Digital Privacy*

Itay P. Fainmesser† Andrea Galeotti‡ Ruslan Momot§

First Draft: September 2019. This Draft: April 2022.

Abstract

We study the incentives of a digital business to collect and protect users' data. The users' data the business collects improve the service it provides to consumers, but they may also be accessed, at a cost, by strategic third parties in a way that harms users, imposing endogenous users' privacy costs. We characterize how the revenue model of the business shapes its optimal data strategy: collection and protection of users' data. A business with a more *data-driven* revenue model will collect more users' data and provide more data protection than a similar business that is more *usage-driven*. Consequently, if users have small direct benefit from data collection, then more usage-driven businesses generate larger consumer surplus than their more data-driven counterparts (the reverse holds if users have large direct benefit from data collection). Relative to the socially desired data strategy, the business may over- or under-collect users' data and may over- or under-protect it. Restoring efficiency requires a two-pronged regulatory policy, covering both data collection and data protection; one such policy combines a minimal data protection requirement with a tax proportional to the amount of collected data. We finally show that existing regulation in the US, which focuses only on data protection, may even harm consumer surplus and overall welfare.

"The problem with data protection laws is that it presumes the data collection was ok."

Eduard Snowden, NSA whistleblower

September 19, 2019

*We thank Susan Athey, Heski Bar-Issac, Otávio Bartalotti, Roland Bénabou, Devesh Raval, Douglas S. Smith, Long Chen, and participants of talks and seminars at the Retreat on Networks, Information, and Social Economics (RINSE); INFORMS; MSOM; London Business School; Paris School of Economics; Toulouse School of Economics; Privacy Workshop at Princeton University; University of Pennsylvania; Tepper School of Business, Carnegie Mellon University; Renmin University; Hong Kong Baptist University; Nanyang Technological University; Northwestern University, Kellogg School of Management; Microsoft Research New York; Kelley School of Business, Indiana University; David Eccles School of Business, the University of Utah; Rady School of Management, the University of California San Diego; Luohan Academy; Virtual Finance Theory Seminar (VFTS), École Polytechnique CREST; and the Federal Trade Commission for helpful comments and discussions. Andrea Galeotti gratefully acknowledges financial support from European Research Council through the ERC-consolidator grant (award no. 724356). Ruslan Momot gratefully acknowledges financial support from HEC Paris Foundation and a grant of the French National Research Agency (ANR), "Investissements d'Avenir" (LabEx Ecodec/ANR-11-LABX-0047).

†The Johns Hopkins Carey Business School and The Department of Economics, The Johns Hopkins University, Baltimore, MD 21202 (e-mail: itay_fainmesser@jhu.edu)

‡Department of Economics, London Business School, London, NW1 4SA, United Kingdom (e-mail: agaleotti@london.edu)

§Operations Department, Kellogg School of Management, The Northwestern University, Evanston, IL 60208 (e-mail: ruslan.momot@kellogg.northwestern.edu)

1. Introduction

The growing social and economic activity conducted online – from sharing location data on Uber to searching for medications or diagnoses on Google – generates extensive amounts of data. These data are used to improve products and services offered to consumers, but there are also undesirable consequences. From firms like Cambridge Analytica using Facebook data to sway election outcomes and manipulate public opinion to health insurance companies anticipating medical needs of potential insurees based on undisclosed personal data – opportunities for user data exploitation are rife.[1] These and other numerous privacy scandals and data breaches of recent years have further raised consumer privacy concerns and data privacy has been singled out as one of the biggest challenges faced by the digital economy.[2] Governments responded with new data privacy laws and regulations, which, as argued by many, are only partially effective at best.[3]

This paper addresses four fundamental questions: (1) What are the trade-offs that people face when using online services? (2) What are the determinants of harmful use of users' data? (3) What are the incentives of digital businesses to collect and protect users' data? and (4) What actions should be taken by regulatory authorities in order to protect consumer privacy and maximize social welfare?

We develop an economic model of the creation, collection, protection, and potential misuse of users' data (Section 2). We focus on *activity data*: information on users' interactions with the digital business's services such as users' posts, messages, clicks, etc.[4] A digital business chooses a *data strategy* which comprises a choice of data collection and data protection. The *data collection strategy* specifies the proportion of users' activity that is collected, stored, and processed by the business. Examples include the decision by Whatsapp to encrypt users' text messages (thus reducing the amount of information it collects) and Facebook's practices (at least until August 2019) of

[1] A few articles that illustrate these undesirable consequences are "How Trump Consultants Exploited the Facebook Data of Millions", *New York Times*, 17 March 2018 (see also Papanastasiou 2020 and Candogan and Drakopoulos 2020),and " 'We've Been Breached': Inside the Equifax Hack", *Wall Street Journal*, 18 September 2017

[2] "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information", Pew Research Center, 15 November 2019.

[3] "Edward Snowden Thinks Even The EU's Sweeping Privacy Law Is Too Weak", *Forbes*, 5 November 2019; "What Does California's New Data Privacy Law Mean? Nobody Agrees", *New York Times*, 29 December 2019.

[4] Our results carry over to when *registration data* is considered. Such data may include the name, age, gender, credit card number of the user, etc. For a discussion of data types collected by digital businesses see "How Businesses Are Collecting Data (And What They're Doing With It)", *Business News Daily*, 17 June 2020. The formal analysis of registration data is available in Online Appendix C.4.

transcribing users' audio chats (thereby increasing the amount of accessible information it stores) as well as of retaining information from deleted accounts.[5] The *data protection strategy* specifies a costly investment that determines how difficult it is for third parties to access stored data (e.g., see De Cornière and Taylor 2020). Examples include investment in firewall enhancements, API updates, and hiring ethical hackers who help the business in detecting and repairing vulnerabilities.

Users choose how much time to spend using the business's services. The more active the users are, the more data the business can collect about them. These collected data are then used by the business to offer higher quality service, which furnishes *positive externalities* to users. At the same time, data collection raises users' privacy concerns – *negative externalities* – the risk that users perceive from their data being potentially accessed and misused by the third parties – hereafter *adversaries*.

We explicitly model the strategic interaction between users and adversaries. Therefore, users' demand for the business's services and adversaries' demand for users' data are both endogenous. This provides a natural economic definition of privacy costs and reveals a new channel of *negative network effects* – as average users' activity increases, more information is collected and the platform attracts more adversarial activity, decreasing both the total and marginal utility of each user from using the business's services. These data-driven negative network effects make the implicit marginal costs of data collection to the business increase in the total amount of data collected. To the best of our knowledge, this is a novel feature in the literature on data privacy.

Another important feature of our framework is that we allow for different revenue models of the business. We postulate that the business's profit is an increasing function of users' demand for service and of the data collected by the business. At the one extreme, we have *purely data-driven* digital businesses whose sole source of revenue stems from selling data or data-based services to third-parties. Examples include weather apps, most of which are free and do not display advertisements, but rather collect user location data and sell it to data aggregators such as Acxiom and Infogroup. At the other extreme, we distinguish *purely usage-driven* businesses that collect users' payments in the form of subscription fees or commissions. Ride-hailing platforms Uber and Lyft, and many online

[5]See, for example, "WhatsApp Introduces End-to-End Encryption", *New York Times*, 5 April 2016., and also "Facebook Paid Contractors to Transcribe Users' Audio Chats", *Bloomberg*, 13 August 2019 and "OK, You've Deleted Facebook, but Is Your Data Still Out There?", *CBS News*, 23 March 2018.

dating services, are some of the numerous examples of such businesses. Between these two extremes, lie ad-driven companies like Facebook and Google, whose main source of revenue is offering targeted advertisements and, therefore, they capitalize directly on the users' information they collects. At the same time, these businesses also attaches a direct value to user activity because they need users to be active for them to view and click on the ads.[6]

We first characterize, in Section 3, how different data strategies shape users' demand for the business's services and the adversaries' demand for users' data (Proposition 1). We show that, as the business's data collection strategy becomes more expansive, users' activity first increases and then decreases. The resulting amount of users' data that is actually collected by the business, follows a similar pattern. Such non-monotonicity reflects the endogenous reaction of adversarial activity to the change in the data collection strategy that, in turn, shapes users' privacy costs. When the data collection strategy is restricted, users' privacy costs are low because only a handful of adversaries are active. Hence, an increase in data collection improves the service to users at a little privacy cost. As the business collects data on a larger fraction of users' activity, adversaries' activity also increases, thereby imposing larger privacy costs on users, who, in turn, reduce their activity. With respect to the data protection strategy, we show that an increase in data protection reduces adversarial activity and, therefore, lowers privacy costs and increases both average users' activity and total users' data collected.

Our second set of results, in Section 4, provides a characterization of the optimal business data strategy (Theorem 1). We show that data-collection and data-protection are complementary instruments in generating profit for the business. This implies that, all else equal, a more data-driven digital business sets higher levels of data collection and data protection. Consequently, if users have small direct benefit from data collection, then usage-driven businesses generate larger consumer surplus than their more data-driven counterparts. The opposite is true if users' direct benefit from data collection are significant (Proposition 2)

Section 5 compares the business's data strategy with the data strategy that maximizes social welfare (a weighted sum of consumer surplus and the business's profit). Theorem 2 shows that

[6]The exact way that an advertisement-driven company weighs users' activity vs. collected data may depend, among other things, on the life cycle of the business: at the startup phase, the objective is, generally, to maximize activity as this is the metric that allows raising capital through investors. As the platform matures, the weight is often shifted towards monetizing collected data.

a business may, relative to the social optimal policy, over-collect and over-protect users' data, over-collect and under-protect, or under-collect and under-protect, depending on the parameters of the model and, in particular, the business's revenue model. To complement this result, our numerical analysis shows that, typically, businesses with significant usage-driven revenue components tend to under-collect and under-protect users' data, whereas businesses with revenue models that include significant data-driven components tend to over-collect users' data and often also over-protect it.

There are three implications of this comparison. First, a data strategy policy must take into considerations the underlying business model. For example, a policy that regulates only one dimension of the data strategy, say data protection, should incentivize data protection investments for usage-driven businesses, and may need to disincentivize such investments for data-driven businesses. Second, it is difficult to restore efficiency with a regulation that focuses only on one aspect of the data policy. For example, the practice of the US Federal Trade Commission (FTC), which has a mandate to enforce a minimum level of data protection, is not sufficient to restore efficiency.[7] In fact, Proposition 3 shows that such regulations may even decrease consumer surplus and overall welfare, especially when a business's revenue model is intermediate, putting similar weights on data and usage. Third, efficiency can be restored by a two-pronged regulatory policy that combines a requirement of a minimum level of data protection together with either a liability policy or a tax on stored data (Proposition 4). The challenge of implementing this policy is how to measure data collection in order to properly calibrate the tax/liability rate.

We discuss broader policy implications in Section 6; Section 7 offers a review of related literature and provides concluding remarks. All proofs are given in Appendix A.

2. Model

A digital business (*it*) chooses a data strategy that specifies: a) what proportion of users' activity the business records and stores – a *data collection strategy*, and b) a costly investment in data protection – *a data protection strategy*.[8] Each user (*she*) decides how much to use the services provided by

[7] See, for example, the case of FTC vs D-Link: "D-Link agrees to 10 years of security audits to settle FTC case", *The Verge*, 4 Jul 2019; https://www.ftc.gov/enforcement/cases-proceedings/132-3157/d-link.

[8] We focus on a monopolistic digital business. However, we note that even if the business is not in direct competition with other platforms it still faces pressures in choosing a data policy that provides users sufficient value for them to

the business – her *activity level*. By analyzing the stored users' activity data, the business learns about relevant users' characteristics and provides higher quality services to them. Third parties (henceforth, *adversaries*) can, at a cost that is increasing in the business's data protection investment, attempt to access and use the data for purposes that are not in line with users' preferences. Thus, if successful, an adversary (*he*) can harm users. We next introduce formally these elements.

2.1. Users

There is a unit mass of users of a digital business. Each user i chooses activity level $a_i \in \mathbb{R}^+$, which can be thought of as the amount of time that the user spends using the business's services. A proportion $\xi \in [0,1]$ of each user's activity is recorded and stored by the business, and therefore, $a_i\xi$ is the total amount of stored data on user i's activity (here, ξ is the business's data collection strategy, to be specified in Section 2.3). Denote by $\bar{a} = \int_j a_j \, \mathrm{d}j$, the average user activity. We assume that users are homogeneous, and that the utility of user i is as follows:[9]

$$U_i(a_i, \bar{a}) = \underbrace{a_i - \frac{1}{2}a_i^2}_{\text{standalone benefit and cost}} + \underbrace{\beta a_i \bar{a}}_{\text{network effects}} + \underbrace{(\rho - \omega) f(a_i\xi)}_{\text{positive and negative information externalities}}.$$

The first term summarizes user i's standalone benefits and costs of using the service. The second term introduces classical positive network effects that are parameterized by $\beta \in [0,1)$.[10] The last term captures positive and negative information externalities imposed on user i due to user's profiling by the business and third parties. Informally, the data collected on user's activity, $a_i\xi$, allow an entity in possession of these data to learn with probability $f(a_i\xi)$ some of user i's traits. Upon learning the user's traits, the business can offer her better services, as captured by the positive externalities $\rho f(a_i\xi)$, where $\rho \in [0,1)$. However, profiling by individuals, firms, and governments who exploit users' data and pursue goals that are in conflict with users' preferences, imposes negative externalities on the user. These are captured by $-\omega f(a_i\xi)$, where $\omega \geq 0$ is the expected number of

engage with the services offered by the business. Adding multiple digital businesses competing for users' attention would allow to understand how competitive forces may discipline further the choice of the data policy and alleviate inefficiencies.

[9] In Online Appendix C.1 we extend the analysis to allow for multiple dimensions of users' heterogeneity. Furthermore, the linear-quadratic specification of users' preferences allows us to derive closed-form solutions, but the qualitative results generalize beyond this specification; see the formal discussion in Online Appendix C.2.

[10] The specification of network effects is widely used in network economics literature (see, e.g., Bloch and Quérou 2013, Candogan et al. 2012, Fainmesser and Galeotti 2016, to name a few). The assumption that $\beta < 1$ guarantees that there is a unique activity level in equilibrium.

such adversarial activities and we refer to it as the *demand for user information from adversaries*; we explain how it is derived in Section 2.2. In Online Appendix C.3 we provide a formal example of profiling.[11]

Remark 1 *Some digital businesses collect data about users primarily during registration. These data often include demographic and financial information (e.g., age, address, credit card details). In this case, when it comes to privacy concerns, the most important choice faced by users is whether to register to the service. That is, users' choices, instead of reflecting engagement, are discrete: users decide whether to register or not on the platform. The business, in turn, can determine what information is required to complete registration to the service (the parameter ξ). For example, the business may require storing credit card information on file, which will facilitate seamless future transactions and be beneficial for consumers. However, storing credit card information may also introduce concerns of credit card fraud by third party adversaries. In Online Appendix C.4 we re-formulate the model and show that all of our results carry over to these settings with no change.*

To simplify our presentation and obtain closed-form solutions, we assume for the remainder of the paper that $f(a_i\xi) = a_i\xi$ and therefore user i's utility becomes:

$$U_i(a_i, \bar{a}) = a_i - \frac{1}{2}a_i^2 + \beta a_i \bar{a} + (\rho - \omega)a_i\xi. \tag{1}$$

2.2. Adversaries

There is a large number M of potential adversaries, who are heterogeneous in their cost to access information collected by the digital business. This heterogeneity is captured by the parameter γ, which is drawn for each adversary from a uniform distribution over $[0, M]$ (see Online Appendix C.2 for a generalization to non-uniform distributions). An adversary observes his own γ and chooses whether to be active (action 1) or not (action 0). The gain to an inactive adversary is his outside option, which we normalize to zero ($\pi(0|\gamma) = 0$). An active adversary with characteristic γ incurs a

[11] Information is modeled as a one-dimensional variable, which means that the information about users that is valuable to the business is the same as the one that is valuable to the adversaries. This assumption is partly justified by the correlation across information types that are exploited by AI. However, by taking into account the multidimensional structure of information, one could explore how different businesses may choose to collect different attributes and to what extent it is possible for the business to collect data without attracting adversarial actions. This question is related to the field of differential privacy and additional research in computer science, operations research, and related fields.

fixed cost γC to access the data collected by the business on all users and gains $\bar{a}\xi$. C describes how well data are protected against misuse by third parties and it is a choice of the business. The total payoff expected by an active adversary with γ is then:[12]

$$\pi(1|\gamma) = \bar{a}\xi - \gamma C.$$

To simplify the presentation of the results, we let $M \to \infty$. This assumption does not have an effect on our qualitative insights, and the only role it plays is to ensure that the number of adversaries who are active and the number of those who are inactive, are both strictly positive.

2.3. The Digital Business

The digital business chooses a data strategy that consists of:

(a) A data collection strategy: a proportion $\xi \in [0, 1]$ of each user i's activity a_i that is collected, stored, and processed by the business;

(b) A data protection strategy: a protection level $C \geq 0$ at a cost ψC for some $\psi \geq 0$.

The objective of the business is a function which is increasing in users' activity, $\bar{a}$, and in the amount of users' activity that the business records – collected data, $\xi\bar{a}$. Where not stated otherwise, we focus on a linear profit function that takes the following form:

$$\Pi(\xi, C) = (1 - P) \cdot \bar{a} + P \cdot \xi\bar{a} - \psi C \tag{2}$$

where $P \in [0, 1]$. That is, $1 - P$ is the additional profit to the business from a marginal increase in users' activity, ceteris-paribus, and P is the additional profit to the business from a marginal increase in data collected by the business. In that sense, $1 - P$ and P are, respectively, the "prices" that the business extracts for each unit of user activity and for each unit of user data collected, respectively.

A *purely data-driven* business's sole source of revenue is the sale of data or data-based services to third parties. For such businesses, $P = 1$. A *purely usage-driven* business's source of revenue are the payments made by users in the form of subscription fees or commissions. For such businesses,

[12] Another interpretation of this model of the adversary is that there is a mass of adversaries, who upon gaining access to the digital business's data, attack one user chosen uniformly at random.

$P = 0$. Between these two extremes, we have advertisement-driven companies, like Facebook and Google, who capitalize directly on users' data that they collect by selling ads, but that also attach a direct value to users' activity, since users have to be active to view and click on the ads.

Remark 2 *The linear formulation of the business's profit function is chosen for analytical tractability and allows us to develop clear intuitions. However, our main results extend to a model in which the business's profit function is much more general and takes the following form:*

$$\Pi(\xi, C) = \Phi(\bar{a}, \xi\bar{a}) - K(C).$$

The analysis for this formulation imposes standard smoothness/concavity/convexity assumptions on the function $\Phi(\cdot, \cdot)$ *and has the linear case as a special case; the details are available in Appendix C.5.*

2.4. Timeline and Equilibrium Concept

We consider the following sequential game. In the first stage, the digital business chooses its data strategy and the choice is observed by users and adversaries. Then, users choose their activity levels and, simultaneously, adversaries decide whether or not to be active.[13] The strategy of a digital business is its data strategy: $\xi \in [0, 1]$ and $C \in \mathbb{R}_+$. User i's strategy is a function $a_i \colon [0, 1] \times \mathbb{R}_+ \to \mathbb{R}_+$ that specifies user i's activity for every possible data strategy, (ξ, C). The strategy of an adversary is a function $v_j \colon [0, M] \times [0, 1] \times \mathbb{R}_+ \to \{0, 1\}$ that specifies, for every possible $\gamma \in [0, M]$ and data strategy (ξ, C) whether adversary j is active and attempts to access the business's database. We use $\mathbf{a}$ and $\mathbf{v}$ to denote the *strategy profiles* of users and adversaries respectively. We focus on perfect Bayesian equilibria of the game: a data strategy choice (ξ^*, C^*) and a strategy profile $(\mathbf{a}^*, \mathbf{v}^*)$ such that: (a) the digital business maximizes its profit given $(\mathbf{a}^*, \mathbf{v}^*)$; and (b) for every ξ and C, $(\mathbf{a}^*, \mathbf{v}^*)$ is a Bayesian equilibrium in the ensuing subgame.[14]

[13] The assumption that users know the data strategy of the digital business can be easily relaxed. We clarify this in Section 6.1 where we discuss policies that attempt to increase users' awareness like the EU's GDPR regulation.

[14] In each subgame, users and adversaries have a common prior that γ is uniformly distributed between 0 and M.

3. The Users-Adversaries Game

Our first result clarifies how the equilibrium users' and adversaries' activities depend on the business data strategy.

Proposition 1 *Fix the business's data strategy (ξ, C). The ensuing subgame has a unique equilibrium in which users' and adversaries' activities are:*

$$\bar{a}^*(\xi, C) = \frac{C(1+\rho\xi)}{C(1-\beta)+\xi^2} \quad \textit{and} \quad \omega^*(\xi, C) = \frac{\xi\bar{a}^*(\xi, C)}{C}, \tag{3}$$

and the resulting consumer surplus is:

$$\mathrm{CS}(\xi, C) = \frac{1}{2}\bar{a}^*(\xi, C)^2. \tag{4}$$

Furthermore, equilibrium users' activity, $\bar{a}^*(\xi, C)$ and users' data collected, $\xi\bar{a}^*(\xi, C)$ both: (a) Increase in data protection C; (b) First increase and then decrease in data collection ξ.[15]

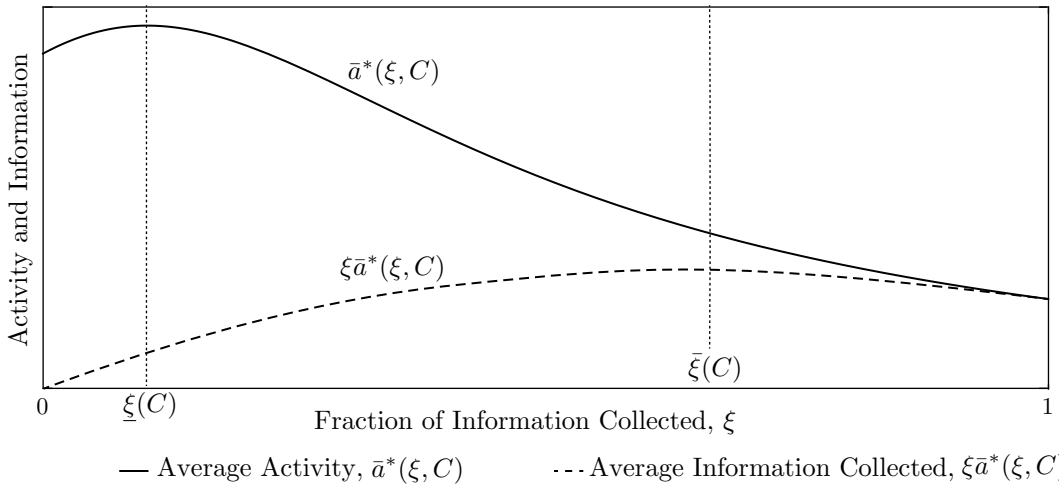

Figure 1: Users' activity $\bar{a}^*(\xi, C)$ and data collected $\xi\bar{a}^*(\xi, C)$ as a function of data collection ξ.

An increase in data protection decreases the adversaries' demand for stored data, thereby decreasing users' privacy concerns. This, in turn, increases users' activity in the business. More subtle is the effect of a change in the data collection strategy on users' activity and information collected; this is illustrated in Figure 1. By collecting larger proportions of users' data (increasing ξ), the digital business creates new benefits for users since it can then offer tailored services based

[15] In particular, there exist $0 \leq \underline{\xi}(C) \leq \bar{\xi}(C)$ such that (i) $\bar{a}^*(\xi, C)$ increases with ξ for $\xi \in [0, \underline{\xi}(C)]$ and decreases otherwise; (ii) $\xi\bar{a}^*(\xi, C)$ increases with ξ for $\xi \in [0, \bar{\xi}(C)]$ and decreases otherwise.

on users' information. Consequently, users' demand for the business's service increases. At the same time, increasing ξ also boosts adversaries' demand for information. This creates a negative externality on users' participation and offsets the increase in users' demand for the business. Which effect dominates depends on the level of ξ.

Adversaries impose small costs on users when ξ is small and, therefore, an increase in ξ will increase users' activity. With increasing ξ further, the stored dataset becomes more valuable to adversaries and thus they have more to gain from the attack; this leads to further increase not only in adversaries' demand for users' data but also in the loss that users suffer from each adversarial action. At some point, these negative effects outweigh the benefits to users from their information being used for tailored services. When this happens, users' average activity starts declining in ξ.

Even though users' average activity declines in ξ for every $\xi > \underline{\xi}(C)$, total information collected by the business keeps increasing when $\xi \in [\underline{\xi}(C), \bar{\xi}(C)]$. In this region, negative externalities imposed by adversaries on users are sufficiently significant to lead to a decrease in usage, but not severe enough to make this decrease large. It is only when $\xi > \bar{\xi}(C)$ that any additional increase in ξ leads to a decrease in users' activity that is steep enough to reduce total information collected, notwithstanding an increase in the fraction of information stored.

4. Data Strategy

We characterize the business's strategy, and show that a more data-driven business will collect a higher fraction of the data generated by users' activity and, at the same time, provide more data protection. How this increase in data collection and data protection shapes consumer surplus depends on the direct benefit to consumer from data collection.

Theorem 1 *The digital business's data collection, $\xi^\star$ and data protection, $C^\star$ are:*

$$\xi^\star = \max\Big\{0,\, \min\Big\{1,\, \frac{1}{2P\rho}\Big(-(1-P)\rho - P + |P-(1-P)\rho| \cdot \sqrt{\frac{\psi}{\max\{0, \psi - P\rho\}}}\Big)\Big\}\Big\}, \tag{5}$$

$$C^\star = \frac{\xi^\star}{1-\beta} \cdot \Big(-\xi^\star + \sqrt{\frac{1}{\psi}(1+\rho\xi^\star)(1-P(1-\xi^\star))}\Big). \tag{6}$$

All else equal, a more data-driven digital business (i.e., higher P) sets weakly higher levels of data

collection, $\xi^\star$ and data protection, $C^\star$.

Figure 2 illustrates how equilibrium data collection and protection change with the business's revenue model. That a more data-driven business collects a larger fraction of the data generated by users is intuitive. More subtle is the intuition for the difference in data protection. As a business collects more data, it attracts more adversarial activity, and, as a result, is required to protect the data more to prevent a significant decrease in users' activity. In other words, the digital business's data collection and data protection strategies are complements, as captured by the positive cross partial derivative of the business's profit function with respect to ξ and C at the equilibrium strategy. This complementarity between data collection and data protection is robust to a more general specification of the business objective (see Proposition 6 in Online Appendix C.5) and it leads to many interesting economic insights, as we elaborate in the next sections.

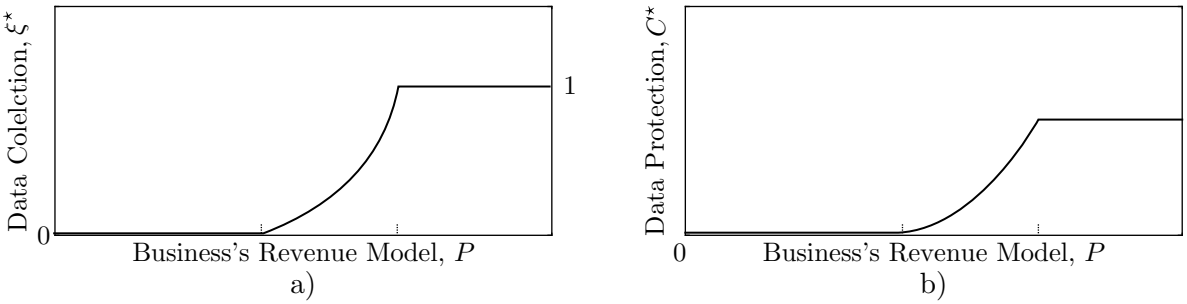

Figure 2: Equilibrium data collection and data protection strategies as a function of the business's revenue model, P (higher P implies a more data-driven business model).

4.1. Consumer Surplus

We next show that depending on the direct benefits to consumers from data collection, consumers may be better or worse off from the business having a more data-driven revenue model.

Proposition 2 *If $P < \rho/(1+\rho)$, then a more data-driven digital business (i.e., higher P) generates weakly higher consumer surplus,* $\mathrm{CS}(\xi^\star, C^\star)$. *Otherwise,* $\mathrm{CS}(\xi^\star, C^\star)$ *weakly decreases with P.*

Proposition 2 tells us that there is a best revenue model from users' prospective, that is, consumer surplus is the highest when the business's revenue model is set at an intermediate level $P = \rho/(1+\rho)$. To understand the intuition behind the result, we first note that consumer surplus is proportional to the square of the average users' activity level. Hence businesses that lead to high consumer

surplus are those who choose a data policy that generates a lot of users' activity. Second, as we move on the spectrum from usage- to data-driven revenue models, both data protection and data collection increase (see Theorem 1). This generates two conflicting effects. On the one hand, for a given data protection level, the increase in data collection leads to a decrease in users' activity. On the other hand, for a given data collection level, the increase in data protection increases users' activity. Which effect dominates depends on the the revenue model, P and on the direct utility users have from data collection, ρ. When ρ is small, average activity is very sensitive to changes in data collection. This implies that for a large range of values of P, a shift towards a more data-driven revenue model has an overall negative effect on average activity and subsequently on consumer surplus. The opposite intuition holds when ρ is large.

5. Socially Optimal Strategies and Regulatory Policy

In this section we compare the business's choice of data strategy with the choice of a benevolent social planner. This highlights the sources of inefficiencies in data collection and data protection, and allows us to evaluate the strengths and weaknesses of existing regulations and to propose efficient regulations. The social planner chooses a data strategy to maximize the weighted average of consumer surplus and the business's profit. Hence, the planner's prescribed data strategy, ξ^W, C^W (here the superscript W stands for *welfare*) solves the following problem:

$$(\xi^W, C^W) = \arg \max_{\substack{\xi \in [0,1] \\ C \geq 0}} \alpha \text{CS}(\xi, C) + (1-\alpha)\Pi(\xi, C), \tag{7}$$

where $\alpha \in [0,1]$. Note that the business's data strategy given by $(\xi^\star, C^\star)$ is the solution to problem 7 under the special case of $\alpha = 0$.

Theorem 2 *Relative to the socially optimal strategy, the equilibrium data strategy of a purely usage-driven business ($P = 0$) prescribes under-collection and under-protection of users' data, i.e., $\xi^\star \leq \xi^W$ and $C^\star \leq C^W$. The equilibrium data strategy of a business with any data-driven component in its revenue model ($P > 0$) never prescribes under-collection and over-protection of users' data i.e., it is never the case that $\xi^\star \leq \xi^W$ and $C^\star \geq C^W$ with at least one of the inequalities being strict. Any other direction in which the optimal business's data strategy deviates from the socially optimal*

strategy is the outcome for some specification of the business's revenue model and values of other model parameters.

Theorem 2 implies that while the business never simultaneously under-collects and over-protects users' data (as compared to the socially optimal strategy), any of the following relationships between the business's data strategy and the socially optimal strategy is possible:

1. over-collection & over-protection: $\xi^\star > \xi^W$ and $C^\star > C^W$;
2. over-collection & under-protection: $\xi^\star \geq \xi^W$ and $C^\star \leq C^W$;
3. under-collection & under-protection: $\xi^\star < \xi^W$ and $C^\star < C^W$.

We obtain more definite characterizations for special cases.[16] But we were not able to do so generally. We can however rely on numerical analysis to get a better picture of how the business's revenue model, P, and the direct benefit for consumers from data-collection, ρ, jointly determine the misalignment between the socially optimal and the business's data strategies. Figure 4 summarizes this numerical analysis.

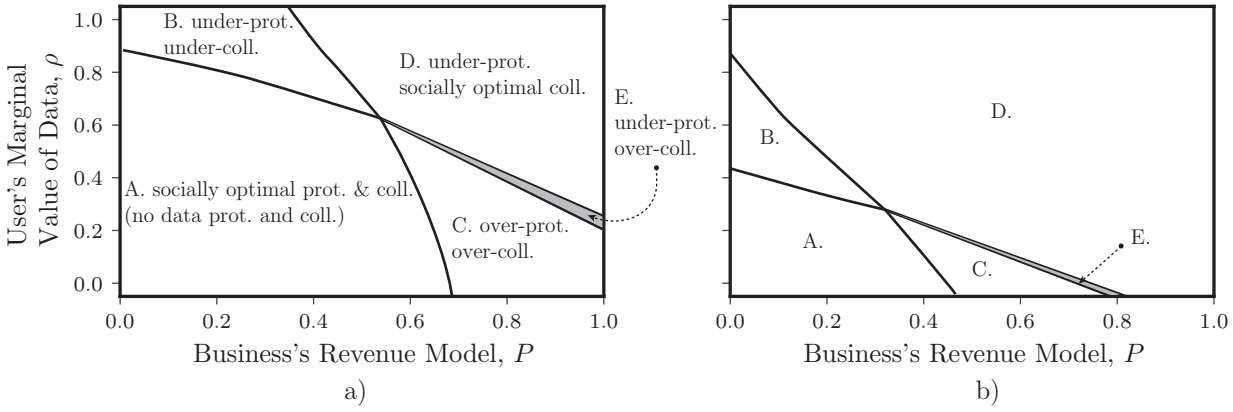

Figure 3: Regions of inefficiencies in the business's data strategy relative to the socially optimal strategy, as a function of the business's revenue model, P, and users' marginal value of data, ρ. The numerical example is generated with the following parameters: $\alpha = 0.5, \beta = 0$ and (a) $\psi = 0.35$; (b) $\psi = 0.1$.

When the business is sufficiently usage-driven and when the value of data to users is low (region A in Figure 4) the benefits from data collection are too low to justify the cost of data protection, both from the business's and the socially optimal perspective. In that case, the business collects no data and this is efficient. There are then three main regions.

[16] For example, if users do not receive benefit from data collection (i.e., if $\rho = 0$), then the equilibrium data strategy always prescribes over-collection of users' data (i.e., $\xi^\star \geq \xi^W$), see appendix C.6.

When the business is sufficiently usage-driven and the value of data to users is sufficiently high (region B), the business under-protects the information relative to the socially optimal and, because of the complementary in the business's data strategy, it also under-collects data. The reverse occurs in region C where the business is sufficiently data-driven and the value of data to users is low. In this case the platform over-collects data, and, to keep users active, it also over-protects the data. In region D the value of users' data is high enough for both the social planner and the business to optimally collect all available information. Yet, despite the efficient data collection, the digital business under-protects the data.

These four regions are the typical regions that we have observed through numerical analysis. The shaded region E in Figure 4 illustrates that there is another possibility, which is less prevalent. This is when the business revenue model is sufficiently data-driven and the users' value of data is moderate. In this case the platform over-collects and under-protects relative to the planner. We stress that the intricacies of the possible misalignment of social and business incentives illustrated in Theorem 2 and Figure 4 result from the fact that the data policy is multi-dimensional: it prescribes both collection and protection of data.[17] An important implication of these results is that regulation that aims at reconciling the private incentives of a business with the social planner's objective must regulate both components of the data strategy, i.e., both data protection and data collection. We expand on this point in the next two sections.

5.1. Existing Regulations

The US Federal Trade Commission (FTC) has a mandate to enforce a minimal level of data protection.[18] In our model, such requirement maps into guaranteeing a level of data protection C not lower than a certain threshold. We now show that a minimal data protection requirement is insufficient to achieve social efficiency and it may, in fact, decrease consumer surplus, profits, and overall welfare. In particular, we show that whether a minimal data protection requirement is beneficial to consumers depends on the business's revenue model, P, the direct benefit to consumers

[17] Indeed, when either data-collection or data-protection are held fixed we get straightforward results and these are available in Proposition 5 in appendix C.5.

[18] For instance, in recent settlements with Zoom and D-Link, FTC required these companies to enhance their data protection: "FTC Requires Zoom to Enhance its Security Practices as Part of Settlement", 9 November 2020, https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement, and "D-Link Agrees to Make Security Enhancements to Settle FTC Litigation", 2 July 2019, https://www.ftc.gov/news-events/press-releases/2019/07/d-link-agrees-make-security-enhancements-settle-ftc-litigation.

from data collection, ρ, and the cost of data protection, ψ.

Consider a regulatory imposed minimal data protection level $C_{\min}$ such that the business is obligated to choose a protection level $C > C_{\min}$. We focus on the relevant case for which the regulation is binding with respect to the business's incentives for data protection investment (i.e., $C_{\min} \geq C^\star$). The next proposition shows that even when $C_{\min}$ is only slightly larger than $C^\star$, it may lead to a decrease in consumer surplus. Because regulations that impose a minimum level of data protection always reduced the business's profits, we get that whenever the regulation reduces consumer surplus it also reduces total welfare.

Proposition 3 *Consider a regulation that imposes a minimum level of data protection $C_{\min}$. Then, there exists $\hat{C} > C^\star$ such that for all $C_{min} \in (C^\star, \hat{C})$ consumer surplus decreases as compared to when no regulation is imposed if and only if the business is moderately data-driven (i.e., $P \in [\frac{\rho}{1+\rho}, \frac{2\sqrt{\psi(1+\rho)}-\rho}{1+\rho}]$) .*[19]

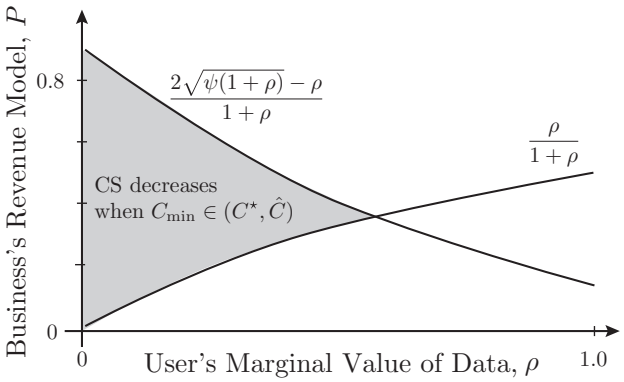

Figure 4: Introduction of minimal data protection regulation hurts consumer surplus in the shaded area when $C_{\min}$ is moderate. Here, $\psi = 0.1$.

As our discussion surrounding Theorem 2 suggests, if a business is mostly usage-driven, it is likely to be under-protecting and under-collecting user data. In this case, forcing the business to increase it's protection level means that the business will also collect more data and, in this case, this increases consumer surplus. On the other hand, if a business is heavily data-driven, it is likely to be already collecting all (or almost all) of the data generated by users' activity. In this case, forcing the business to provide additional protection will not come at the cost of an increase in data collection. In between these extremes, the business may already be over-collecting users' data and

[19] The interval $[\frac{\rho}{1+\rho}, \frac{2\sqrt{\psi(1+\rho)}-\rho}{1+\rho}]$ is non-empty if and only if the direct benefit for consumers from data collection is small and the cost of data protection is large (i.e., $\psi > \rho^2/(1+\rho)$)

any regulation that forces the business to provide more data protection will lead to an undesirable increase in data collection. Whether the latter overwhelms the benefits of the added protection depends on the cost of data protection and the direct benefits to users from data collection.

5.2. Optimal Regulation

In this section, we show that to achieve the socially optimal outcome regulatory authorities could supplement the minimal level of data protection requirement with either (i) liability fines proportional to the damage inflicted on users by adversarial activity or (ii) a tax on data collected. Our prescribed policies are *not* unique, and, as such, could be substituted with alternative policies, as long as such policies address both the data collection and the data protection aspects of the business's data strategy. We discuss some alternative policies below. Formally,

Definition 1 *Let $D_i(\xi, C) = a_i \xi \omega^*(\xi, C)$ be the damage to user i that is caused by adversarial activity; denote by $D(\xi, C) = \int_i D_i(\xi, C) \mathrm{d}i$ the average user's damage. A liability policy is a fine $\ell \times D$ on the business in the event that users suffer average damage of D.*

Definition 2 *A data collection tax policy imposes a tax rate t on the business for each unit of users' data collected. The expected amount of tax that the business pays is therefore $t \times \xi \bar{a}^*(\xi, C)$*

Remark 3 *In our model the amount of data collected, $\xi \bar{a}^*(\xi, C)$, enters directly into the users' utility function, adversaries' payoff function, and the business's profit function. That is, data "quantity" is measured by the usability of the information contained within the data rather than by physical measures related to the data itself (such as server storage units). Getting the measurement right may be important, because distortion in taxation may affect the business's incentives to collect one type of data versus another.*

The next proposition characterizes a simple two-pronged policy that restores efficiency regardless of the business's revenue model. Let $r(\xi, C) = -\frac{1}{\xi} \times \frac{\mathrm{d}(\xi \bar{a}^*(\xi, C))}{\mathrm{d}\xi} \Big/ \frac{\mathrm{d}(\bar{a}^*(\xi, C))}{\mathrm{d}\xi}$ be the ratio between the elasticity of the total amount of user's data collected, $\xi \bar{a}^*(\xi, C)$ with respect to the data collection strategy ξ and the elasticity of users' activity, $\bar{a}^*(\xi, C)$ with respect to ξ. At $\xi = \underline{\xi}(C)$ this ratio of elasticities is equal to $+\infty$, it then decreases in ξ and it equals zero at $\xi = \bar{\xi}(C)$.

Proposition 4 *The following two-pronged policy induces an equilibrium in which the business chooses the socially optimal data collection and data protection strategies:*

a) *a required minimum level of data protection* $C_{\min} = C^W$ *(where* C^W *is the socially-optimal data protection level)* ***combined with either***

b_1) *a liability fine proportional to the expected damage from adversarial activity with the rate*

$$\ell^\star = \frac{\alpha}{1-\alpha} \frac{C^W}{2r(\xi^W, C^W)(\xi^W)^2} \tag{8}$$

b_2) *or a data collection tax policy with a tax rate*

$$t^\star = \frac{\alpha}{1-\alpha} \frac{\bar{a}^*(\xi^W, C^W)}{r(\xi^W, C^W)\xi^W}, \tag{9}$$

Furthermore, if a business is purely usage-driven (i.e., if $P = 0$*), then imposing only a minimum level of data protection requirement is sufficient.*

Intuitively, imposing a liability fine or a tax on information collected guarantees that the socially-optimal data collection level ξ^W coincides with the business's optimal choice of data collection under socially-optimal data protection level C^W. At the same time, by reducing the level of data collection, a liability fine or data tax also eliminate any incentive the business may have to over-protect the data. A minimal protection level is then sufficient to guarantee that the business protects the collected data appropriately from a welfare standpoint.

To establish the liability rate that leads to efficient data collection, note that under an arbitrary liability policy ℓ and an arbitrary data collection strategy ξ, the average fine that the business expects to pay is

$$F(\xi, C, \ell) = \ell \times D(\xi, C) = \ell \times \omega^*(\xi, C) \times \xi\bar{a}^*(\xi, C) = \frac{\ell}{C}[\xi\bar{a}^*(\xi, C)]^2,$$

where the third equality follows by noticing that, from Proposition 1, $\omega^*(\xi) = \xi\bar{a}^*(\xi, C)/C$. Hence, the objective function of the business becomes

$$\Pi(\xi, C, \ell) = (1-P)\bar{a}^*(\xi, C) + P\xi\bar{a}^*(\xi, C) - F(\xi, C, \ell) - \psi C.$$

The fine $F(\xi, C, \ell)$ is an increasing function of total information collected, and therefore it reduces the benefit that the business obtains by capitalizing on the information. The magnitude of the

reduction increases with the level of ℓ. Because it is exactly the direct capitalization on user data that drives the over-collection of information by the business in the first place, the introduction of such policy, if rightly calibrated, eliminates the misalignment with the social objective.

In practice, despite the FTC's mandate to enforce a minimal level of data protection, the vast majority of the FTC's actions against firms come in response to documented data breaches. Once such breaches have been exposed and verified, the FTC imposes heavy fines on the businesses involved. Our analysis suggests that the FTC's practice of imposing fines on businesses based on the documented data breaches has the potential to be welfare enhancing if calibrated correctly. We do note, however, that imposing liability fines requires a litigation process to establish and quantify damages. An alternative policy that takes a more legislative and bureaucratic path is imposing a *tax on collected user information*. The tax rate that aligns the incentive of the business with the regulator's incentives, is derived in a similar way of the liability rate. Alternative policies, such as regulating directly the amount of data collected, subsidies for investment in data protection, etc., may also replace some of the suggested policies. The important practical lesson is that both aspects of the data strategy need to be regulated in a way that acknowledges their interdependence. Whether a tax, liability fines, or alternative policies are recommended depends on feasibility constraints, both technological and political. For example, whether it is easier to measure damages or data collection.

6. Broader Policy Implications

We conclude by discussing broad policy issues that our framework sheds light on.[20]

6.1. Awareness of users about the data policy

We have assumed that users know the data collection strategy of the digital business, which captures the common practice where users accept *terms and conditions* when opening an account in a digital business. However, in reality, some users may not read those terms. This could be because they have no privacy concerns or because they lack awareness and do not internalize the privacy costs. The model can easily accommodate heterogeneity across users in their sophistication or awareness

[20] In addition to the discussion below, Online Appendix C.9 discusses how the endogenous reactions of users affect the welfare costs of adversarial activities, and Online Appendix C.10 discusses how our model can address the implications of harmful ads.

levels and the qualitative results do not change. In fact, in our model, the reaction of users to the data policy disciplines, to some extent, the incentive of the platform to collect too much information and to protect it too little. Less sophisticated users will not react to the business's data policy, which implies that the presence of such users makes the business's incentives even less aligned with users' preferences.

More recently, regulations in the EU, California, and to some extent China, focused on increasing users' awareness (and control) of the data collected by digital businesses. For example, many users can now request their information from digital businesses under the European GDPR law (see Art. 15 GDPR - Right of access by the data subject). The GDPR, therefore, allows users to have accurate knowledge of what data is collected about them

Studying the consequences of the rollout of the EU's General Data Protection Regulation (GDPR), Goldberg et al. 2021 show that it increased the businesses' costs of collecting consumer data. On the other hand, Aridor et al. 2020 show that despite the increase in opt-outs that followed the GDPR, the ability of firms to target consumers did not decrease, suggesting that the effective amount of information did not decrease.[21] These results by Aridor et al. 2020 suggest that effective regulation of data collection may require enforcement at a collective level, addressing directly the usable information contained in the data collected. This is in line with our analysis in Section 5.

6.2. Vertical Integration

The last two decades have seen significant consolidation of digital businesses, with many mergers and acquisitions led by the Big Five Tech Giants or GAFAM (Google, Amazon, Facebook, Apple, and Microsoft).[22] Many of those acquisitions were vertical. That is, the acquired business operated in a separate market and/or provided a distinct service from the acquiring business. However, in privacy terms, even seemingly unrelated mergers may have an important effect. This is so because data may be shared between different subsidiaries of the same parent company.[23] And, in fact, much in-line with public discourse, database mergers often involve businesses that collect different

[21] Presumably large digital platforms are at a point in which they can use rich data from past consumers to predict many characteristics of new customers only on the basis of some basic information, e.g., Acemoglu et al. 2019 and Bergemann et al. 2020).

[22] See also https://www.visualcapitalist.com/the-big-five-largest-acquisitions-by-tech-company/

[23] For one of many examples, see https://www.eff.org/deeplinks/2020/04/google-fitbit-merger-would-cement-googles-data-empire about the Google-Fitbit merger. For a recent paper that analyzes how combining datasets could feed back into user behavior see Liang and Madsen 2020.

types of information.[24]

In online appendix C.7 we provide a simple example that demonstrates how our model can incorporate such considerations. We shows that if following the mergers the businesses make joint decisions regarding data collection, consumers will be worse off. This negative effect is not present if the businesses merge their databases but keep the data collection decisions (and revenue from data collections) separate.

6.3. Pay For Data

Whether users should be paid for their data is an interesting question that pertains to the property rights over individual-level data and transcends the analysis in this paper.[25] However, our framework could be useful in evaluating the effect that pay-for-data schemes may have on data collection and data protection, and subsequently on consumer surplus and total welfare.

In Online Appendix C.8, we illustrate that when a regulator requires businesses to pay users for their data, users' direct incentives to exert activity increase (since they are now paid for their data) while business's marginal returns from each unit of user information decrease. The interplay between the two defines whether the business collects a higher fraction of information or not and whether users benefit from such "pay for data" policy. We show that there exist regimes in which the incentives of users to increase activity are so strong that the business can gain from an imposed payment by increasing data collection, ξ, despite of the lowered returns from user information. When the price per data is sufficiently large, we find that consumer surplus can be higher than without the "pay for data" policy, and it can actually reach the socially optimal level.

7. Related Literature and Conclusion

This paper contributes to an active interdisciplinary area of research that studies the consequences for market outcomes of the ability of digital institutions to amass large data sets. The main issues

[24] See, e.g., https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking

[25] In related work, Arrieta-Ibarra et al. 2018 make the case that users should be paid for their data as if that data were labor, whereas Ichihashi 2020a explores a scenario in which competing data brokers compensate users for their data, and Bergemann and Bonatti 2019 and Acemoglu et al. 2019 study a setting where a data intermediary extracts users' information by offering monetary transfers. Emerging work in the marketing literature seeks to evaluate users' valuation of privacy via empirical and experimental approaches (see Lin 2019 and references therein).

discussed in the literature are the collection and management of consumer information, consumer privacy, and possible policy intervention.

Recent work has focused on understanding how user information is either voluntarily disclosed (Ali et al. 2020) or inferred from users' actions such as purchasing behavior over time (Conitzer et al. 2012, Fudenberg and Villas-Boas 2006), ratings (Bonatti and Cisternas 2017), formation of social links (Acemoglu et al. 2017), platform usage (Ichihashi 2020a), or gathered through monetary transfers (Bergemann et al. 2020). We rely on this line of work and assume that there is a one-to-one mapping between any user's actions (usage of the platform) and the information that is revealed about this user to the platform.[26]

Other work has explored how the mechanisms for extracting user information and possession of information itself affect the design of targeted/personalized pricing (e.g., Candogan et al. 2012, Bloch and Quérou 2013, Fainmesser and Galeotti 2016, 2020, Elliott et al. 2021, Montes et al. 2018, Ichihashi 2020b, Valletti and Wu 2020), selective selling (Momot et al. 2020), service systems (Hu et al. 2020); what is the impact on social image visibility (Ali and Bénabou 2020), advertising strategies (Galeotti and Goyal 2009, Shen and Miguel Villas-Boas 2017, Bimpikis et al. 2016), the extent of competition (Casadesus-Masanell and Hervas-Drane 2015) and mergers of digital businesses (Prat and Valletti 2019), overall consumer behavior (Goldfarb and Tucker 2011, Koh et al. 2015, Jann and Schottmüller 2020, Gradwohl 2017).[27] Jullien et al. 2020 considers a digital business that sells data services to third-parties who may be good or bad for users. The focus of this work is on data monetization and on the market for data services and is therefore very different from ours. Yet we share the intuition that the business faces a trade-off between data exploitation and user recruitment/retention/activity.[28]

More recent work investigates the impact of privacy regulation on the operations of platforms and their users' behavior. Argenziano and Bonatti 2021 and Bimpikis et al. 2021 study the effectiveness

[26] The computer science literature has addressed the design of algorithmic mechanisms for anonymizing and protecting individual-level data (for reviews of this research stream, see e.g. Dwork and Roth 2014, Cummings et al. 2015, Ghosh and Roth 2015, Abowd and Schmutte 2019). The operations management literature has employed algorithmic mechanisms to design privacy-preserving personalized data-driven revenue management algorithms (see, Lei et al. 2021).

[27] Excellent surveys are provided by Acquisti et al. 2016, Mayzlin 2016, and Bergemann and Bonatti 2019. See also https://www.heinz.cmu.edu/~acquisti/economics-privacy.htm#Papers for a structured list of papers in this area by Alessandro Acquisti.

[28] The business's tradeoff is driven by users' tradeoff between providing data (via usage) and potential privacy infringements. Cong et al. 2020 show the implications of this tradeoff for the growth of the data economy.

of privacy regulation (such as requiring customers' consent or prohibiting data tracking) in scenarios in which customers interact with firms sequentially and the customers' data can be shared among these firms (so-called, data linkages). Markovich and Yehezkel 2021 investigate whether users or the platform should have control over users' data.

Notably, information generated by different users might be interdependent, so that information generated by one user can reveal information on another. Such considerations could be introduced into our model by: (1) replacing $a_i\xi$ in user's i utility with a function of other users' usage levels, and (2) replacing everywhere $\bar{a}$ with a different function aggregating the usage levels of all users. We defer this analysis for future work and refer the interested reader to work on the topic by Acemoglu et al. 2019, Bergemann and Bonatti 2019, Gradwohl 2017, and Ichihashi 2020c.

Our contribution is to formulate a model that captures the different components of a business's data strategy and in which privacy costs are endogenous and therefore change with the data strategy of the business. This allows us to assess positive and normative implications of data policy design and to compare conclusions across different domains—in particular, between data-driven and usage-driven revenue models. We demonstrate how our framework is useful to study broader policy issues such as the motivations and welfare effect of vertical integration in digital markets and the potential welfare benefits of introducing a carefully calibrated payment to users for their data.

References

J. M. Abowd and I. M. Schmutte. An economic analysis of privacy protection and statistical accuracy as social choices. *American Economic Review*, 109(1):171–202, 2019.

D. Acemoglu, A. Makhdoumi, A. Malekian, and A. Ozdaglar. Privacy-constrained network formation. *Games and Economic Behavior*, 105:255–275, 2017.

D. Acemoglu, A. Makhdoumi, A. Malekian, and A. Ozdaglar. Too much data: Prices and inefficiencies in data markets. Technical report, National Bureau of Economic Research, 2019.

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

S. N. Ali and R. Bénabou. Image versus information: Changing societal norms and optimal privacy. *American Economic Journal: Microeconomics*, 12(3):116–64, 2020.

S. N. Ali, G. Lewis, and S. Vasserman. Voluntary disclosure and personalized pricing. In *Proceedings of the 21st ACM Conference on Economics and Computation*, pages 537–538, 2020.

R. Argenziano and A. Bonatti. Data linkages and privacy regulation. Working Paper, 2021.

G. Aridor, Y.-K. Che, and T. Salz. The economic consequences of data privacy regulation: Empirical evidence from GDPR. SSRN 3522845, 2020.

I. Arrieta-Ibarra, L. Goff, D. Jiménez-Hernández, J. Lanier, and E. G. Weyl. Should we treat data as labor? moving beyond "free". In *aea Papers and Proceedings*, volume 108, pages 38–42, 2018.

D. Bergemann and A. Bonatti. Markets for information: An introduction. *Annual Review of Economics*, 11:85–107, 2019.

D. Bergemann, A. Bonatti, and T. Gan. The economics of social data. SSRN 3459796, 2020.

K. Bimpikis, A. Ozdaglar, and E. Yildiz. Competitive targeted advertising over networks. *Operations Research*, 64(3):705–720, 2016.

K. Bimpikis, I. Morgenstern, and D. Saban. Data tracking under competition. SSRN 3808228, 2021.

F. Bloch and N. Quérou. Pricing in social networks. *Games and Economic Behavior*, 80:243–261, 2013.

A. Bonatti and G. Cisternas. Ratings-based price discrimination. *Working Paper*, 2017.

O. Candogan and K. Drakopoulos. Optimal signaling of content accuracy: Engagement vs. misinformation. *Operations Research*, 68(2):497–515, 2020.

O. Candogan, K. Bimpikis, and A. Ozdaglar. Optimal pricing in networks with externalities. *Operations Research*, 60(4):883–905, 2012.

R. Casadesus-Masanell and A. Hervas-Drane. Competing with privacy. *Management Science*, 61(1): 229–246, 2015.

L. W. Cong, D. Xie, and L. Zhang. Knowledge accumulation, privacy, and growth in a data economy. *Management Science*, forthcoming, 2020. doi: 10.1287/mnsc.2021.3986. URL https://doi.org/10.1287/mnsc.2021.3986.

V. Conitzer, C. R. Taylor, and L. Wagman. Hide and seek: Costly consumer privacy in a market with repeat purchases. *Marketing Science*, 31(2):277–292, 2012.

R. Cummings, K. Ligett, M. M. Pai, and A. Roth. The strange case of privacy in equilibrium models. *arXiv:1508.03080*, 2015.

A. De Cornière and G. Taylor. Information security and competition. Working Paper, 2020.

C. Dwork and A. Roth. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2014.

M. Elliott, A. Galeotti, and L. Koh. Market segmentation through information. *CWPE2105*, 2021.

I. P. Fainmesser and A. Galeotti. Pricing network effects. *The Review of Economic Studies*, 83(1): 165–198, 2016.

I. P. Fainmesser and A. Galeotti. Pricing network effects: Competition. *American Economic Journal: Microeconomics*, 12(3):1–32, 2020.

D. Fudenberg and J. M. Villas-Boas. Behavior-based price discrimination and customer recognition. *Handbook on economics and information systems*, 1:377–436, 2006.

A. Galeotti and S. Goyal. Influencing the influencers: a theory of strategic diffusion. *The RAND Journal of Economics*, 40(3):509–532, 2009.

A. Ghosh and A. Roth. Selling privacy at auction. *Games and Economic Behavior*, 91:334–346, 2015.

E. L. Glaeser and J. Scheinkman. Non-market interactions. Technical report, National Bureau of Economic Research, 2000.

S. G. Goldberg, G. A. Johnson, and S. K. Shriver. Regulating privacy online: An economic evaluation of the GDPR, 2021.

A. Goldfarb and C. E. Tucker. Privacy regulation and online advertising. *Management Science*, 57 (1):57–71, 2011.

R. Gradwohl. Information sharing and privacy in networks. In *Proceedings of the 2017 ACM Conference on Economics and Computation*, pages 349–350. ACM, 2017.

M. Hu, R. Momot, and W. Jianfu. Privacy management in service systems. SSRN 3628751, 2020.

S. Ichihashi. Dynamic privacy choices. In *Proceedings of the 21st ACM Conference on Economics and Computation*, pages 539–540, 2020a.

S. Ichihashi. Online privacy and information disclosure by consumers. *American Economic Review*, 110(2):569–95, 2020b.

S. Ichihashi. The economics of data externalities. 2020c. URL https://shota2.github.io/research/externality.pdf.

O. Jann and C. Schottmüller. An informational theory of privacy. *The Economic Journal*, 130(625): 93–124, 2020.

B. Jullien, Y. Lefouili, and M. H. Riordan. Privacy protection, security, and consumer retention. SSRN 3655040, 2020.

B. Koh, S. Raghunathan, and B. R. Nault. Is voluntary profiling welfare enhancing? *Management Information Systems Quarterly*, forthcoming, 2015.

M. A. Lariviere. A note on probability distributions with increasing generalized failure rates. *Operations Research*, 54(3):602–604, 2006.

Y. Lei, S. Miao, and R. Momot. Privacy-preserving personalized revenue management. SSRN 3704446, 2021.

A. Liang and E. Madsen. Data and incentives. In *Proceedings of the 21st ACM Conference on Economics and Computation*, pages 41–42, 2020.

T. Lin. Valuing intrinsic and instrumental preferences for privacy. *SSRN 3406412*, 2019.

J. Z. Liu, M. Sockin, and W. Xiong. Data privacy and temptation. 2020. URL http://wxiong.mycpanel.princeton.edu/papers/Privacy.pdf.

S. Markovich and Y. Yehezkel. Data regulation: who should control our data? SSRN 3801314, 2021.

D. Mayzlin. Managing social interactions. In *The Oxford Handbook of the Economics of Networks*. 2016.

R. Momot, E. Belavina, and K. Girotra. The use and value of social information in selective selling of exclusive products. *Management Science*, 66(6):2610–2627, 2020.

R. Montes, W. Sand-Zantman, and T. Valletti. The value of personal information in online markets with endogenous privacy. *Management Science*, 65(3):1342–1362, 2018.

Y. Papanastasiou. Fake news propagation and detection: A sequential model. *Management Science*, 66(5):1826–1846, 2020.

A. Prat and T. M. Valletti. Attention oligopoly. SSRN 3197930, 2019.

Q. Shen and J. Miguel Villas-Boas. Behavior-based advertising. *Management Science*, 64(5): 2047–2064, 2017.

T. Valletti and J. Wu. Consumer profiling with data requirements: Structure and policy implications. *Production and Operations Management*, 29(2):309–329, 2020.

A. Appendix: Proofs of the Main Results

A.1. Proof of Proposition 1 (Page 10)

Given users' expectation of the adversaries' demand for information ω, there exists a unique response of the users. Existense (sufficient condition) follows from Glaeser and Scheinkman 2000: $\exists_{\widetilde{a}\geq 0}\forall_{\bar{a}\leq\widetilde{a}}\frac{\partial U_i(a_i,\bar{a})}{\partial a_i}\Big|_{a_i=\widetilde{a}}<0$ or $\exists_{\widetilde{a}\geq 0}\forall_{\bar{a}\leq\widetilde{a}}\ 1+\beta\bar{a}+\xi[\rho-\omega]-\widetilde{a}<0$. Because $\rho,\xi\in[0,1]$ and $\omega\geq 0$ this is satisfied whenever $\exists_{\widetilde{a}\geq 0}\ 2<\widetilde{a}\,(1-\beta)$, which can only be satisfied if $\beta<1$. Condition for the uniqueness of the users' response also follows from Glaeser and Scheinkman 2000: $\forall_i\left|\frac{\partial^2 U_i}{\partial a_i\partial\bar{a}}/\frac{\partial^2 U_i}{\partial a_i^2}\right|<1$ which is satisfied if $\beta<1$.

Next, we derive our characterization of the unique response. Denote $\mathbf{a}_{-i}$ the activity choice that i conjecture about the other users. Then user i's best reply is $a_i=1+\beta\bar{a}-\omega\xi+\rho\xi$ where $\bar{a}=\int_j a_j\mathrm{d}j$. In equilibrium users' expectation are correct and so $\int_i a_i\mathrm{d}i=1+\beta\bar{a}-\omega\xi+\rho\xi=\bar{a}$ or $\bar{a}(\omega)=\frac{1+\rho\xi-\omega\xi}{1-\beta}$ (this expression is positive in equilibrium). Such response induces adversaries with $\bar{a}(\omega)\xi\geq\gamma C$ to be active. Therefore, the induced adversaries' demand for information is $\bar{a}(\omega)\xi/C$ which should be consistent with the initial belief ω, hence ω should solve $\omega=\frac{\bar{a}(\omega)\xi}{C}$. The expressions for $\bar{a}^*(\xi,C)$ and $\omega^*(\xi,C)$ then follow by substitution. Consumer surplus is derived as follows: $\mathrm{CS}(\xi)=\int U_i(a_i^*(\xi,C),\bar{a}^*(\xi,C))\mathrm{d}i$ where $a_i^*(\xi,C)=1+\beta\bar{a}^*(\xi)-\omega^*(\xi)\xi+\rho\xi$.

Comparative Statics of $\bar{a}^*(\xi,C)$ and $\xi\bar{a}^*(\xi,C)$.– Behavior of $\bar{a}^*(\xi,C)$ and $\xi\bar{a}^*(\xi,C)$ wrt C is trivial and follows from showing that derivative of $\bar{a}^*(\xi,C)$ wrt C is always positive. Derivative of $\bar{a}^*(\xi,C)$ wrt ξ is $\frac{C(\rho C(1-\beta)-2\xi-\rho\xi^2)}{(C(1-\beta)+\xi^2)^2}$ the sign of which is defined by the sign of $\rho C(1-\beta)-2\xi-\rho\xi^2$. For any $C>0$, this expression is first positive, then negative. The change of sign happens at $\xi_1(C)$ (largest solution of $\rho C(1-\beta)-2\xi-\rho\xi^2=0$). Similarly, derivative of $\xi\bar{a}^*(\xi,C)$ can be derived as $\frac{C(C(1-\beta)-\xi^2+2C(1-\beta)\rho\xi)}{(C(1-\beta)+\xi^2)^2}$ which has sign of $-\xi^2+2\rho\xi C(1-\beta)+C(1-\beta)$. For any $C>0$, the latter expression is first positive, then negative. The change of sign happens at $\xi_2(C)$ (largest solution to $-\xi^2+2\rho\xi C(1-\beta)+C(1-\beta)=0$). Finally, $\xi_2(C)>\xi_1(C)$ holds trivially when $1<\rho^2C(1-\beta)$, otherwise, rewrite it as $\rho C(1-\beta)+\frac{1}{\rho}>\sqrt{\frac{1}{\rho^2}+C(1-\beta)}-\sqrt{(\rho C(1-\beta))^2+C(1-\beta)}$, RHS is non-negative when $1\geq\rho^2C(1-\beta)$, taking square of the both sides and rearranging, we can show that this inequality holds. Finally, it always holds that $\xi_1(C)\geq 0$ and $\xi_2(C)\geq 0$. We define $\underline{\xi}(C)=\min\{1,\xi_1(C)\}$ and $\bar{\xi}(C)=\min\{1,\xi_2(C)\}$.

A.2. Proof of Theorem 1 (Page 11)

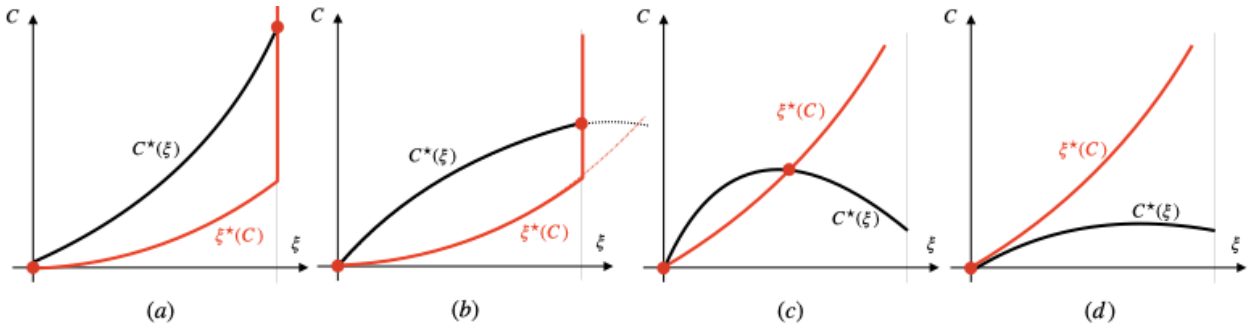

Figure 5: Functions $C^\star(\xi)$ and $\xi^\star(C)$ depending on ψ: (a) $\psi < P\rho$; (b) $\psi \in [P\rho, \psi_L]$; (c) $\psi \in [\psi_L, \psi_H]$; (d) $\psi > \psi_H$. Points ψ_L, ψ_H are defined in the proof of Theorem 1; functions $\xi^\star(C)$ and $C^\star(\xi)$ are defined in Lemmas 1 and 2.

Lemma 1 (Lemma 2) characterizes the business's data collection (data protection) strategy when data protection (data collection) is held fixed, and is used in the proof of Theorem 1. The proofs of these lemmas are technical and deferred to Appendix B.

Lemma 1 (Optimal Data Protection $C^\star(\xi)$ as a Function of Data Collection) *Given a data collection level ξ, the business sets data protection $C^\star(\xi) = \max\{C_h(\xi), 0\}$, where* $C_h(\xi) = \frac{1}{1-\beta}\left(-\xi^2 + \xi\sqrt{\frac{1}{\psi}(1+\rho\xi)(1-P+P\xi)}\right)$.[29]

Lemma 2 (Optimal Data Collection $\xi^\star(C)$ as a Function of Data Protection) *Given a data protection level C, the business stores:*

- *part of the information $\xi^\star(C) = -\kappa(C) + \sqrt{\kappa(C)^2 + C(1-\beta)} < 1$ (increasing in C) if data protection policy level is low $C < C_l$;*
- *all the information ($\xi^\star(C) = 1$) if data protection policy level is high $C > C_l$.*

Here $\kappa(C) = \frac{1-P-P\rho C(1-\beta)}{P+(1-P)\rho}$ *and* $C_l = \frac{1}{1-\beta}\frac{2+\rho-P(1+\rho)}{P+\rho+P\rho}$.

We know that $-\kappa(C) + \sqrt{\kappa(C)^2 + C(1-\beta)}$ is increasing and concave in C. Denote $C_{inv}(\xi)$ solution to $-\kappa(C) + \sqrt{\kappa(C)^2 + C(1-\beta)} = \xi$ wrt C (here $\kappa(C)$ is defined in Lemma 2). We have that:

$$C_{inv}(\xi) = \frac{1}{1-\beta}\frac{\xi[(P+(1-P)\rho)\xi + 2(1-P)]}{P+(1-P)\rho+2\xi P\rho}.$$

Case $\psi < P\rho$: We first show that $C_{inv}(\xi) < C_h(\xi)$ (where $C_h(\xi)$ is defined in Lemma 1) and they

[29] $C_h(\xi) > 0$ if either (i) $\psi < P\rho$ or (ii) $\psi > P\rho$ and $\xi < \min\{1, \frac{P+\rho(1-P)+\sqrt{(P-(1-P)\rho)^2+4(1-P)\psi}}{2(\psi-P\rho)}\}$.

only intersect at $\xi = 0$ under this condition. That is, we need to show:

$$\xi + \frac{(P + (1-P)\rho)\xi + 2(1-P)}{P + (1-P)\rho + 2\xi P\rho} < \sqrt{\frac{1}{\psi}(1+\rho\xi)(1-P+P\xi)}$$

The LHS can be rewritten as $\frac{2(1+\rho\xi)(1-P+P\xi)}{P+\rho-P\rho+2\xi P\rho}$. Developing, we need to show that $4\psi(1+\rho\xi)(1-P+P\xi) < (P+(1-P)\rho+2\xi P\rho)^2$. The LHS of the latter inequality is the highest under $\psi = P\rho$ and the RHS is the lowest under $\psi = P\rho$ (since we consider case $\psi < P\rho$). It is easy to check that inequality holds in this case and hence $C_{inv}(\xi) < C_h(\xi), \forall \xi > 0$. Thus, the only two points of intersection of best-responses $C^\star(\xi)$ and $\xi^\star(C)$ are $\xi = 0, C = 0$ and $\xi = 1, C = C_h(1)$. We evaluate company's profit at both points. The first point gives $\pi_0 = \frac{1-P}{1-\beta}$, while the second gives $\pi_1(\psi) = \frac{1}{1-\beta}(1+\rho+\psi-2\sqrt{\psi(1+\rho)})$ - decreasing in ψ on the interval $\psi < P\rho$ (the derivative wrt ψ is $1-\sqrt{(1+\rho)/\psi}$). Since $\pi_1(0) > \pi_0$, the business is choosing $\xi^\star = 1, C^\star = C_h(1)$ for the case that $\psi < P\rho$ (it is also easy to verify that $\pi_1(P\rho) > \pi_0$). Figure 5 (a) illustrates this case.

Case $\psi > P\rho$: Solve $C_{inv}(\xi) = C_h(\xi)$. We get two non-negative roots: $\xi = 0$ and $\xi_i = \frac{1}{2P\rho}(-(1-P)\rho - P + |P-(1-P)\rho|\sqrt{\frac{\psi}{\psi - P\rho}})$. We will establish first conditions when $\xi_i \in [0,1]$. We will consider case of $P > (1-P)\rho$ (case $P < (1-P)\rho$ can be considered similarly and leads to the same result). $\xi_i > 0$ when $\psi \in [P\rho, \psi_H]$, where $\psi_H = \frac{(P+(1-P)\rho)^2}{4(1-P)}$ is a solution to $\xi_i = 0$ wrt ψ. Similarly, $\xi_i < 1$ when $\psi > \psi_L$, where $\psi_L = \frac{(P+\rho+P\rho)^2}{4(1+\rho)}$ is a solution to $\xi_i = 1$ wrt ψ. Both $\psi_L > P\rho$ and $\psi_H > P\rho$, also $\psi_H > \psi_L$ (ξ_i decreases with ψ).

On the interval $\psi \in [P\rho, \psi_L)$, $\xi_i > 1$, hence on $\xi \in [0,1]$ we have $C_{inv}(\xi) < C_h(\xi)$. Thus, the two points of intersection of the best-response functions are $\xi = 0, C = 0$ and $\xi = 1, C = C_h(1)$. $\pi_1(\psi)$ decreases with ψ on $[P\rho, \psi_L)$ (derivative $\pi_1'(\psi)$ changes sign only once and at ψ_L it is negative). Plugging ψ_L into $\pi_1(\psi)$ defined above, we get $\pi_1(\psi_L) > \pi_0$. We thus conclude that $\pi_1(\psi) > \pi_0$ on $[P\rho, \psi_L)$ and thus $\xi^\star = 1, C^\star = C_h(1)$. Figure 5 (b) illustrates this case.

On the interval $\psi > \psi_H$, $C_{inv}(\xi) > C_h(\xi)$, $\forall \xi \in [0,1]$. Hence, the only point of intersection of the best-responses is $\xi^\star = 0, C^\star = 0$. Figure 5 (d) illustrates this case.

Finally, on the interval $\psi \in [\psi_L, \psi_H]$, there are two points of intersection of the best-responses:

$\xi = 0, C = 0$ (delivering profit π_0) and $\xi = \xi_i \in [0,1], C = C_h(\xi_i)$ with profit:

$$\pi_{\xi_i}(\psi) = \frac{\psi}{4P^2\rho^2}\left[P + (1-P)\rho + P\rho(P-(1-P)\rho)\frac{z(\psi)}{\psi} - Pz(\psi) + (1-P)\rho z(\psi)\right]^2$$

Where $z(\psi) = \sqrt{\frac{\psi}{\psi - P\rho}}$ - decreasing function of ψ. Taking derivative $\pi'_{\xi_i}(\psi)$ we obtain:

$$\pi'_{\xi_i}(\psi) = \frac{1}{4\psi P^2\rho^2}\frac{P\rho z(\psi)}{z(\psi)^2 - 1}\left[(1-P)^2\rho^2(z(\psi)+1)^2 - P^2(z(\psi)-1)^2\right]$$

Where we substituted $\psi = \frac{z(\psi)^2 P\rho}{z(\psi)^2 - 1}$ and also $z(\psi) > 1$ on $\psi > P\rho$. Notice that $\xi_i = \frac{1}{2P\rho}[P(z(\psi) - 1) - (1-P)\rho(z(\psi)+1)]$ and $\xi_i > 0$ on $\psi < \psi_H$. Developing $\pi'_{\xi_i}(\psi)$ we obtain:

$$\pi'_{\xi_i}(\psi) = \frac{1}{4\psi P^2\rho^2}\frac{P\rho z(\psi)}{z(\psi)^2 - 1}\left[(1-P)\rho(z(\psi)+1) - P(z(\psi)-1)\right]\cdot\left[(1-P)\rho(z(\psi)+1) + P(z(\psi)-1)\right] < 0$$

Here, inequality follows from noticing that the expression in the second brackets is $-\xi_i < 0$. To check that $\pi_{\xi_i}(\psi) > \pi_0$ on $\psi \in [\psi_L, \psi_H]$ we thus need to check this inequality at ψ_H. It is easy to verify that $\pi_{\xi_i}(\psi_H) = \frac{1-P}{1-\beta} = \pi_0$. Thus, on $\psi \in [\psi_L, \psi_H]$ digital business optimally chooses $\xi^\star = \xi_i \in [0,1]$ and $C^\star = C_h(\xi_i)$. Figure 5 (c) illustrates this case. Finally, second-order conditions can be verified in the linear model as a particular case of a more general proof of Lemma 3 in Appendix C.5.

Summarizing the above, we have two thresholds $P\rho < \psi_L \leq \psi_H$ such that: (i) if $\psi \leq \psi_L$, then $\xi^\star = 1$ and $C^\star = C_h(1)$; (ii) if $\psi \in (\psi_L, \psi_H)$, then $\xi^\star = \xi_i = \frac{1}{2P\rho}(-(1-P)\rho - P + |P - (1-P)\rho|\sqrt{\frac{\psi}{\psi - P\rho}}) \in (0,1)$ and $C^\star = C_h(\xi_i)$; (iii) if $\psi \geq \psi_H$, then $\xi^\star = 0$ and $C^\star = 0$. Here function $C_h(\xi)$ is defined in Lemma 1. The three cases can then be written succinctly as in the statement of the Theorem. In particular, the expression for $\xi^\star$ is just ξ_i bounded within $[0,1]$ interval and with an additional $\max\{0, \psi - P\rho\}$ which does not change ξ_i when $\psi > P\rho$, but turns ξ_i into ∞ (and, thus guarantees that $\xi^\star = 1$ is chosen) when $\psi < P\rho < \psi_L$. Expression for $C^\star$ is just the one for $C_h(\xi)$ evaluated at $\xi^\star$.

Finally, in order to show that both $\xi^\star$ and $C^\star$ weakly increase with P, it is necessary to consider the behavior of ψ_L, ψ_H as functions of P and then analyze the behavior of $\xi^\star, C^\star$ in the three regions defined by these functions. We delegate this proof to the last part of the following Appendix A.3.

A.3. Proof of Proposition 2 (Page 12)

From Theorem 1, we know that the business sets: (a) $\xi^\star = 1, C^\star = \frac{1}{1-\beta}(-1+\sqrt{\frac{1+\rho}{\psi}})$ if $\psi \leq \psi_L$; (b) $\xi^\star \in (0,1), C^\star > 0$ if $\psi \in (\psi_L, \psi_H)$; and (c) $\xi^\star = 0, C^\star = 0$ if $\psi \geq \psi_H$. Substituting optimal $\xi^\star, C^\star$ into the expression for $\bar{a}^*(\xi, C)$, we obtain: (a) $\bar{a}^a = \frac{1}{1-\beta}(1+\rho-\sqrt{\psi(1+\rho)})$ when $\psi \leq \psi_L$; (b) $\bar{a}^b(P) = a^*(\xi^\star, C^\star)$ when $\psi \in (\psi_L, \psi_H)$; and (c) $\bar{a}^c = \lim_{\xi^\star=0, C^\star=0} \bar{a}^*(\xi^\star, C^\star) = \frac{1}{1-\beta}$ when $\psi > \psi_H$. First, notice that $\bar{a}^a$ and $\bar{a}^c$ do not depend on P and $\bar{a}^a > \bar{a}^c$ when $\psi < \frac{\rho^2}{1+\rho}$.

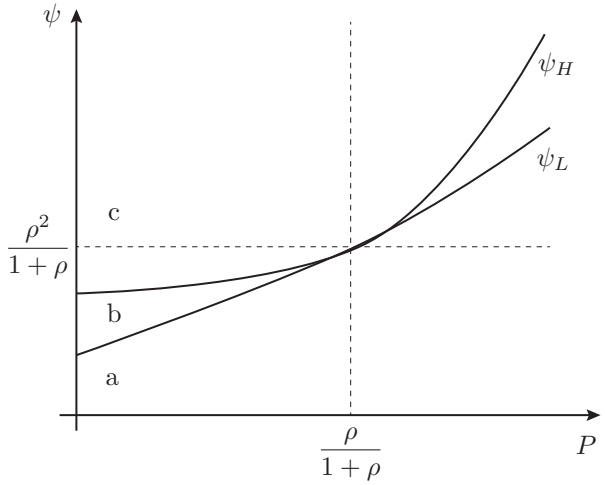

Figure 6: Behavior of functions ψ_L and ψ_H with P. There are three regions: (a) $\psi < \psi_L$; (b) $\psi \in (\psi_L, \psi_H)$; and (c) $\psi > \psi_H$.

It is easy to verify that both ψ_L, ψ_H are increasing, convex functions of P. Furthermore, $\psi_H \geq \psi_L$ and they intersect only at one point $P = \frac{\rho}{1+\rho}$ for $P \in [0,1]$ where $\psi_L = \psi_H = \frac{\rho^2}{1+\rho}$. At $P = 0$ we have $\psi_L(P=0) = \frac{\rho^2}{4(1+\rho)}$ and $\psi_H(P=0) = \frac{\rho^2}{4}$. Figure 6 illustrates behavior of the functions ψ_L, ψ_H with P.

Region (b) consists of two sub-regions: $P < \frac{\rho}{1+\rho}$ and $P > \frac{\rho}{1+\rho}$. Clearly, region (b) is such that $\psi > P\rho$ (since $P\rho < \psi_L$). Consider $P < \frac{\rho}{1+\rho}$ (the other sub-region can be analyzed similarly). Here $P - (1-P)\rho < 0$. Denoting $z = \sqrt{\frac{\psi}{\psi - P\rho}}$ (and, thus, $\psi = \frac{z^2 P\rho}{z^2-1}$), one can write down $\frac{d\bar{a}^b(P)}{dP}$ as:

$$\frac{d\bar{a}^b(P)}{dP} = \frac{z(z-1)(\rho - \rho z + P(1+z+\rho(-1-(P-(1-P)\rho)\frac{z^2-1}{zP\rho}+z))}{2P(1-\beta)(z^2-1)}$$

After algebraic simplification we obtain: $\frac{P(1+z)+(1-P)(z-1)\rho}{2P(1+z)(1-\beta)}$. Given that $z \geq 1$, we conclude that this expression is non-negative. Hence, consumer surplus weakly increases in the sub-region (b) $P < \frac{\rho}{1+\rho}$.

Furthermore, one can verify that $\bar{a}^c = \bar{a}^b(P_H)$ where P_H solves $\psi = \psi_H$ and that $\bar{a}^a = \bar{a}^b(P_L)$ where P_L solves $\psi = \psi_L$. Taken together with the behavior of consumer surplus in regions (a) and (c), we conclude that consumer surplus weakly increases with P when $P < \frac{\rho}{1+\rho}$. The other case can be derived similarly.

Finally, we can verify that $\xi^\star, C^\star$ weakly increase with P using the techniques from above. First, clearly both protection and collection are higher in region (a) than in region (c). Both do not change with P in these regions. We are left to show that in region (b) both protection and collection also increase with P (there are no jumps on the borders of regions (c)-(b) and (b)-(a) as per Theorem 1). Consider first behavior of $\xi^\star$ in the sub-region (b) $P < \frac{\rho}{1+\rho}$ (the other sub-region can be considered in similar fashion). Signs of the derivative is defined by the following function:

$$\frac{d\xi^\star(P)}{dP} \sim \frac{P^2 z\rho(\rho(z^2+z-2) - Pz(1+z)(1+\rho))}{(z-1)(1+z)^2}$$

The sign of the numerator of this expression is defined by $z^2(\rho - P(1+\rho)) + z(\rho - P(1+\rho)) - 2\rho$ – an increasing function for any $z > 0$. Given that $\psi \in [\psi_L, \psi_H]$ in this region, we have $z \in [\frac{P+\rho-P\rho}{-P+(1-P)\rho}, \frac{P+\rho(1+P)}{-P+\rho(1-P)}]$. Evaluating this expression at the left border we obtain $\frac{2P\rho(-2+P+\rho-P\rho)}{P-\rho+P\rho} > 0$ (recall that $P \in [0,1], \rho \in [0,1]$ and that $P < \frac{\rho}{1+\rho}$ in the sub-region under consideration). Hence, we conclude that on $\psi \in [\psi_L, \psi_H]$ and when $P < \frac{\rho}{1+\rho}$, $\xi^\star$ increases with P. The sign of $\frac{dC^\star(P)}{dP}$ can be shown to be positive in sub-region $P < \frac{\rho}{1+\rho}$ and the behavior of the data protection and data collection in sub-region $P > \frac{\rho}{1+\rho}$ can be derived using techniques similar to those used above.

Finally, for a fixed ψ regions (a), (b), (c) can be characterized by thresholds P_L and P_H. One can derive these thresholds by simply solving $\psi = \psi_L$ and $\psi = \psi_H$ wrt P.

Figure 7 summarizes how consumer surplus changes as a function of P, ρ, and ψ.

A.4. Proof of Theorem 2 (Page 13)

We will first prove that relative to the socially optimal strategy, the business's data strategy never prescribes a combination of higher level of data protection and lower level of data collection. That all other combinations are possible is shown numerically with the linear example on page 16 (see Figure 4).

Taking into account the users and adversaries' equilibrium strategies, the social welfare function 7

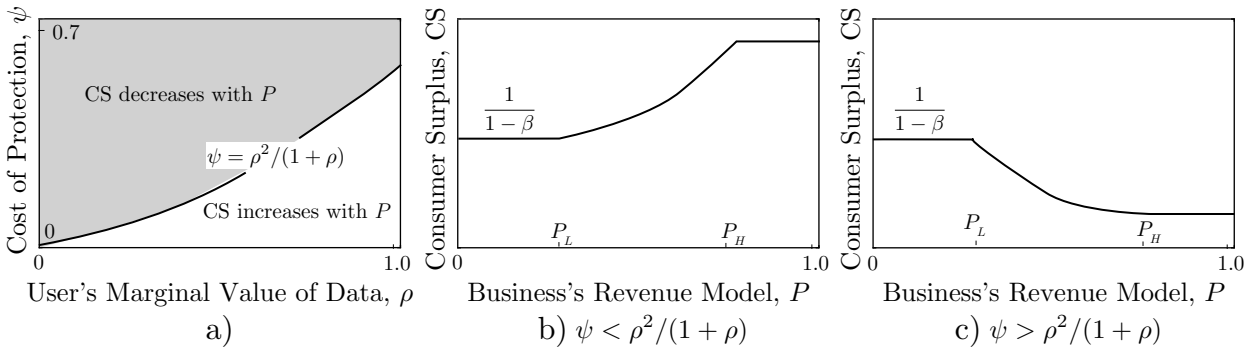

Figure 7: Consumer surplus, $\text{CS}(\xi^\star, C^\star)$, as a function of the business's revenue model, P, and the marginal benefit for consumers from data collection and usage, ρ.

can be rewritten as follows in order to capture dependence on $\bar{a}^*$ and $\bar{a}^*\xi$:

$$\alpha \text{CS}(\cdot|\bar{a}^*) + (1-\alpha)\Pi(\cdot|C, \bar{a}^*, \bar{a}^*\xi), \tag{10}$$

where CS is increasing in $\bar{a}^*$ and Π is decreasing in C and increasing in $\bar{a}^*$ and $\bar{a}^*\xi$.

Assume by contradiction that $\xi^\star \leq \xi^W$ and $C^\star \geq C^W$, and let $W^\star = W(\cdot|C^\star, \xi^\star)$ and $W^W = W(\cdot|C^W, \xi^W)$. By definition, $W^\star \leq W^W$ and $\Pi^\star \geq \Pi^W$. Consequently, it must be true that

$$\bar{a}^*(\xi^W, C^W) \geq \bar{a}^*(\xi^\star, C^\star). \tag{11}$$

Given our contradiction assumption that $\xi^\star \leq \xi^W$ this equation implies that

$$\bar{a}^*(\xi^W, C^W)\xi^W \geq \bar{a}^*(\xi^\star, C^\star)\xi^\star. \tag{12}$$

Then, given our contradiction assumption that $C^\star \geq C^W$ this equation implies that $\Pi^W \geq \Pi^\star$. It can never be the case that $\xi^\star = \xi^W$ and $C^\star = C^W$ (unless $\alpha = 0$). Therefore, for our contradiction assumption to hold it must be that either $\xi^\star < \xi^W$ or $C^\star > C^W$, implying that $\Pi^W > \Pi^*$ in contradiction to the optimality of the business's strategy (that is, contradicting that by definition $\Pi^W \leq \Pi^\star$.

Finally, for purely usage-driven business ($P = 0$): assume that the business over-collects (i.e., $\xi^\star > \xi^W$). Then, necessarily $C^\star > C^W$ from the first-order conditions on the data collection. The argument then follows the one from above: we have by definition $\Pi^\star \geq \Pi^W$ and $W^\star \leq W^W$.

Then, it has to be that $\bar{a}^*(\xi^\star, C^\star) \leq \bar{a}^*(\xi^W, C^W)$. But then it also has to be that $C^\star \leq C^W$, which is a contradiction. Therefore, purely usage-driven business under-collects and under-protects (under-collection and over-protection is prohibited due to the argument in the first part of the proof).

A.5. Proof of Proposition 3 (Page 16)

Without loss of generality, we set $\beta = 0$ ($\beta > 0$ case can be considered in the same way). First, it is easy to show that, when regulation $C_{\min} > C^\star$ is imposed, the firm sets $C = C_{\min}$ and $\xi = \xi^\star(C_{\min})$ (where $\xi^\star(C)$ is derived from the first-order condition on data collection and is given by technical Lemma 2). There exists $C_l = \frac{2+\rho-P(1+\rho)}{P+\rho+P\rho}$ such that $\xi^\star(C_{\min}) = 1$ if $C_{\min} > C_l$ and $\xi^\star(C_{\min}) < 1$ otherwise. Consider three cases:

Case A: $C^\star > C_l$ **hence** $C_{\min} > C_l$ We have $\xi^\star = \xi^*(C_{\min}) = 1$ hence it is obvious that CS increases with introduction of $C_{\min}$ (as users' activity is an increasing function of data protection, C).

Case B: $C^\star < C_l$ **and** $C_{min} < C_l$ Condition $C^\star < C_l$ can be rewritten as $\psi > \psi_L$, which can be rearranged as $P < \frac{2\sqrt{\psi(1+\rho)}-\rho}{1+\rho}$. Furthermore, we can write down users' activity to which the firm shifts upon introduction of the regulation: $\frac{C_{\min}(1+\rho\xi^\star(C_{\min}))}{C_{\min}+\xi^\star(C_{\min})^2}$. Plugging the expression for $\xi^\star(C_{\min})$ and taking the derivative wrt to $C_{\min}$, we obtain after simplification:

$$\frac{(P-1)((P-1)\rho+P)}{4(P(C_{\min}P+P-2)+1)\sqrt{\frac{(C_{\min}P\rho+P-1)^2}{(P(-\rho)+P+\rho)^2}+C_{\min}}}$$

This expression is positive when $\frac{\rho-P\rho-P}{(1-P)^2+C_{\min}P^2} > 0$ which is true when $P < \frac{\rho}{1+\rho}$. This is the condition for CS to increase on $C^\star < C_{\min} < C_l$ upon introduction of $C_{\min}$. If $P > \frac{\rho}{1+\rho}$, CS decreases on this interval.

Case C: $C^\star < C_l$ **and** $C_{min} > C_l$ If $P < \frac{\rho}{1+\rho}$ then CS is increasing for $C_{\min} < C_l$ as per Case B above. For $C_{min} > C_l$ we have $\xi^\star(C_{\min}) = 1$ and an increase in $C_{\min}$ leads to even higher CS. Therefore, $\text{CS}(C_{\min} > C_l) > \text{CS}(C_{\min} = C_l) > \text{CS}(C_{\min} < C_l)$. If $P > \frac{\rho}{1+\rho}$ then $\text{CS}(C_{\min} > C_l, \xi = 1) < \text{CS}(\xi^\star, C^\star)$ unless $C_{\min}$ is higher than $\hat{C}$ such that solves $\text{CS}(\xi^\star, C^\star) = \text{CS}(\hat{C} > C_l, \xi = 1)$.

In summary: when $C_{\min} > C^\star$ we have three regimes. First, if $P > \frac{2\sqrt{\psi(1+\rho)}-\rho}{1+\rho}$ then $C^\star > C_l$

and regulation leads to higher CS. If, $P < \frac{\rho}{1+\rho}$ then $C^\star < C_l$ and regulation also leads to higher CS. In all other cases, regulation hurts if $C_{\min} \in (C^\star, \hat{C})$ and improves CS otherwise (here $\hat{C} > C_l$).

A.6. Proof of Proposition 4 (Page 17)

The proof is a particular case of a more general proof in Online Appendix C.5 (Page 9) which considers business's general profit function.

Online Appendices

B. Appendix: Technical Lemmas

B.1. Proof of Lemma 1

Profit function is concave in C on $C \geq 0$ (by verifying the second-order derivative). Taking the derivative wrt C and solving the FOC, we obtain: $C_h(\xi) = \frac{1}{1-\beta}\left(-\xi^2 + \xi\sqrt{\frac{1}{\psi}(1+\rho\xi)(1-P+P\xi)}\right)$ (the only positive root). Taking the derivative of $C_h(\xi)$ wrt ξ, we get that it's sign is defined by:

$$3\xi\rho - 4\xi\sqrt{\psi(\xi\rho+1)((\xi-1)P+1)} + P((4\xi-3)\xi\rho + 3\xi - 2) + 2$$

It is non-negative at $\xi = 0$. Developing equality $\frac{dC_h(\xi)}{d\xi} = 0$, we get that it is equivalent to:

$$\xi^4 \cdot 16P\rho(P\rho-\psi) + \xi^3 \cdot 8(3P\rho-2\psi)(\rho+P(1-\rho)) + \xi \cdot 12(1-P)(\rho+P(1-\rho)) +$$
$$\xi^2 \cdot ((34P\rho-16\psi)(1-P) + 9\rho^2(1-P) + 9P^2(1+\rho^2)) + 4(1-P)^2$$

Consider two cases. First, let $P\rho > \psi$ then also $3P\rho > 2\psi$. Note also that $34P\rho - 16\psi > 0$. Then coefficients of the polynomial don't change sign, hence there are no positive roots and hence $\frac{dC_h(\xi)}{d\xi} > 0$, $\forall \xi \geq 0$. Since, $C_h(0) = 0$, then $C_h(\xi) > 0, \forall \xi > 0$ in this case.

Now let $\psi > P\rho$. In case $3P\rho < 2\psi$, irrespective of the sign of the coefficient in front of ξ^2, coefficients of the polynomial change sign only once, hence there is one positive root and thus $\frac{dC_h(\xi)}{d\xi}$ changes sign only once for $\xi > 0$. If $3P\rho > 2\psi$ then $34P\rho > 16\psi$ even in the worst case of $\psi = \frac{3}{2}P\rho$, hence coefficient in front of ξ^2 is positive. Thus, there is only one change of sign and hence also one root in this case. Thus, we conclude that when $\psi > P\rho$, derivative $\frac{dC_h(\xi)}{d\xi}$ changes sign only once for $\xi > 0$.

It is easy to see that $C_h(0) = 0$. Also, solving $C_h(\xi) = 0$ for $\xi > 0$ we obtain: $\xi = \frac{P+\rho(1-P)+\sqrt{(P-(1-P)\rho)^2+4(1-P)\psi}}{2(\psi-P\rho)} > 0$ when $\psi > P\rho$. Knowing that $C_h'(\xi)$ changes sign only once if $\psi > P\rho$ and that it increases at $\xi = 0$, we conclude that $C_h(\xi) > 0$ for low ξ if $\psi > P\rho$. The result of lemma now follows.

B.2. Proof of Lemma 2

Expression for $\xi^\star(C)$ follows from solving the first-order condition which has one positive root. Also $-\kappa(C)+\sqrt{\kappa(C)^2+C(1-\beta)}$ is increasing and concave in C. Indeed, the sign of it's derivative wrt C is defined by:

$$\frac{P\rho}{P+(1-P)\rho}+\frac{((1-P)^2\rho^2+P^2(1+2\rho^2C(1-\beta)))}{2(P+(1-P)\rho)^2\sqrt{C(1-\beta)+\kappa^2}}>0$$

Second-order derivative of $-\kappa(C)+\sqrt{\kappa(C)^2+C(1-\beta)}$ is negative. We derive C_l through solving $-\kappa(C)+\sqrt{\kappa(C)^2+C(1-\beta)}<1$. Finally, second-order derivative of the profit function wrt ξ has the sign of $\xi^3+3\xi^2\kappa(C)-3\xi C(1-\beta)-C(1-\beta)\kappa(C)$. Plugging $-\kappa(C)+\sqrt{\kappa(C)^2+C(1-\beta)}$ into this expression, we obtain $-2(C(1-\beta)+\kappa(C)^2)(-\kappa(C)+\sqrt{\kappa(C)^2+C(1-\beta)})<0$.

C. Additional Analysis

C.1. User Heterogeneity

We can consider the following three specifications of user's utility:

$$\begin{aligned}
U_i(a_i,\bar{a}) &= b_ia_i-\frac{1}{2}a_i^2+\beta a_i\bar{a}+(\rho-\omega)a_i\xi\\
U_i(a_i,\bar{a}) &= a_i-\frac{1}{2}a_i^2+\beta a_i\bar{a}+(\rho_i-\omega)a_i\xi\\
U_i(a_i,\bar{a}) &= a_i-\frac{1}{2}a_i^2+\beta a_i\bar{a}+(\rho-\delta_i\omega)a_i\xi
\end{aligned}$$

The three utility specifications capture (i) heterogeneity in standalone benefit, as captured by b_i; (ii) heterogeneity in sensitivity to positive information externalities, as captured by ρ_i; (iii) heterogeneity in sensitivity to negative information externalities, i.e., privacy concerns, as captured by δ_i. In the remainder of this analysis we will focus on the first type of heterogeneity. The other two utility speicfications can be analyzed in similar fashion.

The analysis for utility specification with heterogeneous standalone benefit, b_i follows the proof of Proposition 1 and leads to $\bar{a}^*(\xi,C)=\frac{C(\bar{b}+\rho\xi)}{C(1-\beta)+\xi^2}$, $\omega^*(\xi,C)=\xi\bar{a}^*(\xi,C)/C$, and $\mathrm{CS}(\xi,C)=\frac{1}{2}[\sigma_b^2+\bar{a}^*(\xi,C)^2]$, where $\bar{b}$ and σ_b^2 are users' average standalone benefit and its variance. The only exception is that it has to be checked that in equilibrium best reply of the users $(b_i+\beta\bar{a}+(\rho-\omega)\xi)$

and average activity in response to users' expectation ω of the adversaries' demand for information $\frac{\bar{b}+(\rho-\omega)\xi}{1-\beta}$) are positive. It is easy to verify that the latter is positive. Best reply is positive if: $\xi^2(b_i-\bar{b})+\rho C\xi+C(\bar{b}\beta+b_i(1-\beta))>0$. This inequality holds true for all $b_i>\bar{b}$, otherwise, if $b_i(1+C(1-\beta))-\bar{b}(1-C\beta)+\rho C>0$ for all $b_i<\bar{b}$ and $C>0$ then the inequality holds. Similar conditions can be derived for the other two cases of heterogeneity in sensitivity to positive and negative information externalities.

C.2. General User Utility and Adversary Specification

Assume that user i's utility is generalized to the following form: $U_i(a_i)=U[a_i,\xi(\rho-\omega)]$.[1] The first argument is the user's activity, while the second argument is the user's expectation on the benefit/downside of exerting each unit of activity. We assume that function U is concave in its two arguments and the arguments are complements. We will denote U'_x, U'_y – partial derivatives of U wrt the first and the second arguments respectively. The first-order condition for the user is thus $U'_x(a,\xi(\rho-\omega))=0$.

We assume that adversaries' abilities γ are distributed with cdf G and pdf g. We also assume that distribution of γ satisfies increasing generalized failure rate (IGFR) property (see Lariviere 2006). In other words, we have that $xg(x)/(1-G(x))$ increases in x or alternatively $g'(z)\geq-\frac{g(z)^2}{1-G(z)}$.

The main driving force of the results of the paper was the fact that the equilibrium average activity was non-monotone in the level of data collection strategy ξ. In particular, activity increases with ξ for low ξ and it decreases in ξ when ξ is large. This non-monotonicity in user activity is the result of the interplay between positive and negative externalities that information imposes on users along with the adversaries' endogenous demand for information. When ξ is low, adversaries' demand for information is small, hence information produces more positive than negative externality to users – thus, an increase in ξ incentivises users to be more active. When ξ is large, the adversaries' demand for information is strong, and so negative externalities dominate, and users decrease their activity as ξ grows. We can show that the behavior of user activity inherits such traits in this more general model.

Similar to the result of Proposition 1 we can solve for user's equilibrium activity. In particular,

[1] For simplicity, we omit network effects and assume that data protection strategy C is fixed.

it is such $a^*(\xi)$ solves: $U'_x(a, \xi\rho - \xi G(a\xi/C)) = 0$. Derivative of user activity wrt ξ:

$$\frac{\mathrm{d}a^*(\xi)}{\mathrm{d}\xi} = -\frac{U''_{x,y}(a, \xi\rho - \xi G(a\xi/C))[\rho - G(a\xi/C) - g(a\xi/C)a\xi/C]}{U''_{x,x}(a, \xi\rho - \xi G(a\xi/C)) - U''_{x,y}(a, \xi\rho - \xi G(a\xi/C))g(a\xi/C)\xi^2/C}|_{a=a^*(\xi)}$$

Thus, the sign of this expression is defined by $\mu(\xi) = \rho - G(a^*(\xi)\xi/C) - g(a^*(\xi)\xi/C)a^*(\xi)\xi/C$. At $\xi = 0$ this expression is positive. Its derivative wrt ξ is $\mu'(\xi) = (a^*(\xi)'\xi + a^*(\xi))(-2g(a^*(\xi)\xi/C) - g'(a^*(\xi)\xi/C))$. In order to show that $a^*(\xi)$ first increases and then decreases with ξ, we need to show that $\mu(\xi)$ either always remains positive (then $a^*(\xi)$ always increases) or crosses 0 only once. Assume that there exists $\hat{\xi}$, such that $\mu(\hat{\xi}) = 0$, then also $\frac{\mathrm{d}a^*(\xi)}{\mathrm{d}\xi}|_{\hat{\xi}} = 0$. Using IGFR property of distribution of γ, we conclude that sign of $\mu'(\hat{\xi})$ is defined by $-2 + 2G(a^*(\hat{\xi})\hat{\xi}/C) + g(a^*(\hat{\xi})\hat{\xi}/C)$ which is negative given that we know that at $\hat{\xi}$: $\rho = G(a^*(\hat{\xi})\hat{\xi}/C) + g(a^*(\hat{\xi})\hat{\xi}/C)$. Clearly $a^*(\xi)\xi$ increases with ξ when $a^*(\xi)$ increases. Behavior of $a^*(\xi)\xi$ when $a^*(\xi)$ decreases is defined by the sign of $\xi U''_{x,y}(\ldots)(\rho - G(a^*(\xi)\xi/C)) - U''_{x,x}(\ldots)a^*(\xi)$ and depends on the higher-order derivatives of function U. Notice that for $a^*(\xi)\xi$ to decrease, necessarily it must be that $\rho < \omega = G(a^*(\xi)\xi/C)$ or $a^*(\xi)\xi$ is high enough. $a^*(\xi)\xi$ increases first and then decreases if $\xi(\rho - \omega)/a^*(\xi)$ single-crosses $U''_{x,x}(a^*(\xi), \xi(\rho - \omega))/U''_{x,y}(a^*(\xi), \xi(\rho - \omega))$.

C.3. Users' profiling: an example

Our specification of the users' utility function is motivated by the following simple example. Consider a business – a digital platform that collects information about users' activity for the purpose of user profiling. A user has a characteristic $\theta_i \in \{0, 1\}$ (each realized with probability 1/2) that represents, for example, her political ideology, consumption patterns, dating preferences, etc. Ex ante, the platform has a uniform prior about this characteristic, but can learn it by collecting, storing, and processing what the user writes, shares, and likes. In particular, if the platform stores and analyzes a proportion ξ of user's activity a_i, then it learns the true characteristic θ_i of user i with probability $f(a_i\xi)$, and learns nothing about the user with probability $1 - f(a_i\xi)$.

The business recommends services/products/matches to the user (e.g., a movie, a book, a post, or a date). Recommendation $r = \theta$ creates value of V to a user of type θ and no value to a user of the opposite type. Without learning the user's characteristic, the platform chooses a recommendation at random, and the expected value to the user is $V/2$. On the other hand, if the platform learns the

user's characteristic, the user obtains a perfect recommendation of value V. Hence, in this simple example $\rho = V/2$. The exact magnitude of ρ depends on the specific domain the platform operates in. One could expect ρ to be high in the case of dating platforms, search engines like Google, and marketplaces similar to Amazon. At the same time, one could expect that ρ is lower for platforms offering more impersonal services: e.g., weather forecast services.

Once a user's activity is stored in the platform's database, there is a risk that the very same data will be accessed by individuals and organizations that may try to sway election outcomes, manipulate users' perceptions, personalize health insurance offerings based on confidential data, or commit identity theft (see the introduction for specific examples and a discussion). Such adversarial activities impose a cost on the user, which is normalized to 1. Then, the expected harm to the user is the probability that a third party correctly infers their type, $f(a_i\xi)$, multiplied by the expected number of adversarial activities, ω.

C.4. Product adoption and registration data

Some digital businesses collect data about users primarily during their registration. These data often include demographic and financial information (e.g., age, address, credit card details). In this case, when it comes to privacy concerns, the most important choice faced by users is whether to register or not to the service. To affect users' decisions, the business can determine what and how much information is required to complete registration to the service. The trade-offs we study in previous sections are still present: for example, the business may require storing credit card information on file, which will facilitate seamless future transactions and be beneficial for consumers. However, storing credit card information may also introduce concerns of credit card fraud by adversaries who may get a hold of the data.

In this section we formalize the *adoption model* and show that all of our results carry over to this model with no change. The models of the adversaries and of the business carry over as-is. Our model of users requires accounting for the binary adoption decisions and the introduction of user heterogeneity to facilitate the study of the extensive (adoption) margins.

Let $a_i \in \{0, 1\}$ be the decision ({not register, register}) of user i and consider the following utility

function:

$$U_i(a_i, \bar{a}) = a_i b_i + \beta a_i \bar{a} + (\rho - \omega) a_i \xi. \tag{13}$$

where $b_i \sim U[0,1]$ i.i.d. across users. As a result, user i registers if and only if $b_i + \beta\bar{a} + (\rho-\omega)\xi > 0$ or $b_i > -\beta\bar{a} - (\rho-\omega)\xi$ which happens for mass $\min\{\max\{0, 1 + \beta\bar{a} + (\rho-\omega)\xi\}, 1\}$ of users. That is, as long as some users register and some do not, $\bar{a} = 1 + \beta\bar{a} + (\rho-\omega)\xi$ or, substituting $\omega = \bar{a}\xi/C$ and rearranging, $\bar{a}^* = \frac{C(1+\xi\rho)}{C(1-\beta)+\xi^2}$ as before.

To conclude that all of our results above, including the welfare results, carry over unchanged, it is therefore left to establish that consumers surplus is captured by $CS = \frac{1}{2}\bar{a}^2$. By definition, $\text{CS} = \int_x^1 (b + \beta\bar{a} + (\rho-\omega)\xi)\text{d}b$, where x solves $x + \beta\bar{a} + (\rho-\omega)\xi = 0$. Opening the integral and simplifying we get that $\text{CS} = \frac{1}{2}(1-x)^2$. It is then sufficient to notice that by definition $1 - x = \bar{a}$ to establish that $\text{CS} = \frac{1}{2}\bar{a}^2$ as required.

C.5. General Profit Function

Assume that the profit function of the business is $\Pi(\xi, C) = \Phi(\bar{a}, \bar{a}\xi) - K(C)$. Here, $\bar{a}$ is users' activity as defined in the model section of the paper; function Φ increases in both arguments and is weakly concave in these two arguments; $K(C)$ is an increasing convex function and also $K'(0) = 0$ and $K'(\bar{C}) = \infty$ where $\bar{C} = \frac{1}{(1-\beta)(1+2\rho)}$. The last two assumptions on function $K(C)$ are technical and they guarantee that the business's optimal choice of data protection is always positive and lower than $\bar{C}$, which in turn assures that ξ is interior.

We will show that under this general profit function, our main results are structurally equivalent to that under the linear model. In particular, business's data strategy is inefficient, in general, there are three types of inefficiencies, two-pronged regulatory policy is enough to fix these inefficiencies; and finally, we identify conditions when data protection and data collection are complements.

First-order conditions for profit maximization take the following form:

$$q(\xi^\star, C^\star) = \frac{\Phi'_{\bar{a}}(\bar{a}^*(\xi^\star, C^\star),\, \xi^\star \bar{a}^*(\xi^\star, C^\star))}{\Phi'_{\xi\bar{a}}(\bar{a}^*(\xi^\star, C^\star),\, \xi^\star \bar{a}^*(\xi^\star, C^\star))}, \tag{14}$$

$$\frac{\partial \bar{a}^*(\xi^\star, C^\star)}{\partial C}\left[\Phi'_{\bar{a}}(\bar{a}^*(\xi^\star, C^\star), \xi^* \bar{a}^*(\xi^\star, C^\star)) + \xi \Phi'_{\xi\bar{a}}(\bar{a}^*(\xi^\star, C^\star), \xi\bar{a}^*(\xi^\star, C^\star))\right] = K'(C^\star). \tag{15}$$

Here, function $q(\xi, C) = -\frac{d(\xi\bar{a}^*(\xi,C))}{d\xi} \Big/ \frac{d\bar{a}^*(\xi,C)}{d\xi}$, and by $\Phi'_{\bar{a}}, \Phi'_{\xi\bar{a}}$ we denote first-order partial derivatives

of function Φ with respect to the first (activity) and second (information) arguments, respectively. We will first verify that solution to the above system of equations is indeed maximum.

Lemma 3 *Hessian of* $\Pi(\xi, C)$ *is negative semi-definite when evaluated at* $\xi^\star, C^\star$.

Proof. First, solve first-order condition (14) and (15) wrt $\Phi'_{\bar{a}}$ and $\Phi'_{\xi\bar{a}}$. We get:

$$\Phi'_{\bar{a}}(\bar{a}^*(\xi, C)) = -K'(C)\frac{(\xi^2 + \tilde{C})(\bar{b}(\xi^2 - \tilde{C}) - 2\rho\xi\tilde{C})}{\xi^2(\bar{b} + \rho\xi)^2}$$
$$\Phi'_{\xi\bar{a}}(\bar{a}^*(\xi, C)) = K'(C)\frac{(\xi^2 + \tilde{C})(2\bar{b}\xi + \rho\xi^2 - \tilde{C}\rho)}{\xi^2(\bar{b} + \rho\xi)^2}$$

where $\tilde{C} = C(1 - \beta)$. As before, we will use shorthand notation $\Phi''_{\bar{a},\bar{a}}, \Phi''_{\xi\bar{a},\xi\bar{a}}, \Phi''_{\xi\bar{a},\bar{a}}$ to denote second-order derivatives of function Φ. For the rest of the proof, all functions are evaluated at optimal $\xi^\star, C^\star$, yet we will write ξ, C for simplicity. We will also use the following notation: $A \equiv \frac{\partial \bar{a}^*(\xi,C)}{\partial \xi}, B \equiv \frac{\partial(\xi\bar{a}^*(\xi,C))}{\partial \xi}$ and $D \equiv \frac{\partial \bar{a}^*(\xi,C)}{\partial C}, E \equiv \frac{\partial(\xi\bar{a}^*(\xi,C))}{\partial C}$. Then second-order derivatives of the function $\tilde{\Pi}(\xi, C) = \Phi(\bar{a}^*(\xi, C), \xi\bar{a}^*(\xi, C))$:

$$\frac{\partial^2\tilde{\Pi}(\xi,C)}{\partial\xi^2} = \Phi''_{\bar{a},\bar{a}}A^2 + 2\Phi''_{\xi\bar{a},\bar{a}}AB + \Phi''_{\xi\bar{a},\xi\bar{a}}B^2 + \Phi'_{\bar{a}}\frac{\partial^2\bar{a}^*(\xi,C)}{\partial\xi^2} + \Phi'_{\xi\bar{a}}\frac{\partial^2(\xi\bar{a}^*(\xi,C))}{\partial\xi^2}$$
$$\frac{\partial^2\tilde{\Pi}(\xi,C)}{\partial\xi\partial C} = \Phi''_{\bar{a},\bar{a}}AD + \Phi''_{\xi\bar{a},\bar{a}}(AE + BD) + \Phi''_{\xi\bar{a},\xi\bar{a}}BE + \Phi'_{\bar{a}}\frac{\partial^2\bar{a}^*(\xi,C)}{\partial\xi\partial C} + \Phi'_{\xi\bar{a}}\frac{\partial^2(\xi\bar{a}^*(\xi,C))}{\partial\xi\partial C}$$
$$\frac{\partial^2\tilde{\Pi}(\xi,C)}{\partial C^2} = \Phi''_{\bar{a},\bar{a}}D^2 + 2\Phi''_{\xi\bar{a},\bar{a}}DE + \Phi''_{\xi\bar{a},\xi\bar{a}}E^2 + \Phi'_{\bar{a}}\frac{\partial^2\bar{a}^*(\xi,C)}{\partial C^2} + \Phi'_{\xi\bar{a}}\frac{\partial^2(\xi\bar{a}^*(\xi,C))}{\partial C^2}$$

Substituting $\Phi'_{\bar{a}}, \Phi'_{\xi\bar{a}}$ found above, we get:

$$\tilde{\Pi}''_{\xi\xi}(\xi,C) = \Phi''_{\bar{a},\bar{a}}A^2 + 2\Phi''_{\xi\bar{a},\bar{a}}AB + \Phi''_{\xi\bar{a},\xi\bar{a}}B^2 + \lambda_{\xi\xi}, \text{ where } \lambda_{\xi\xi} = -2K'(C)\frac{C(\bar{b}^2 + \tilde{C}\rho)}{\xi^2(\bar{b} + \rho\xi)^2} < 0$$
$$\tilde{\Pi}''_{\xi C}(\xi,C) = \Phi''_{\bar{a},\bar{a}}AD + \Phi''_{\xi\bar{a},\bar{a}}(AE + BD) + \Phi''_{\xi\bar{a},\xi\bar{a}}BE + \lambda_{\xi C}, \text{ where } \lambda_{\xi C} = 2K'(C)\frac{\tilde{C}}{\xi(\xi^2 + \tilde{C})} > 0$$
$$\tilde{\Pi}''_{\xi\xi}(\xi,C) = \Phi''_{\bar{a},\bar{a}}D^2 + 2\Phi''_{\xi\bar{a},\bar{a}}DE + \Phi''_{\xi\bar{a},\xi\bar{a}}E^2 + \lambda_{CC}, \text{ where } \lambda_{CC} = -2K'(C)\frac{(1-\beta)}{\xi^2 + \tilde{C}} < 0$$

It can be easily shown that $\tilde{\Pi}''_{\xi\xi}(\xi, C) \leq 0$ and $\tilde{\Pi}''_{CC}(\xi, C) \leq 0$ using concavity of Φ (e.g., see, proof of Proposition 6). Finally, $\tilde{\Pi}_{\xi\xi}(\xi, C)\tilde{\Pi}_{CC}(\xi, C) - \tilde{\Pi}^2_{\xi C}(\xi, C)$ after simple algebraic manipulations can

be rewritten as:

$$\left(\Phi''_{\bar{a},\bar{a}}\Phi''_{\xi\bar{a},\xi\bar{a}} - (\Phi''_{\xi\bar{a},\bar{a}})^2\right)(BD-AE)^2 + \lambda_{CC}\lambda_{\xi\xi} - \lambda_{\xi C}^2 + 2\Phi''_{\xi\bar{a},\bar{a}}(AB\lambda_{CC} - (BD+AE)\lambda_{\xi C} + DE\lambda_{\xi\xi}) +$$
$$\Phi''_{\bar{a},\bar{a}}(A^2\lambda_{CC} - 2AD\lambda_{\xi C} + D^2\lambda_{\xi\xi}) + \Phi''_{\xi\bar{a},\xi\bar{a}}(B^2\lambda_{CC} - 2BE\lambda_{\xi C} + E^2\lambda_{\xi\xi})$$

The first term is non-negative due to concavity of Φ. The second and the third terms can be combined and simplified (substitute the expressions for λ) to $\frac{4\tilde{C}(\bar{b}\xi-\rho\tilde{C})^2K'(C)^2}{\xi^2(\xi^2+\tilde{C})^2(\bar{b}+\rho\xi)^2}$ which is non-negative. Thus, we are left to determine the sign of the last three terms. We can rewrite those as follows:

$$\frac{2CK'(C)}{(\xi^2+\tilde{C})^4}\left(-\Phi''_{\bar{a},\bar{a}}\mu^2 - 2\Phi''_{\xi\bar{a},\bar{a}}\mu\eta - \Phi''_{\xi\bar{a},\xi\bar{a}}\eta^2 - \Phi''_{\xi\bar{a},\xi\bar{a}}\tilde{C}\xi^2(\bar{b}+\rho\xi)^2\right) \tag{16}$$

where $\mu = \bar{b}\xi - \tilde{C}\rho$ and $\eta = \bar{b}(\xi^2 - \tilde{C}) - 2\rho\xi\tilde{C}$. Notice that sign of μ can be either positive or negative, while $\eta < 0$ since $\xi < \bar{\xi}(C)$, where $\bar{\xi}$ solves $\eta = 0$. The multiplier of expression (16) is positive. The last term is also positive since $\Phi''_{\xi\bar{a},\xi\bar{a}} \leq 0$. Finally, irrespective of the sign of μ The first three terms can also be shown positive using concavity of Φ (applying the same technique as in the proof of Proposition 6). Hence, we showed that at optimal $\xi^\star, C^\star$ Hessian of $\tilde{\Pi}(\xi, C)$ is negative semi-definite. Given that $K''(C) \geq 0$, we have Hessian of the profit function $\Pi(\xi, C)$ is also negative semi-definite at $\xi^\star, C^\star$. ■

Proposition 5 *(i) Fix the level of data protection, C. The data collection strategy of a purely-usage driven business is socially optimal. For all other types of businesses (i.e., not purely usage-driven), their optimal data collection level as well as total users' data collected are too large, while users' activity (and consequently consumer surplus) are too low, as compared to socially optimal outcome.*

(ii) Fix the level of data collection, ξ. Relative to the socially optimal outcome, the business's data protection level, total users' data collected and users' activity are too low.

Proof. Fix C, the derivative of the welfare function $W(\xi, C)$ (Eq. 7) wrt ξ and divided by $1-\alpha$ is

$$\frac{1}{1-\alpha}W'_\xi(\xi, C) = \frac{\alpha}{1-\alpha}\bar{a}^*(\xi, C)\frac{\partial\bar{a}^*(\xi, C)}{\partial\xi} + \Phi'_{\bar{a}}\cdot\frac{\partial\bar{a}^*(\xi, C)}{\partial\xi} + \Phi'_{\xi\bar{a}}\cdot\frac{\partial(\xi\bar{a}^*(\xi, C))}{\partial\xi} \tag{17}$$

For brevity here we denote $\Phi'_{\bar{a}}$ and $\Phi'_{\xi\bar{a}}$ partial derivatives of the profit function wrt activity

and information respectively (first and second arguments). Both derivatives are evaluated at $(\bar{a}^*(\xi,C),\xi\bar{a}^*(\xi,C))$. For $\alpha\in(0,1)$ and non purely usage-driven business (i.e., $\Phi'_{\xi\bar{a}}>0$), expression (17) is positive at $\underline{\xi}(C)$ and negative at $\bar{\xi}(C)$. The first term of Eq. (17) is negative for any $\xi\in(\underline{\xi}(C),\bar{\xi}(C))$. When solving the first-order-condition $W'_\xi(\xi,C)=0$ to obtain socially-optimal $\xi^W(C)$, only solutions, which are such that $W'_\xi(\xi,C)$ intersects horizontal axis from above, can be local maxima. It is clear then that when comparing those solutions to profit-maximizing $\xi^\star(C)$ (i.e., $\alpha=0$), we get $\xi^W(C)\geq\xi^\star(C)$. The ordering of total users' data collected and users' activity then follow. When the business is purely usage-driven, the last term of Eq. (17) is zero. Then the first-order condition for socially-optimal data collection level $\xi^W(C)$ is such that $\bar{a}^*(\xi,C)$ is maximized. This holds for any level of α, including $\alpha=0$, which implies $\xi^\star(C)=\xi^W(C)$.

Now, fix ξ. The derivative of $W(\xi,C)$ wrt C is:

$$\frac{1}{1-\alpha}W'_C(\xi,C)=\frac{\alpha}{1-\alpha}\bar{a}^*(\xi,C)\frac{\partial\bar{a}^*(\xi,C)}{\partial C}+\Phi'_{\bar{a}}\cdot\frac{\partial\bar{a}^*(\xi,C)}{\partial C}+\xi\Phi'_{\xi\bar{a}}\cdot\frac{\partial\bar{a}^*(\xi,C)}{\partial C}-K'(C) \tag{18}$$

The derivative is positive at $C=0$ and is $-\infty$ at $\bar{C}$. The first term of Eq. 18 is positive. Any local maximum is such that Eq. 18 intersects horizontal axis from above. Hence, an increase in α shifts local maxima to the right. Hence $C^\star(\xi)\leq C^W(\xi)$ and the result follows. ■

Theorem 2 and its proof are the same for the case of the general profit function.

The statement of Proposition 4 is not changed. Below we provide its proof for the case of the general profit function.

Proof of Proposition 4 (Page 17) with General Profit Function.

Proof. We will prove statement of the proposition for the case when liability policy $\ell^\star$ is used. The proof when tax rate $t^\star$ is used is similar. The profit function of the business under liability policy is $\Pi(\xi,C,\ell)=\Phi(\bar{a}^*(\xi,C),\xi\bar{a}^*(\xi,C))-K(C)-\frac{\ell}{C}[\xi\bar{a}^*(\xi,C)]^2$. The first-order conditions are:

$$\frac{\partial\Pi(\xi,C,\ell)}{\partial\xi}=\frac{\partial\Phi(\bar{a}^*(\xi,C),\xi\bar{a}^*(\xi,C))}{\partial\xi}-2\frac{\ell}{C}\bar{a}^*(\xi,C)\xi\frac{\partial(\xi\bar{a}^*(\xi,C))}{\partial\xi} \tag{19}$$

$$\frac{\partial\Pi(\xi,C,\ell)}{\partial C}=\frac{\partial\Phi(\bar{a}^*(\xi,C),\xi\bar{a}^*(\xi,C))}{\partial C}+\frac{\ell}{C}\bar{a}^*(\xi,C)\xi^2\left(\frac{\bar{a}^*(\xi,C)\xi}{C}-2\frac{\partial(\xi\bar{a}^*(\xi,C))}{\partial C}\right) \tag{20}$$

Now, evaluate these conditions at socially-optimal ξ^W,C^W. The first-order condition for socially-optimal data collection is $\frac{\partial\Phi}{\partial\xi}(1-\alpha)+\alpha\frac{\partial\bar{a}^*(\xi,C)}{\partial\xi}=0$ (by derivation of Eq. 7). Substitute $\frac{\partial\Phi}{\partial\xi}$ into

Eq. (19) and solve for ℓ. We will get expression (8) for optimal liability rate $\ell^\star$. After simplification (use $\frac{\partial \Phi}{\partial C}$ from the first-order condition for socially-optimal data protection), the first-order conditions for business's profit at $\xi^W, C^W, \ell^\star$ become:

$$\frac{\partial \Pi(\xi, C, \ell^\star)}{\partial \xi}\Big|_{\xi^W, C^W} = 0$$
$$\frac{\partial \Pi(\xi, C, \ell^\star)}{\partial C}\Big|_{\xi^W, C^W} = \frac{C^W \rho \xi^W (1+\rho\xi^W)^2}{2((\xi^W)^2 + C^W(1-\beta))((\xi^W)^2 - C^W(1-\beta) - 2\rho\xi^W C^W(1-\beta))} < 0$$

Where the second inequality follows from the fact that ξ^W, C^W are such that $\xi^W < \bar{\xi}(C)$ (To see that, notice that $-\xi^2 + C(1-\beta) + 2\rho\xi C(1-\beta)$ defines the sign of $\partial \bar{a}\xi/\partial\xi$. In equilibrium, both for the business and for the social planner it must be that $\partial \bar{a}\xi/\partial\xi > 0$ and $\partial \bar{a}/\partial\xi < 0$, otherwise, they would be able to increase their objectives by either increasing or decreasing ξ depending on the signs of the derivatives). Thus, business under minimum data protection $C \geq C_{\min}$ requirement and liability policy $\ell^\star$, sets ξ^W, C^W. In case if $\Phi'_{\xi\bar{a}} = 0$, welfare is maximized when activity $\bar{a}^*(\xi, C)$ is maximized, hence condition $\frac{\partial \Pi(\xi,C)}{\partial \xi}|_{\xi^W, C^W, \ell} = 0$ is satisfied with $\ell = 0$. ■

Finally, we will show that under the general profit function, the business sees its data collection and data protection strategies as complements for a large and economically relevant family of revenue models.

Proposition 6 *Suppose that for any $\bar{a}$ and ξ, $\Phi''_{\xi\bar{a},\bar{a}}(\bar{a}, \xi\bar{a}) \geq -\xi\Phi''_{\xi\bar{a},\xi\bar{a}}(\bar{a}, \xi\bar{a})$, then at the business's equilibrium strategy, data collection ξ and data protection C are complements. That is, $\frac{\partial^2 \Pi(\xi,C)}{\partial\xi\partial C}|_{\xi^\star, C^\star} > 0$.*

Intuitively, the condition of Proposition 6 guarantees that, for the business's profit, users' activity and users' information are sufficiently strong complements, relative to the second-order effects of users' activity data. This condition is satisfied in many formulations often used in economics, such as in the case that Φ is linear as well as if Φ is a Cobb-Douglas or a CES function. It is also satisfied for a business that is purely usage-driven, regardless of the specific functional form of Φ.

Proof. First-order conditions for profit-maximizing $\xi^\star, C^\star$ can be rewritten as:

$$\Phi'_{\bar{a}} = -K'(C)\frac{(\xi^2+\tilde{C})(\xi^2-\tilde{C}-2\rho\xi\tilde{C})}{\xi^2(1+\rho\xi)^2}$$
$$\Phi'_{\xi\bar{a}} = K'(C)\frac{(\xi^2+\tilde{C})(2\xi+\rho\xi^2-\tilde{C}\rho)}{\xi^2(1+\rho\xi)^2}$$

where $\tilde{C} = C(1-\beta)$ and as in the proofs above we use $\Phi'_{\bar{a}}, \Phi'_{\xi\bar{a}}$ for brevity. We will also use shorthand notation $\Phi''_{\bar{a},\bar{a}}, \Phi''_{\xi\bar{a},\xi\bar{a}}, \Phi''_{\xi\bar{a},\bar{a}}$ to denote second-order derivatives of function Φ. For the rest of the proof, all functions are evaluated at optimal $\xi^\star, C^\star$, yet we will write ξ, C for brevity. We will also use the following notation: $A \equiv \frac{\partial\bar{a}^*(\xi,C)}{\partial\xi}, B \equiv \frac{\partial(\xi\bar{a}^*(\xi,C))}{\partial\xi}$ and $D \equiv \frac{\partial\bar{a}^*(\xi,C)}{\partial C}, E \equiv \frac{\partial(\xi\bar{a}^*(\xi,C))}{\partial C}$. Then the mixed derivate of the profit function is:

$$\frac{\partial^2\Pi(\xi,C)}{\partial\xi\partial C} = \Phi''_{\bar{a},\bar{a}}AD + \Phi''_{\xi\bar{a},\bar{a}}(AE+BD) + \Phi''_{\xi\bar{a},\xi\bar{a}}BE + \Phi'_{\bar{a}}\frac{\partial^2\bar{a}^*(\xi,C)}{\partial\xi\partial C} + \Phi'_{\xi\bar{a}}\frac{\partial^2(\xi\bar{a}^*(\xi,C))}{\partial\xi\partial C} \quad (21)$$

Using the first-order conditions, the last two terms can be shown to be equal to $2K'(C)\frac{\tilde{C}}{\xi(\xi^2+\tilde{C})} > 0$. The first three terms of Eq. 21 can be rearranged as follows:

$$\frac{\partial\bar{a}^*(\xi,C)}{\partial C}\frac{\partial\bar{a}^*(\xi,C)}{\partial\xi}\left(\Phi''_{\bar{a},\bar{a}} + 2\Phi''_{\xi\bar{a},\bar{a}}\xi + \xi^2\Phi''_{\xi\bar{a},\xi\bar{a}}\right) + \bar{a}^*(\xi,C)\frac{\partial\bar{a}^*(\xi,C)}{\partial C}\left(\Phi''_{\xi\bar{a},\bar{a}} + \xi\Phi''_{\xi\bar{a},\bar{a}}\right) \quad (22)$$

The first term is non-negative due to concavity of function Φ. Indeed, we have $\Phi''_{\bar{a},\bar{a}} \leq 0, \Phi''_{\xi\bar{a},\xi\bar{a}} \leq 0$ and $|\Phi''_{\xi\bar{a},\bar{a}}| \leq \sqrt{\Phi''_{\bar{a},\bar{a}}\Phi''_{\xi\bar{a},\xi\bar{a}}}$. If at $\xi^\star, C^\star$, $\Phi''_{\xi\bar{a},\bar{a}} \leq 0$ then the first term is non-negative. Similarly, if at $\xi^\star, C^\star$, $\Phi''_{\xi\bar{a},\bar{a}} \geq 0$, then substitute $\Phi''_{\xi\bar{a},\bar{a}} = -\sqrt{\Phi''_{\bar{a},\bar{a}}\Phi''_{\xi\bar{a},\xi\bar{a}}}$ to the first term to find its lower bound which can be shown to be non-negative. The second term of Eq. (22) is non-negative by assumption of the Proposition, which finishes the proof. ■

C.6. Business Always Weakly Over-Collects Data when $\rho = 0$

Set $\rho = 0$. One can use similar techniques to those in the proof of Theorem 1 to derive welfare maximizing ξ^W, C^W (i.e., those that maximize Eq. (7)). In particular, there exist $\psi_L(\alpha) = \frac{P-P\sqrt{1-2P\alpha(1-\alpha)}}{4\alpha}$ and $\psi_H(\alpha) = \frac{P^2(1-\alpha)}{4(1-P(1-\alpha))}$ such that $\xi^W = 1$ when $\psi < \psi_L(\alpha)$; $\xi^W = 0$ when $\psi > \psi_H(\alpha)$; and $\xi^W(\alpha) = \frac{P(4\psi-P(1-\alpha)(P+4\psi))}{4\psi(2\alpha\psi-P^2(1-\alpha))}$ otherwise. Trivially, $\psi_L(\alpha) < \lim_{\alpha\to 0}\psi_L(\alpha), \forall\alpha > 0$. Also, $\psi_H(\alpha) < \psi_H(0), \forall\alpha > 0$. Finally, $\xi^W(\alpha) < \xi^W(0) = \xi^\star$, where $\xi^\star$ is profit-maximizing data

collection strategy. Thus, we conclude that the business always weakly over-collects data when $\rho = 0$.

C.7. Vertical Integration Example (Section 6.2, Page 20)

Consider the linear model and two digital businesses $j \in \{1, 2\}$. The profit function of business j has now an added term $\delta_j \mathbb{1}_{merger} \xi_{-j} \bar{a}^*_{-j}$, where $\delta_j > 0$ and $\mathbb{1}_{merger}$ is the indicator function, taking a value of 1 if the businesses allow for reciprocal access to their databases and 0 otherwise (i.e., $\mathbb{1}_{merger} = 1$ if business 1 can access database of business 2 and vice versa). Users' utilities and adversaries' cost-benefit structure remain the same as before.

Now consider the following three scenarios: Scenario 0 is the pre-merger scenario, the two businesses act independently without sharing information. In Scenario DM (Data Merger), the businesses allow for reciprocal access to their databases but maintain autonomy over setting their data collection policies. Finally, in Scenario SM (Strategy Merger), in addition to the reciprocal access to data, businesses decide jointly on their data collection policies.

It is easy to see that in Scenario DM, businesses' data collection policies, user activity, privacy costs, and consumer surplus will remain the same as in Scenario 0, but profits will increase. In contrast, in Scenario SM the businesses will internalize the positive externalities they impose on each other by collecting information. As a result, data collection, profits, and privacy costs will increase, whereas user activity and consumer surplus will decrease relative to Scenarios 0 and DM. Intuitively, the move to Scenario SM is akin to a business becoming more data-driven, leading to increased data collection and a decrease in user activity.

C.8. Paying Users for Data (Section 6.3, Page 21)

Users' utility is modified by adding $t\bar{a}\xi$, which, in the case of exogenous t is equivalent to setting $\tilde{\rho} = \rho + t$. Thus, $\bar{a}^*(\xi, C)$ is modified by increasing ρ to $\tilde{\rho}$. Denote modified users' response as $\tilde{a}^*(\xi, C)$. Then business's profit without paying for data is $\Pi(\xi) = (1-P)\bar{a}^*(\xi, C) + P\xi\bar{a}^*(\xi, C)$ and when paying for data it is $\tilde{\Pi} = (1-P)\tilde{a}^*(\xi, C) + P\xi\tilde{a}^*(\xi, C) - t\tilde{a}^*(\xi, C)\xi$. Without loss of generality let $\beta = 0$.

Fix C. Equilibrium data collection strategy of the business which pays for data $\xi^\star(t)$ has the following form: $(1-P)\frac{\partial \bar{a}^*(\xi, C)}{\partial \xi} + (P-t)\frac{\partial (\xi \bar{a}^*(\xi, C))}{\partial \xi} = 0$. Solving for equilibrium $\xi^\star(t, C)$ we obtain:

$\xi^\star(t,C) = -\kappa(t,C) + \sqrt{\kappa(t,C)^2 + C}$ – decreasing in $\kappa(t,C)$, where $\kappa(t,C) = \frac{1-P-(P-t)(\rho+t)C}{P-t+(1-P)(\rho+t)}$. The sign of the derivative of $\kappa(t,C)$ wrt t is defined by $-CPt^2 + 2tC(P+\rho(1-P)) + (1-P)P + C((1-P)\rho^2 - P^2)$. Equilibrium data collection strategy of the business which doesn't pay for data is $\xi^\star = \xi^\star(0,C)$. If $P(1-P) + C((1-P)\rho^2 - P^2) < 0$ then at $t \to 0$, we will get $\xi^\star(t,C) > \xi^\star$ – at least for small t business collects higher fraction of user information than with $t = 0$. Now, consider $t = P$, then business sets $\underline{\xi}(t = P)$ (s.t. $\frac{\mathrm{d}\tilde{a}^*(\xi)}{\mathrm{d}\xi} = 0$) – data collection strategy maximizing consumer surplus.

C.9. The Real Cost of Adversarial Activity: Beyond Regulating Business

Even under the socially optimal data strategy, users experience negative externalities caused by adversarial activity. In fact, it turns out that the direct disutility or damage inflicted on users by adversaries capture only a small part of the loss of welfare due to adversarial activity, and that the total welfare loss from the presence of adversaries can be arbitrarily large.

Proposition 7 *Let* $\mathrm{CS}_{no\ adversaries}(\xi, C)$ *be consumer surplus in the absence of adversaries.*[2] *For any data strategy* (ξ, C)*, the total decrease in consumer surplus due to the presence of adversaries,* $\mathrm{CS}_{no\ adversaries}(\xi, C) - \mathrm{CS}(\xi, C)$*, equals* $\mathcal{M}(\xi, C) \cdot D(\xi, C)$*, where* $D(\xi, C)$ *is the average damage caused to a user as described in Definition 1 and* $\mathcal{M}(\xi, C)$ *is the adversarial loss multiplier. Moreover,* $\mathcal{M}(\xi, C) \geq \frac{2}{1-\beta}$.

Proof. Average activity in the case with no adversaries can be obtained by setting $\omega = 0$ in the proof of Proposition 1. Average damage from Definition 1 is $D(\xi, C) = \frac{(\xi \bar{a}^*(\xi,C))^2}{C}$. Then we have:

$$\mathcal{M}(\xi, C) = \frac{\mathrm{CS}_{\text{no adversaries}}(\xi, C) - \mathrm{CS}(\xi, C)}{D(\xi, C)} = \frac{C}{2\xi^2}\left(\left(\frac{1+\rho\xi}{1-\beta}\right)^2 - \left(\frac{C(1+\rho\xi)}{C(1-\beta)+\xi^2}\right)^2\right) \Big/ \left(\frac{C(1+\rho\xi)}{C(1-\beta)+\xi^2}\right)^2$$

Simplifying we obtain $\mathcal{M}(\xi, C) = \frac{\xi^2 + 2C(1-\beta)}{2C(1-\beta)^2} = \frac{\xi^2}{2C(1-\beta)^2} + \frac{1}{1-\beta} \geq \frac{1}{1-\beta}$. ■

Proposition 7 suggests that governments may want to take a more comprehensive approach that supplements the aforementioned policies with steps to minimize the government's share of adversarial activities as well as outlawing a wider range of private adversarial activities and establishing corresponding independent enforcement authorities.

[2] In particular, $\bar{a}(\xi, C)_{\text{no adversaries}} = \frac{1+\rho\xi}{1-\beta}$ and $\mathrm{CS}_{\text{no adversaries}}(\xi, C) = \frac{1}{2}\bar{a}(\xi, C)^2_{\text{no adversaries}}$.

C.10. Harmful Ads

In our narrative throughout the paper, we included the targeting of ads as a positive factor in users' utility functions. That is, users prefer relevant ads and information revealed by users through their activity improves the match between them and the ads they observe. However, in practice, targeting of certain ads may also lead to a reduction in users' utility. Consider, for instance, targeting adds of addictive products to vulnerable users (e.g., an AA member can be targeted with an ad for alcoholic beverages), similarly some ads may be misleading or even manipulative.[3]

Notably, harmful targeting relies on data collected and quality targeting technology in order to be effective. Moreover, if, as digital businesses often argue, they prefer not to advertise harmful ads, they may invest in the better screening of the advertising content that they post. Circumventing the additional screening is costly to marketers who seek to post harmful ads, and thus the extra screening can be thought of as a form of data protection (or protection of the ability to target using the data). Our analysis of optimal regulation thus follows with this alternative interpretation.

[3]See, e.g., Liu et al. 2020 and references therein; see also "Facebook Says It Won't Back Down From Allowing Lies in Political Ads", *The New York Times*, 9 Jan 2020, on Facebook's policy regarding misleading campaign ads.