w(V_1)}{V_1} = (\lambda + (1-\lambda)\, E(\theta))\, Q(\Phi(0, Z_w)) - \lambda Q(r_G) - (1-\lambda)\, E(\theta) Q(r_B) \tag{18}$$

which decreases with V_1.

Moreover, condition 14 and $\Phi(1, Z_s) < \Phi(0, Z_w) < \Phi(0, 0)$ imply that $v_s < v_w < \psi^n V_1$.

Random privacy regime

Consider now the case $0 < X < 1$. In this equilibrium, it must be the case that $B_G\left(r_\emptyset^*\right) = B_B\left(r_\emptyset^*\right)$ so that equation (10) holds so that the posterior is the same with inspection and no inspection:

$$\Phi(X^*, Z^*) = \Phi\left(X^0, 0\right)$$

This implies in particular that $\psi^f V_1 < v_0 < \psi^n V_1$, and either $X^* > X^0 > X_\infty$ or $X^* < X^0 < X_\infty$.

At the equilibrium Z, the firm is indifferent between inspecting, blocking or selling so that

$$\frac{v_0}{V_1} = E(\theta)\left[Q\left(r_\emptyset^*\right) - Q(r_B)\right] - \frac{Z^*}{(1-\lambda)\, V_1} = \left[Q\left(r_\emptyset^\mu\right) - Q(r_G)\right] + \frac{Z^*}{\lambda V_1}. \tag{19}$$

The latter two equations yield

$$\frac{Z^*}{V_1} = (1-\lambda)\,\lambda\left[Q(r_G) - E(\theta)\, Q(r_B) - (1 - E(\theta))\, Q\left(r_\emptyset^*\right)\right] \tag{20}$$

and

$$\frac{Z^*}{V_1} = \frac{\lambda(1-\lambda)}{\lambda + (1-\lambda)\, E(\theta)}\left[E(\theta)\,(Q(r_G) - Q(r_B)) - (1 - E(\theta))\,\frac{v_0}{V_1}\right] \tag{21}$$

Moreover, conditions (20) and (21) imply condition (10). Thus, the two conditions (20) and (21) along with $r_{\emptyset}^{*} = \Phi\left(X^{*}, Z^{*}\right)$ characterize an equilibrium.

By construction, at v_s and at v_w, the website is indifferent between inspecting, blocking or selling so that (20) and (21) hold. Thus, Z^{*} solution of (21) decreases from Z_s to Z_w when v_0 increases from v_s to v_w. For any such $Z \in (Z_w, Z_s)$, a unique solution $\hat{X}(Z)$ to equation (20) exists which varies from 0 to 1 because

$$\begin{aligned} & (1-\lambda)\lambda\left[Q\left(r_G\right) - E\left(\theta\right)Q\left(r_B\right) - \left(1-E\left(\theta\right)\right)Q\left(\Phi\left(1,Z\right)\right)\right] \\ > \quad & (1-\lambda)\lambda\left[Q\left(r_G\right) - E\left(\theta\right)Q\left(r_B\right) - \left(1-E\left(\theta\right)\right)Q\left(\Phi\left(1,Z_s\right)\right)\right] = \frac{Z_s}{V_1} > \frac{Z}{V_1} \end{aligned}$$

and

$$\begin{aligned} & (1-\lambda)\lambda\left[Q\left(r_G\right) - E\left(\theta\right)Q\left(r_B\right) - \left(1-E\left(\theta\right)\right)Q\left(\Phi\left(0,Z\right)\right)\right] \\ < \quad & (1-\lambda)\lambda\left[Q\left(r_G\right) - E\left(\theta\right)Q\left(r_B\right) - \left(1-E\left(\theta\right)\right)Q\left(\Phi\left(0,Z_w\right)\right)\right] = \frac{Z_w}{V_1} < \frac{Z}{V_1} \end{aligned}$$

Note that it must be the case that $r_{\emptyset}^{*}$ increases with v_0.

Notice that a mixed strategy equilibrium exists only if $v_s < v_0 < v_w$ because outside this range the equilibrium value of Z would require X negative or larger than 1. Hence the equilibrium is unique. ■

Proof of Proposition 4.

The proof is the same as for Proposition 5 with the following two differences:

- First, the weak privacy regime with $Z > 0$ doesn't exist.

- Second, in the range $v_0 \in \left(v_s, \bar{\psi}^{i}\right)$, conditions (20) and (21) hold at $\bar{\psi}^{i}$ for $Z = 0$ and $X = \bar{X}^{i} > 0$. Thus, we have $Z \in (0, Z_s)$ and no equilibrium with inspection can occur above $\bar{\psi}^{i}$. For $Z \in (0, Z^{s})$ a solution X of (20) exists in $(0,1)$. ■

References

[1] Acquisti, A, Taylor, C., and L. Wagman (2015), "The Economics of Privacy," mimeo.

[2] Acquisti, A., and H. Varian (2005), "Conditioning Prices on Purchase History," *Marketing Science* 24:3, 367-381.

[3] Bergemann, D., and A. Bonatti (2015), "Selling Cookies," *American Economic Journal: Microeconomics*, 7(3): 259-94.

[4] Calzolari, G., and A. Pavan (2006), "On the Optimality of Privacy in Sequential Contracting," *Journal of Economic Theory*, 130:1, 168-204.

[5] de Cornière, A., and R. De Nijs (2015), "Online Advertising and Privacy", *The RAND Journal of Economics*, forthcoming.

[6] Goldfarb, A., and C. Tucker (2011), "Privacy Regulation and Online Advertising," *Management Science*, 57(1), 57-71.

[7] Hermalin, B. and M. Katz (2006), "Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy," *Quantitative Marketing and Economics*, 4:3, 209-239.

[8] Kox, H., Straathof, B., and G. Zwart (2015), "Targeted Advertising, Platform Competition and Privacy", mimeo.

[9] O'Brien, D.P., and D. Smith (2014), "Privacy in Online Markets: A Welfare Analysis of Demand Rotations," *FTC Bureau of Economics Working Paper*.

[10] Taylor, C. (2004), "Consumer Privacy and the Market for Customer Information," *The RAND Journal of Economics*, 35:4, 631-650.

[11] Taylor, C., and L. Wagman (2014), "Consumer Privacy in Oligopolistic Markets: Winners, Losers, and Welfare," *International Journal of Industrial Organization*, 34, 80-84.