Information Sciences 424 (2018) 354–384

Contents lists available at ScienceDirect

Information Sciences

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

Optimized, direct sale of privacy in personal data marketplaces

Javier Parra-Arnau[*]

Department of Computer Science and Mathematics, Universitat Rovira i Virgili (URV), E-08034 Tarragona, Spain

ARTICLE INFO

Article history:
Received 2 May 2017
Revised 30 August 2017
Accepted 4 October 2017
Available online 6 October 2017

Keywords:
User privacy
disclosure risk
data brokers
disclosure-money trade-off

ABSTRACT

Very recently, we are witnessing the emergence of a number of start-ups that enables individuals to sell their private data directly to brokers and businesses. While this new paradigm may shift the balance of power between individuals and companies that harvest and mine data, it raises some practical, fundamental questions for users of these services: how they should decide which data must be vended and which data protected, and what a good deal is. In this work, we investigate a mechanism that aims at helping users address these questions. The investigated mechanism relies on a hard-privacy model and allows users to share partial or complete profile data with broker and data-mining companies in exchange for an economic reward. The theoretical analysis of the trade-off between privacy and money posed by such mechanism is the object of this work. We adopt a generic measure of privacy although part of our analysis focuses on some important examples of Bregman divergences. We find a parametric solution to the problem of optimal exchange of privacy for money, and obtain a closed-form expression and characterize the trade-off between profile-disclosure risk and economic reward for several interesting cases. Finally, we evaluate experimentally how our approach could contribute to privacy protection in a real-world data-brokerage scenario.

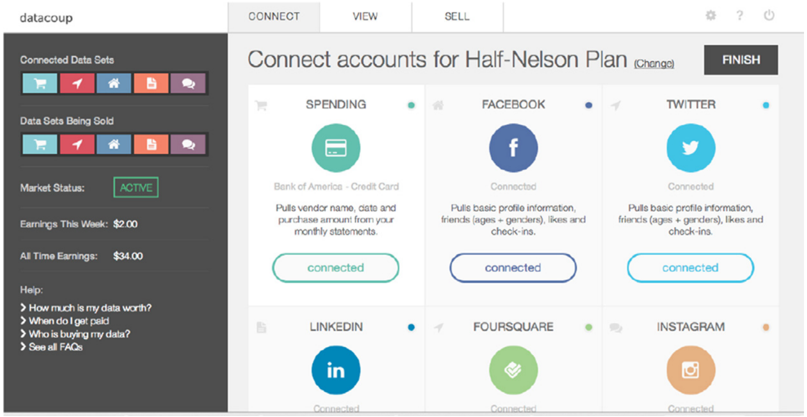
1. Introduction

Over the last recent years, much attention has been paid to government surveillance, and the indiscriminate collection and storage of tremendous amounts of information in the name of national security. However, what most people are not aware of is that a more serious and subtle threat to their privacy is posed by hundreds of companies they have probably never heard of, in the name of commerce.

They are called *data brokers*, and they gather, analyze and package massive amounts of sensitive personal information, which they sell as a product to each other, to advertising companies or marketers, often without our knowledge or consent. A substantial chunk of this is the kind of harmless consumer marketing that has been going on for years. Nevertheless, what has recently changed is the amount and nature of the data being extracted from the Internet and the rapid growth of a tremendously profitable industry that operates with no control whatsoever. Our habits, preferences or interests, our friends, personal data such as date of birth, number of children or home address, and even our daily movements, are some examples of the personal information we are giving up without being aware it is being collected, stored and finally sold to a wide range of companies.

[*] *E-mail address:* javier.parra@urv.cat

https://doi.org/10.1016/j.ins.2017.10.009
0020-0255/© 2017 Elsevier Inc. All rights reserved.



Connect accounts for Half-Nelson Plan (Change)

Connected Data Sets

Data Sets Being Sold

Market Status: ACTIVE

Earnings This Week: $2.00

All Time Earnings: $34.00

SPENDING

Bank of America - Credit Card

Pulls vendor name, date and purchase amount from your monthly statements.

FACEBOOK

Connected

Pulls basic profile information, friends (ages + genders), likes and check-ins.

TWITTER

Connected

Pulls basic profile information, friends (ages + genders), likes and check-ins.

LINKEDIN

Connected

FOURSQUARE

Connected

INSTAGRAM

Connected

Fig. 1. Screenshot of Datacoup which allows users to earn money by sharing their personal data.

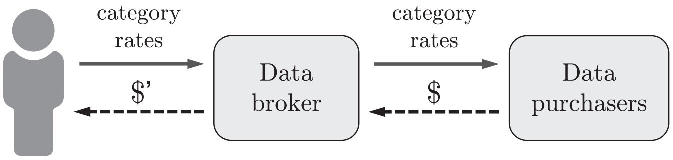


Fig. 2. Conceptual depiction of the data-purchasing model assumed in this work. In this model, users first send the data broker their category rates, that is, the money they would like to be paid for completely exposing their actual interests in each of the categories of a profile. For example, a user might be willing to reveal their purchasing habits on clothing for 7 dollars. Based on the rates chosen for each category, data buyers decide then whether to pay the user for learning their profile and gaining access to the underlying data. Finally, depending on the offer made, the disclosure may range from portions of their profile to the complete actual profile.

A vast majority of the population understands that this is part of an unwritten contract whereby they get content and services free in return for letting advertisers track their behavior; this is the current barker economy that, for example, currently sustains the Web. But while a significant part of the population finds this tracking invasive, there are people who do not give a toss about being mined for data [3].

Very recently we are witnessing the emergence of a number of start-ups that hope to exploit this by buying access to our social-networks accounts and banking data. One such company is Datacoup, which lets users connect their apps and services via APIs in order to sell their data. Datacoup, and similar start-ups, however, do not provide raw data to potential data purchasers, among others, retailers, marketers, insurance companies and banks. Rather, they typically build a profile that gives these companies an overview of a user's data.

The emergence of these start-ups is expected to provide a win-win situation both for users and data buyers. On the one hand, users will receive payments, discounts or various rewards from purchasing companies, which will take advantage of the notion that users are receiving a poor deal when they trade personal data in for access to "free" services. On the other hand, companies will earn more money because the quality of the data these start-ups will offer to them will be much greater than that currently provided by traditional brokers —the problem with the current data brokers is often the stale and inaccurate data [51].

Undoubtedly, the creation of a marketplace in personal data will represent a significant shift in the balance of power between individuals and companies that gather and mine data. According to some recent studies, this is a shift people would be willing to embrace. Just over half of the 9 000 people surveyed worldwide said they would share data about themselves with companies in exchange for cash [5]. A separate survey has found that 42 percent of more than a thousand 13-17-year-olds in the U.K. would rather accept cash for their personal data than earn money from a job [6]. Lastly, it was reported in [4] that 56% of the consumers surveyed would be willing to give up personal data provided that they received some kind of economic compensation.

The possibility that individuals may vend their private data *directly* to businesses and retailers will be one step closer with the emergence of companies like Datacoup. For many, this can have a liberating effect. It permeates the opaque data-exchange process with a new transparency, and empowers online users to decide what to sell and what to retain. However, the prospect of people selling data directly to brokers poses a myriad of new problems for their owners. How should they manage the sale of their data? How should they decide which elements must be offered up for mining and which ones protected? What is a good deal?

1.1. Contribution and plan of this paper

In this paper, we investigate a mechanism that aims at helping users address these questions. The investigated mechanism builds upon the new data-purchasing paradigm developed by broker companies like Datacoup, CitizenMe and DataWallet, which allows users to sell their private data *directly* to businesses and retailers. The mechanism analyzed in this work, however, relies on a variant of such paradigm which gives priority to users, in the sense that they are willing to disclose partial or complete profile data only when they have an offer on the table from a data buyer, and not the other way round. Also, we assume a hard-privacy model by which users take charge of protecting their private data on their own, without the requirement of trusted intermediaries.

The theoretical analysis of the trade-off between disclosure risk and economic reward posed by said mechanism is the object of this work. We tackle the issue in a mathematically, systematic fashion, drawing upon the methodology of multi-objective optimization. We present a mathematical formulation of optimal exchange of profile data for money, which takes into account the trade-off between both aspects and contemplates a rich variety of functions as quantifiable measures of user-profile privacy. Our theoretical analysis finds a closed-form solution to the problem of optimal sale of profile data, and characterizes the optimal trade-off between disclosure risk and money. Experimental results in a real environment demonstrate the suitability and feasibility of our approach in a real-world data-mining scenario.

The remainder of this paper is organized as follows. Section 2 introduces our mechanism for the exchange of profile data for economic reward, proposes a model of user-profile information, and formulates the trade-off between privacy and money. We proceed with a theoretical analysis in Section 3, while Section 3.7 numerically illustrates the main results. Section 4 conducts an experimental evaluation of the proposed mechanism. Next, Section 6 reviews the state of art relevant to this work. Finally, conclusions are drawn in Section 7.

2. A mechanism for the sale of privacy in personal data marketplaces

In this section, we present a mechanism that allows users to share portions of their profile with data-broker companies, in exchange for an economic reward. The description of our mechanism is prefaced by a brief introduction of the concept of hard privacy and our data-purchasing model. Then, we propose a user-profile model and elaborate on our assumptions about the privacy attacker, in our case, data brokers and any entity with access to profile information. Finally, we provide several candidate functions for measuring the privacy of a disclosed profile, and present a formulation of the trade-off between privacy and money.

2.1. Hard-privacy and data-purchasing model

Privacy-enhancing technologies (PETs) can be classified depending on the level of trust placed by their users [16]. A privacy mechanism providing *soft privacy* assumes that users entrust their private data to an entity, which is thereafter responsible for the protection of their data. In the literature, numerous attempts to protect privacy have followed the traditional method of pseudonymization and anonymization [12,45], which are essentially based on the assumptions of soft privacy. Unfortunately, these methods are not completely effective [9,34,38,41], they normally come at the cost of infrastructure, and suppose that users are willing to trust other parties.

The mechanism investigated in this work, per contra, capitalizes on the principle of *hard privacy*, which assumes that users mistrust communicating entities and are therefore reluctant to delegate the protection of their privacy to them. In the motivating scenario of this work, hard privacy means that users do not trust the new data brokerage firms —not to mention data purchasers— to safeguard their personal data. Consequently, because users just trust themselves, it is their own responsibility to protect their privacy.

In the data-purchasing model supported by most of these new data brokers, users, just after registering —and without having received any money yet—, must give these companies access to one or several of their accounts. As mentioned in the introductory section, brokers at first do not provide raw data to potential buyers and data miners. Rather, purchasers are shown a *profile* of the data available at those accounts, which gives them an accurate-enough description of a user's interests, so as to make a decision on whether to bid or not for that particular user. If a purchaser is finally interested in a given profile, the data of the corresponding account are sold at the price fixed by the broker. Obviously, the buyer can at that point verify that the purchased data corresponds to the profile it was initially shown, that is, it can check the profile was built from such data. At the end of this process, users are notified of the purchase.

In this work, we assume a variation of this data-purchasing model that reverses the order in which transactions are made. In essence, we consider a scenario where, first, users receive an economic reward, and then, based on that reward, their data are partly or completely disclosed to the bidding companies; this variation is in line with the literature of pricing private data [47], examined in Section 6. Also, we contemplate that users themselves take charge of this information disclosure, without the intervention of any external entity, following the principle of hard privacy.

More specifically, users of our data-buying model first notify brokers of the compensation they wish to receive for fully disclosing each of the components of their profile —we shall henceforth refer to these compensations as *category rates*. For example, if profiles represent purchasing habits across a number of categories, a user might specify low rates for completely revealing their shopping activity in groceries, and they might impose higher prices on more sensitive purchasing categories

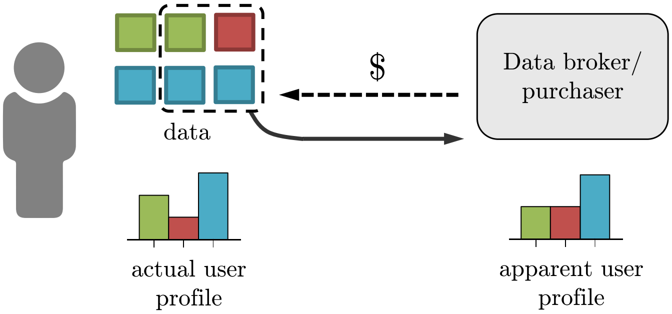


Fig. 3. A data purchaser offers a user a certain amount of money for disclosing their profile. Because the offered money does not satisfy all their demands, they cannot show the buyer their actual profile but a distorted version of it.

like health care[1]. Afterwards, based on these rates, interested buyers try to make a bid for the entire profile. However, as commented above, it is now up to the user to decide whether to accept or decline the offer. Should it be accepted, the user would disclose their profile according to the money offered, and give the buyer —and the intermediary broker— access to the corresponding data.

As we shall describe more precisely in the coming subsections, we shall assume a controlled disclosure of user information that will hinge upon the particular economic reward given. Basically, the more money is offered to a user, the more similar the disclosed profile will be to the actual one. Furthermore, we shall assume that there exists a communication protocol enabling this exchange of information for money, and that users behave honestly in *all* steps of said data-transaction process. This work does not tackle the practical details of an implementation of this protocol and the buying model described above. This is nevertheless an important issue, and dispelling the assumption that must behave honestly is one of the many exciting directions for future work.

2.2. Profile representation

In this work, we model user private data (e.g., posts and tags on social networks, transactions in a bank account) as a sequence of random variables (r.v.'s) taking on values in a common finite alphabet of categories, in particular the set $\mathscr{X} = \{1, \dots, n\}$ for some integer $n \geq 2$. In our mathematical model, we assume these r.v.'s are independent and identically distributed. This assumption permits us to represent the profile of a user by means of the probability mass function (PMF) according to which such r.v.'s are distributed, a model that is widely accepted in the privacy literature [23,40,43,53,54].

Conceptually, we may interpret a profile as a histogram of relative frequencies of user data within that set of categories. For instance, in the case of a bank account, grocery shopping and traveling expenses could be two categories. In the case of social-networks accounts, on the other hand, posts could be classified across topics such as politics, sports and technology.

In our scenario of data monetization, users may accept unveiling some pieces of their profile, in exchange for an economic reward. Users may consider, for example, revealing a fraction of their purchases on Zappoos, and may avoid disclosing their payments at nightclubs. Clearly, depending on the offered compensation, the profile observed by the broker and buying companies will resemble, to a greater or lesser extent, the genuine, accurate shopping habits of the user. In this work, we shall refer to these two profiles as the *actual user profile* and the *apparent user profile*, and denote them by q and t, respectively. Fig. 3 provides an example of these two profiles.

2.3. Privacy models

Before deciding how to disclose a profile for a given reward, users must bear in mind the privacy objective they aim with such disclosure. In the literature of information privacy, this objective is inextricably linked to the concrete assumptions about the attacker against which a user wants to protect. This is known as the *adversary model* and its importance lies in the fact that the level of privacy provided is measured with respect to it.

In this work, data brokers, data-buying companies and in general any entity with access to profile information may all be regarded as privacy attackers. Under this scenario, we consider two possible adversary models which are completely in the line with the technical literature of profiling [27,28] and which have been extensively used by the privacy research community [17,19–21,26,32,44,54,56]. As described below, the difference between these two adversary models lies in the objective of scrutinizing said profile information:

[1] We contemplate that these rates are specified on a per-category basis, and vary over time depending on users' needs and perceptions on privacy, as well as marketers' requirements to satisfy their demand. However, as in any competitive market, the unit price will be determined on the basis of supply and demand.

Table 1
Main conceptual highlights of the adversary model assumed in this work.

What scenario is assumed?	We consider a scenario where a user first communicates their category rates to the data broker. This is the only information that users reveal before the bidding process begins. Then, based on those rates, interested buyers may bid to acquire their profile. If the user accepts the offer, they must disclose their profile in accordance with the offered money, and give the buyer and the broker access to the corresponding data. If no money is offered, the user shows their initial profile.
Who can be the privacy attacker?	Any entity with access to profile information. This includes the entities acquiring this information, i.e., the data-buying companies, and the data broker, which acts as an intermediary between users and such companies.
How are user profiles modeled?	Profiles are modeled as *histograms of relative frequencies* of user data across a predefined set of categories.
What is the attacker after with a user's profile?	We contemplate two possible objectives for an attacker: *individuation* and *classification*. The former objective reflects an attacker wishing to target peculiar users, while the latter objective is associated with an adversary aimed at identifying a given user as a member of a specific group of users.
How is the profile disclosed for a given reward?	The disclosure of a user's profile is conducted to equate to the offered reward while countering an individuation or a classification attack.

- On the one hand, we may consider the attacker strives to target users who deviate from the average profile of interests or habits. We refer to this objective as *individuation* [27,28], meaning that the adversary aims at discriminating a given user from the whole population of users, or said otherwise, wishes to learn what distinguishes that user from the other users;
- On the other hand, we may assume that the attacker's goal is to classify a user into a predefined group of users. To conduct this *classification*, the attacker contrasts the user's profile with the profile representative of a particular group.

In our mathematical model, the choice of either privacy model implies deciding on an *initial profile* p the user wants to impersonate when no money is bid for their data. For example, in the individuation model, a user would want to show common, typical habits, trying to hide their profile in the crowd, and thus making it less interesting to an attacker whose objective is to target peculiar users. In this case, the average profile of the population could be the right choice for p. In the classification model, on the other hand, a user who does not want to be identified as a member of a given group might be comfortable with exhibiting the profile of another, maybe less-sensitive group.

In either case (i.e., individuation or classification), p only represents interests or preferences the user is disposed to show to the broker or purchasing companies when no money is offered for their data. The choice of p is up to the user, who must decide whether or not the impersonation of this profile is sufficiently private for them. As we shall explain in the next subsection, this initial profile will provide a "neutral" starting point for the disclosure of the actual profile q. Table 1 summarizes the assumptions about the adversary model.

2.4. Disclosure-money mechanism

This section proposes a disclosure mechanism appropriate for the data-buying and privacy models described in Secs. 2.2 and 2.3. The proposed mechanism operates between these two scenarios. When no reward is bid for getting access to a user account, the mechanism shows the initial PMF p, which, in the hands of the data broker and any potential purchaser, does not pose any privacy risk to the user. However, when the user is offered sufficient economic reward, the genuine profile q is completely revealed and their privacy fully jeopardized.

Our disclosure mechanism moves in the continuum between these two scenarios by revealing the deviation of the user's initial, fake interest to the genuine one. For any category $i = 1, \ldots, n$, we define the *disclosure rate* δ_i as the percentage of disclosure lying on the line segment between p_i and q_i. Accordingly, we define the user's apparent profile as

$$t = (1 - \delta)\, p + \delta\, q,$$

where $\delta = (\delta_1, \ldots, \delta_n)$ is some *disclosure strategy* provided by the user.

The operation of the mechanism can therefore be viewed as shifting the apparent profile t from the initial distribution to the authentic one, evidently whilst satisfying that the disclosed information equates to the money offered by the data purchaser. However, the question that follows immediately is, how is user privacy affected by this shift? In other words, how do we measure the privacy of t?

In this work, we do not consider one specific privacy criterion but quantify a user's *privacy risk* generically as

$$\mathcal{R} = f(t, p),$$

where $f(t, p)$ is a *privacy function* that measures the extent to which the user is discontent when the initial profile is p and the apparent profile is t.

A variety of functions may be chosen to reflect this degree of dissatisfaction a user experiences when moving from p towards q. The suitability and appropriateness of the chosen privacy function, however, will depend on the user's own perception regarding privacy and the adversary model assumed. Clearly, depending on whether the data purchaser aims at classifying users or finding uncommon profiles, $\mathcal{R}$ will represent a risk of classification or uniqueness.

A particularly interesting class of those privacy functions are the *dissimilarity or distance metrics*, which have been extensively used to measure the privacy of user profiles. The intuitive reasoning behind these metrics is that apparent profiles closer to p offer better privacy protection than those closer to q, which is consistent with the two privacy models described in Section 2.3. Examples of these functions comprise the Euclidean distance, Kullback-Leibler (KL) divergence [13], and the cosine and Hamming distances.

2.5. Optimal trade-off between disclosure risk and money

With a function of the privacy risk a disclosure strategy entails, the proposed mechanism aims at finding the strategy that yields the minimum risk for a given economic reward. Next, we formalize the problem of choosing said strategy as a multiobjective optimization problem whereby users can configure a suitable trade-off between disclosure risk and money.

Let $w = (w_1, \dots, w_n)$ be the tuple of category rates specified by a user, that is, the amount of money they require to completely disclose their interests or habits in each category. Since in our data-buying model users have no motivation for giving their private data for free, we shall assume these rates are positive. Accordingly, for a given economic compensation μ, we define the *disclosure-money function* as

$$\mathcal{R}(\mu) = \min_{\substack{\delta \\ \sum_i (q_i - p_i)\delta_i = 0, \\ \sum_i w_i \delta_i = \mu, \\ 0 \preccurlyeq \delta \preccurlyeq 1}} f(t, p), \tag{1}$$

which characterizes the optimal trade-off between the disclosure of profile data and economic compensation.

The optimization problem above also expresses the intuitive reasoning behind our mechanism. In the case of a similarity function as privacy criterion, for example, the level of exposure is chosen to minimize the differences between t and p. The minimization in (1), however, is also conducted under the premise that the received money is effectively exchanged for private information. In more practical terms, our formulation reflects the desired requirement that neither f nor p can determine the profits to be pocketed: users' profits only depend on the categories rates w_i.

On the other hand, the solution to the optimization problem above is a tuple δ^* that aims to help users decide how they should expose their profiles so that their privacy is maximized for a given compensation. The theoretically investigation of this tuple and, in general, the disclosure-money function, is the object of the following section and this work.

3. Optimal disclosure of profile information

This section is entirely devoted to the theoretical analysis of the disclosure-money function (1) defined in Section 2.5. In our attempt to characterize the trade-off between disclosure risk and money, we shall present a solution to the optimization problem inherent in the definition of this function. Afterwards, we shall analyze some fundamental properties of said trade-off for several interesting cases. For the sake of brevity, our theoretical analysis only contemplates the case when all given probabilities and category rates are strictly positive:

$$q_i, p_i > 0 \text{ for all } i = 1, \dots, n. \tag{2}$$

Without loss of generality, we shall assume that

$$q_i \neq p_i \text{ for all } i = 1, \dots, n. \tag{3}$$

We note that we can always restrict the alphabet $\mathscr{X}$ to those categories where $q_i \neq p_i$ holds, and redefine the two probability distributions accordingly.

In this work, we shall limit our analysis to the case of real-valued privacy functions f: $(t, p) \mapsto f(t, p)$ that are twice differentiable on the interior of their domains. In addition, we shall consider these functions capture a measure of *dissimilarity or distance* between the PMFs t and p, and accordingly assume that

$$f(t, p) \geqslant 0, \tag{4}$$

with equality if, and only if, $t = p$. Occasionally, we shall denote f more compactly as a function of δ_i, on account of the fact that $t_i = (1 - \delta_i)\, p_i + \delta_i\, q_i$, and that p_i and q_i are fixed variables.

Before establishing some notational aspects and diving into the mathematical analysis, it is immediate from the definition of the disclosure-money function and the assumptions made above that its initial value is $\mathcal{R}(0) = 0$. The characterization of the optimal trade-off curve modeled by $\mathcal{R}(\mu)$ at any other values of μ is the focus of this section. Lastly, note that $q = p$ describes the trivial case in which a user accepts disclosing their complete genuine profile for whatever amount of money is given, including $\mu = 0$. Our mathematical model captures this case consistently, although from a practical perspective it may not reflect a realistic or common situation.

3.1. Notation and preliminaries

This section introduces our notation and recalls several measures of statistical distance and key geometric concepts assumed to be known in the remainder of this work.

We shall adopt the same notation for vectors used in [10]. Specifically, we delimit vectors and matrices with square brackets, with the components separated by space, and use parentheses to construct column vectors from comma separated lists.

Occasionally, we shall use the notation $x^{\mathrm{T}}y$ to indicate the standard inner product on $\mathbb{R}^n$, $\sum_{i=1}^{n} x_i y_i$, and $\|\cdot\|$ to denote the Euclidean norm, i.e., $\|x\| = (x^{\mathrm{T}}x)^{1/2}$. Recall [10] that a *hyperplane* is a set of the form

$$\{x : v^{\mathrm{T}}x = b\},$$

where $v \in \mathbb{R}^n$, $v \neq 0$, and $b \in \mathbb{R}$. Geometrically, a hyperplane may be regarded as the set of points with a constant inner product to a vector v. Note that a hyperplane separates $\mathbb{R}^n$ into two halves; each of these halves is called a *halfspace*. The results developed in the coming subsections will build upon a particular intersection of halfspaces, usually referred to as *slab*. Concretely, a slab is a set of the form

$$\{x : b_l \leqslant v^{\mathrm{T}}x \leqslant b_u\},$$

the boundary of which are two hyperplanes. Informally, we shall refer to them as the lower and upper hyperplanes.

In our analysis, we shall focus on three measures of statistical distance between distributions as privacy functions, namely the squared Euclidean distance (SED), the KL divergence [13] and the Itakura-Saito distance (ISD) [30], the three belonging to the family of Bregman divergences [11]. These functions will be denoted respectively by f_{SED}, f_{KL} and f_{ISD}. Finally, when not specified, the base of the logarithms is taken to base 2.

3.2. Monotonicity and convexity

Our first theoretical characterization, namely Theorems 1 and 3, investigates two elementary properties of the disclosure-money trade-off. The theorems in question show that the trade-off is nondecreasing and convex. The importance of these two properties is that they confirm the evidence that an economic reward will never lead to an improvement in privacy protection. In other words, accepting money from a data purchaser does not lower privacy risk. Together, these two results will allow us to determine the shape of $\mathcal{R}(\mu)$.

Before proceeding, define $\mu_{\max} = \sum_i w_i$ and note that when $\mu = \mu_{\max}$, the equality condition $\sum_i w_i \delta_i = \mu$ implies $\delta_i = 1$ for all i. Hence, $\mathcal{R}(\mu_{\max}) = f(q, p)$. Also, observe that the disclosure-money function is not defined for a compensation $\mu > \mu_{\max}$ since the optimization problem inherent in the definition of this function is not feasible.

Theorem 1 (Monotonicity)**.** *The disclosure-money function $\mathcal{R}(\mu)$ is nondecreasing.*

Proof. Consider an alternative disclosure-money function $\mathcal{R}^a(\mu)$ where the condition $\sum_i w_i \delta_i = \mu$ is replaced by these two inequality constraints, $\mu \leq \Sigma_i w_i \delta_i \leq \mu_{\max}$. We shall first show that this function is nondecreasing and, based on it, we shall prove the monotonicity of $\mathcal{R}(\mu)$.

Let $0 \leq \mu < \mu' \leq \mu_{\max}$, and denote by δ' the solution to the minimization problem corresponding to $\mathcal{R}^a(\mu')$. Clearly, δ' is feasible to the problem $\mathcal{R}^a(\mu)$ since $\mu' > \mu$. Because the feasibility of δ' does not necessarily imply that it is a minimizer of the problem corresponding to $\mathcal{R}^a(\mu)$, it follows that

$$\mathcal{R}^a(\mu) \leqslant f\big((1-\delta')p + \delta' q,\ p\big) = \mathcal{R}^a(\mu'),$$

and hence that the alternative disclosure-money function is nondecreasing.

This alternative function can be expressed in terms of the original one, by taking $\mathcal{R}(\mu)$ as an inner optimization problem of $\mathcal{R}^a(\mu)$, namely

$$\mathcal{R}^a(\mu) = \min_{\mu \leqslant \alpha \leqslant \mu_{\max}} \mathcal{R}(\alpha).$$

Based on this expression, it is straightforward to verify that the only condition consistent with the fact that $\mathcal{R}^a(\mu)$ is nondecreasing is that $\mathcal{R}(\mu)$ be nondecreasing too. □

Next, we define an interesting property borrowed from [13] for KL divergence, that will be used in Theorem 3 to show the convexity of the disclosure-money function.

Definition 2. A privacy function *f*(*t*, *p*) is *convex in the pair* (*t*, *p*) if

$$f(\lambda t_1 + (1-\lambda)t_2, \lambda p_1 + (1-\lambda)p_2) \leqslant \lambda f(t_1, p_1) + (1-\lambda) f(t_2, p_2), \tag{5}$$

for all pairs of probability distributions (t_1, p_1) and (t_2, p_2) and all $0 \leq \lambda \leq 1$.

Theorem 3 (Convexity)**.** *If f(t, p) is convex in the pair (t, p), then the corresponding disclosure-money function $\mathcal{R}(\mu)$ is convex.*

Proof. The proof closely follows the proof of Theorem 1 of [43]. We proceed by checking the definition of convexity, that is, that

$$(1-\lambda)\,\mathcal{R}(\mu)+\lambda\,\mathcal{R}(\mu')\geqslant\mathcal{R}((1-\lambda)\,\mu+\lambda\,\mu')$$

for all $0 \le \mu < \mu' \le \mu_{\max}$ and all $0 \le \lambda \le 1$. Denote by δ and δ' the solutions to $\mathcal{R}(\mu)$ and $\mathcal{R}(\mu')$, respectively, and define $\delta_\lambda = (1-\lambda)\,\delta+\lambda\,\delta'$. Accordingly,

$$\begin{aligned}(1-\lambda)\,\mathcal{R}(\mu)+\lambda\,\mathcal{R}(\mu') &= (1-\lambda)\,f((1-\delta)\,p+\delta\,q,\ p)+\lambda\,f((1-\delta')\,p+\delta' q,\ p)\\ &\overset{\text{(a)}}{\geqslant} f\Big((1-\lambda)\,((1-\delta)\,p+\delta\,q)\\ &\quad +\lambda\,((1-\delta')\,p+\delta' q),\ p\Big)\\ &= f((1-\delta_\lambda)\,p+\delta_\lambda\,q,\ p)\\ &\overset{\text{(b)}}{\geqslant} \mathcal{R}((1-\lambda)\,\mu+\lambda\,\mu'),\end{aligned}$$

where

(a) follows from the fact that $f(t, p)$ is convex in the pairs of probability distributions [13, Section 2], and
(b) reflects that δ_λ is not necessarily the solution to the minimization problem $\mathcal{R}((1-\lambda)\,\mu+\lambda\,\mu')$. □

The convexity of the disclosure-money function (1) guarantees its continuity on the interior of its domain, namely (0, $\mu_{\max}$). However, it can be readily checked, directly from the definition of $\mathcal{R}(\mu)$, that continuity also holds at the interval endpoints, 0 and $\mu_{\max}$.

Lastly, we would like to point out the generality of the results shown in this subsection, which are valid for a wide variety of privacy functions $f(t, p)$, provided that they are non-negative, twice differentiable and convex in the pair (t, p). Some examples of functions meeting these properties are the SED and KL divergence. Appendix A shows that the SED satisfies Definition 2.

3.3. Parametric solution

Our next result, Lemma 4, provides a parametric solution to the minimization problem involved in the formulation of the disclosure-money trade-off (1) for certain privacy functions. Even though said lemma provides a parametric-form solution, fortunately we shall be able to proceed towards an explicit closed-form expression, albeit piecewise, for some special cases and values of n. For the sake of notational compactness, we define the difference tuple $d = (q_1 - p_1, \ldots, q_n - p_n)$.

Lemma 4 (General Parametric Solution). *Let f be additively separable into the functions f_i for $i = 1, \ldots, n$. For all i, let $f_i : [0, 1] \to \mathbb{R}$ be twice differentiable in the interior of its domain, with $f_i'' > 0$, and hence strictly convex. Because $f_i'' > 0$, f_i' is strictly increasing and therefore invertible. Denote the inverse by $f_i'^{-1}$. Now consider the following optimization problem in the variables $\delta_1, \ldots, \delta_n$:*

$$\begin{aligned}&\text{minimize} && \sum_{i=1}^{n} f_i(\delta_i)\\ &\text{subjectto} && 0 \leqslant \delta_i \leqslant 1 \text{ for } i = 1, \ldots, n,\\ &&& \sum_{i=1}^{n} d_i\delta_i = 0 \text{ and } \sum_{i=1}^{n} w_i\delta_i = \mu.\end{aligned} \tag{6}$$

The solution to the problem exists, is unique and of the form

$$\delta_i^* = \max\left\{0, \min\{f_i'^{-1}(\alpha\, d_i + \beta\, w_i), 1\}\right\},$$

for some real numbers α, β such that $\sum_i d_i\delta_i^* = 0$ and $\sum_i w_i\delta_i^* = \mu$.

Proof. We organize the proof in two steps. In the first step, we show that the optimization problem stated in the lemma is convex; then we apply Karush-Kuhn-Tucker (KKT) conditions to said problem, and finally reformulate these conditions into a reduced number of equations. The bulk of this proof comes later, in the second step, where we proceed to solve the system of equations.

To see that the problem is convex, simply observe that the objective function f is the sum of strictly convex functions f_i, and that the inequality and equality constraint functions are affine. The existence and uniqueness of the solution is then a consequence of the fact that we minimize a strictly convex function over a convex set. Since the objective and constraint functions are also differentiable and Slater's constraint qualification holds, KKT conditions are necessary and sufficient conditions for optimality [10, Section 5]. The application of these optimality conditions leads to the following Lagrangian cost,

$$\mathcal{L} = \sum f_i(\delta_i) - \sum \lambda_i \delta_i + \sum \mu_i(\delta_i - 1) - \alpha \sum d_i \delta_i - \beta\Big(\sum w_i \delta_i - \mu\Big),$$

and finally to the conditions

$$\begin{aligned} & f_i'(\delta_i) - \lambda_i + \mu_i - \alpha d_i - \beta w_i = 0 && \text{(dualoptimality)},\\ & \lambda_i \delta_i = 0,\ \mu_i(\delta_i - 1) = 0 && \text{(complementaryslackness)},\\ & \lambda_i, \mu_i \geqslant 0 && \text{(dualfeasibility)},\\ & 0 \leqslant \delta_i \leqslant 1,\ \sum d_i \delta_i = 0,\ \sum w_i \delta_i = \mu && \text{(primalfeasibility)}. \end{aligned}$$

We may rewrite the dual optimality condition as $\lambda_i = f_i'(\delta_i) + \mu_i - \alpha d_i - \beta w_i$ and $\mu_i = \alpha d_i + \beta w_i - f_i'(\delta_i) + \lambda_i$. By eliminating the slack variables λ_i, μ_i, and by substituting the above expressions into the complementary slackness conditions, we can formulate the dual optimality and complementary slackness conditions equivalently as

$$f_i'(\delta_i) + \mu_i \geqslant \alpha d_i + \beta w_i, \tag{7}$$

$$f_i'(\delta_i) - \lambda_i \leqslant \alpha d_i + \beta w_i, \tag{8}$$

$$(f_i'(\delta_i) + \mu_i - \alpha d_i - \beta w_i)\, \delta_i = 0, \tag{9}$$

$$(f_i'(\delta_i) - \lambda_i - \alpha d_i - \beta w_i)\, (\delta_i - 1) = 0. \tag{10}$$

In the following, we shall proceed to solve these equations which, together with the primal and dual feasibility conditions, are necessary and sufficient conditions for optimality. To this end, we consider these three possibilities for each i: $\delta_i = 0$, $0 < \delta_i < 1$ and $\delta_i = 1$.

We first assume $\delta_i = 0$. By complementary slackness, it follows that $\mu_i = 0$ and, in virtue of (7), that $f_i'(0) \geqslant \alpha d_i + \beta w_i$. We now suppose that this latter inequality holds and that $\delta_i > 0$. However, if δ_i is positive, by Eq. (8) we have $f_i'(\delta_i) \leqslant \alpha d_i + \beta w_i$, which contradicts the fact that f_i' is strictly increasing. Hence, $\delta_i = 0$ if, and only if, $\alpha d_i + \beta w_i \leqslant f_i'(0)$.

Next, we consider the case $0 < \delta_i < 1$. Note that, when $\delta_i > 0$, it follows from the conditions (8) and (9) that $f_i'(\delta_i) \leqslant \alpha d_i + \beta w_i$, which, by the strict monotonicity of f_i', implies $f_i'(0) < \alpha d_i + \beta w_i$. On the other hand, when $\delta_i < 1$, the conditions (10) and (7) and again the fact that f_i' is strictly increasing imply that $\alpha d_i + \beta w_i < f_i'(1)$.

To show the converse, that is, that $f_i'(0) < \alpha d_i + \beta w_i < f_i'(1)$ is a sufficient condition for $0 < \delta_i < 1$, we proceed by contradiction and suppose that the left-hand side inequality holds and the solution is zero. Under this assumption, Eq. (10) implies that $\mu_i = 0$, and in turn that $f_i'(0) \geqslant \alpha d_i + \beta w_i$, which is inconsistent with the fact that f_i' is strictly increasing. Further, assuming $\alpha d_i + \beta w_i < f_i'(1)$ and $\delta_i = 1$ implies that $\lambda_i = 0$ and, on account of (8), that $f_i'(1) \leqslant \alpha d_i + \beta w_i$, a contradiction. Consequently, the condition $0 < \delta_i < 1$ is equivalent to

$$f_i'(0) < \alpha d_i + \beta w_i < f_i'(1),$$

and the only conclusion consistent with (7) and (8) is that $f_i'(\delta_i) = \alpha d_i + \beta w_i$, or equivalently,

$$\delta_i = f_i'^{-1}(\alpha d_i + \beta w_i).$$

The last possibility corresponds to the case when $\delta_i = 1$, which by Eqs. (9) and (8) imply $f_i'(1) \leqslant \alpha d_i + \beta w_i$. Next, we check that this latter condition is sufficient for $\delta_i = 1$. We first assume $0 < \delta_i < 1$. In this case, $\lambda_i = \mu_i = 0$ and the dual optimality conditions reduce to $f_i'(\delta_i) = \alpha d_i + \beta w_i$, which contradicts the fact that f_i' is strictly increasing. Assuming $\delta_i = 0$, on the other hand, leads to $f_i'(0) \geqslant \alpha d_i + \beta w_i$, which runs contrary to the condition $f_i'(1) \leqslant \alpha d_i + \beta w_i$ and the strict monotonicity of f_i'.

In summary, $\delta_i = 0$ if $\alpha d_i + \beta w_i \leqslant f_i'(0)$, or equivalently, $f_i'^{-1}(\alpha d_i + \beta w_i) \leqslant 0$; $\delta_i = f_i'^{-1}(\alpha d_i + \beta w_i)$ if $f_i'(0) < \alpha d_i + \beta w_i < f_i'(1)$, or equivalently, $0 < f_i'^{-1}(\alpha d_i + \beta w_i) < 1$; and $\delta_i = 1$ if $\alpha d_i + \beta w_i \geqslant f_i'(1)$, or equivalently, $f_i'^{-1}(\alpha d_i + \beta w_i) \geqslant 1$. Accordingly, we may write the solution compactly as

$$\delta_i^* = \max\left\{0, \min\{f_i'^{-1}(\alpha\, d_i + \beta\, w_i), 1\}\right\},$$

where α, β must satisfy the primal equality constraints $\sum_i d_i \delta_i = 0$ and $\sum_i w_i \delta_i = \mu$. □

As mentioned at the beginning of this subsection, the optimization problem presented in the lemma is the same as that of (1) but for additively separable, twice differentiable objective functions, with strictly increasing derivatives. Although these requirements obviously restrict the space of possible privacy functions of our analysis, the fact is that some of the

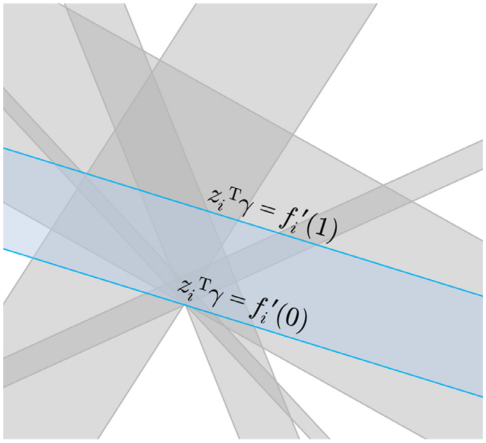

$z_i^{\mathrm{T}}\gamma = f_i'(1)$
$z_i^{\mathrm{T}}\gamma = f_i'(0)$

Fig. 4. Slabs layout on the α–β plane for $n = 6$ categories. Each component of the solution is determined by a slab and, in particular, by the specific γ falling on the plane. We show in dark blue the lower and upper hyperplanes of the i-th slab. In general, it will be difficult to proceed towards an explicit closed-form solution and to study the corresponding optimal disclosure-money trade-off for any configuration of these slabs and any γ and n. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

best known dissimilarity and distance functions satisfy these requirements. This is the case of some of the most important examples of Bregman divergences [11], such as the SED, KL divergence and ISD. In the interest of brevity, many of the results shown in this section will be derived only for some of these three particular distance measures. Due to its mathematical tractability, however, special attention will be given to the SED.

For notational simplicity, hereafter we shall denote by z_i and γ the column vectors (d_i, w_i) and (α, β), respectively. A compelling result of Lemma 4 is the maximin form of the solution and its dependence on the inverse of the derivative of the privacy function. The particular form that each of the n components of the solution takes, however, hinges on whether $d_i\alpha + w_i\beta$ is greater or less than the value of the derivative of f_i at 0 and 1; equivalently, in our vector notation, the lemma shows that the solution is determined by the specific configuration of the n slabs

$$\nabla f(0) \preccurlyeq z^{\mathrm{T}}\gamma \preccurlyeq \nabla f(1),$$

where $\nabla f(0)$ denotes the gradient of f at 0, and z_i are the columns of z. In particular, the i-th component of the solution is equal to 0, 1 or $f_i'^{-1}(z_i^{\mathrm{T}}\gamma)$ if, and only if, $z_i^{\mathrm{T}}\gamma \leqslant f_i'(0)$, $z_i^{\mathrm{T}}\gamma \geqslant f_i'(1)$, or $f_i'(0) < z_i^{\mathrm{T}}\gamma < f_i'(1)$, respectively.

From the lemma, it is clear then that γ, which must satisfy the primal equality constraints $d^{\mathrm{T}}\delta = 0$ and $w^{\mathrm{T}}\delta = \mu$, is the parameter that configures the point of operation within the α–β plane where all such halfspaces lie. Informally, the region of this plane where γ falls on is what determines which precise components are 0, 1 and $f_i'^{-1}(z_i^{\mathrm{T}}\gamma)$. Nevertheless, the problem when trying to determine the particular form of each of the n components is the apparent arbitrariness and lack of regularity of the layout drawn by their corresponding slabs, which makes it difficult to obtain an explicit closed-form solution for any given μ, q, p, w and n. Especially for large values of n, conducting a general study of the optimal trade-off between privacy and economic reward becomes intractable.

Motivated by all this, our analysis of the solution and the corresponding trade-off focuses on some specific albeit riveting cases of slabs layouts. In particular, Section 3.5 will examine several instantiations of the problem (6) for small values of n. Afterwards, Section 3.6 will tackle the case of large n for some special layouts that will permit us to systematize our theoretical analysis. Fig. 4 shows a configuration of slabs for $n = 6$, and illustrates the conditions that define an optimal disclosure strategy.

3.4. Origin of lower hyperplanes

Despite the arbitrariness of the layout depicted by the slabs associated with a particular instantiation of the problem (6), next we shall be able to derive an interesting property for some specific privacy functions. The property in question is related to the need of establishing a fixed point of reference for the geometry of the solutions space.

Proposition 5 (Intersection of Lower Hyperplanes)**.** *In the nontrivial case when $q \neq p$, if $d_i f_j'(0) = d_j f_i'(0)$ for all $i, j = 1, \ldots, n$ and $i \neq j$, then the hyperplanes $z_i^{\mathrm{T}}\gamma = f_i'(0)$ for $i = 1, \ldots, n$ all intersect at a single point O on the plane α–β.*

Proof. Clearly, the consequent of the statement is true if, and only if, the system of equations $z^{\mathrm{T}}\gamma = \nabla f(0)$ has a unique solution. We proceed by proving that the rank of the coefficient and augmented matrices is equal to 2 under the conditions stated in the proposition.

On the one hand, recall that $z_i = (d_i, w_i)$ is the i-th column of z, and check that its rank is two if, and only if, $d_i w_j \neq d_j w_i$ for some $i, j = 1, \ldots, n$ and $i \neq j$. That said, now we show that the consequent of this biconditional statement is true provided that $q \neq p$. To this end, we assume, by contradiction, that $\operatorname{sgn}(d_1) = \cdots = \operatorname{sgn}(d_n)$, where $\operatorname{sgn}(\cdot)$ is the sign function [8]. If $d_i = q_i - p_i > 0$ for $i = 1, \ldots, n$, we have $1 = \sum q_i > \sum p_i = 1$, a contradiction. The case $d_i < 0$ for all i leads to an analogous contradiction, and the case $d_i = 0$ (for all i) contradicts the fact that $q \neq p$. Hence, the condition $q \neq p$ implies that there must exist some indexes *i, j* with $i \neq j$ such that $\operatorname{sgn}(d_i) \neq \operatorname{sgn}(d_j)$, which in turn implies that $d_i w_j \neq d_j w_i$, and that $\operatorname{rank}(z) = 2$.

On the other hand, to check the rank of the augmented matrix, observe that the determinant of any 3x3 submatrix with rows *i, j, k* yields

$$det\,(z|\nabla f(0)) = w_i\big(d_j f_k'(0) - d_k f_j'(0)\big) + w_j\big(d_i f_k'(0) - d_k f_i'(0)\big) + w_k\big(d_i f_j'(0) - d_j f_i'(0)\big).$$

From this expression, it is easy to verify that $\operatorname{rank}(z|\nabla f(0)) = 2$ if all terms $d_i f_j'(0) - d_j f_i'(0)$ with $i \neq j$ vanish, which ensures, by the Rouché-Capelli theorem [33], that there exists a unique solution to $z^{\mathrm{T}}\gamma = \nabla f(0)$. □

The importance of Proposition 5 is obvious: for some privacy functions and distributions q and p, the existence of a sort of origin of coordinates in the slabs layout may reveal certain regularities which may help us systematize the analysis of the solutions space. For example, a trivial consequence of the intersection of all lower hyperplanes on O is that any γ lying on an bounded polyhedron will lead to a solution with at least one component of the form $f_i'^{-1}(z_i^{\mathrm{T}}\gamma)$ on its interior. When the assumptions of the above proposition does not satisfy, however, this property may not hold for any n and the choice of the origin may not be evident.

In the next subsections, we shall investigate the optimal trade-off between privacy and money for several particular cases. As we shall see, these cases will leverage certain regularities derived from, or as a result of, said reference point on the α–β plane. Before that, however, our next result, Corollary 6, provides such point for each of the three privacy functions considered in our analysis.

Corollary 6. *Consider the nontrivial case when $q \neq p$. The solution to $z^{\mathrm{T}}\gamma = \nabla f(0)$ is unique and yields* $(0, 0)$ *for the squared Euclidean and the Itakura-Saito distances, and* $(1, 0)$ *for the KL divergence.*

Proof. We obtain the result as a direct application of Proposition 5. Note that the gradient of the squared Euclidean and the Itakura-Saito distances vanishes at $\delta = 0$. In the case of the KL divergence, $\nabla f(0) = (d_1, \ldots, d_n)$. Clearly, in the three cases investigated, the condition $d_i f_j'(0) = d_j f_i'(0)$ for all $i \neq j$ in the proposition is satisfied, which implies that the solution is unique. Then, it is immediate to derive the solutions claimed in the statement. □

Although it seems rather obvious, the above corollary actually tells us something of real substance. In particular, for the three privacy functions under study, O does not depend on a user's profile nor the particular initial distribution chosen. This result therefore shows the appropriateness of basing our analysis on such functions.

3.5. Case $\mathrm{n} \leq 3$

We start our analysis of several specific instantiations of the problem (6) for small values of the number of interest categories n. We shall first tackle the case $n = 2$ and afterwards the case $n = 3$.

The special case $n = 2$ reflects a situation in which a user may be willing to group the original set of topics (e.g., business, entertainment, health, religion, sports) into a "sensitive" category (e.g., health, religion) and a "non-sensitive" category (e.g., business, entertainment, sports), and disclose their interests accordingly. Evidently, this grouping would require that the user specify the same rate w_i for all topics belonging to one of these two categories. Our next result, Theorem 7, presents a closed-form solution to the minimization problem involved in the definition of function (1) for this special case. As we shall see now, this result can be derived directly from the primal feasibility conditions.

Theorem 7 (Case $n = 2$,*and SED and KL divergence*). *Let $f : [0, 1] \times [0, 1] \to \mathbb{R}_+$ be continuous on the interior of its domain.*

(i) *For any $\mu \in [0, \mu_{\max}]$ and $i = 1, 2$, the optimal disclosure strategy is $\delta_i^* = \frac{\mu}{\mu_{\max}}$.*
(ii) *In the case of the SED and KL divergence, the corresponding, minimum distance yields the disclosure-money functions*

$$\mathcal{R}_{\mathrm{SED}}(\mu) = 2\left(d_i \frac{\mu}{\mu_{\max}}\right)^2 \text{and}$$

$$\mathcal{R}_{\mathrm{KL}}(\mu) = \sum_{i=1}^{2}\left(d_i \frac{\mu}{\mu_{\max}} + p_i\right)\log\left(\frac{d_i\,\mu/\mu_{\max}}{p_i} + 1\right).$$

Proof. Since $n = 2$, we have that $d_1 = -d_2$, which, by virtue of the primal condition $\sum d_i \delta_i^* = 0$, implies that $\delta_1^* = \delta_2^*$. Then, from the other primal condition $\sum w_i \delta_i^* = \mu$, it is immediate to obtain the solution claimed in assertion (i) of the theorem. Finally, it suffices to substitute the expression of δ^* into the functions $f_{\mathrm{SED}}(\delta_i) = \sum_i (t_i^* - p_i)^2$ and $f_{\mathrm{KL}}(t^*, p) = \sum_i t_i^* \log t_i^*/p_i$, to derive the optimal trade-off function $\mathcal{R}(\mu)$ in each case. □

In light of Theorem 7, we would like to remark the simple, linear form of the solution, which, more importantly, is valid for a set of privacy functions which is larger than that considered in Lemma 4. In particular, not only the KL divergence, the squared Euclidean and the Itakura-Saito distances satisfy the conditions of this theorem, but also many others which are not differentiable (e.g., total variation distance) nor additively separable (e.g., Mahalanobis distance).

Another straightforward consequence of Theorem 7 is that the optimal strategy implies revealing both categories (e.g., sensitive and non-sensitive) simultaneously and with the same level of disclosure. In other words, if a user decides to show a fraction of their interest in one category, that same fraction must be disclosed on the other category so as to attain the maximum level of privacy protection.

Before proceeding with Theorem 8, first we shall introduce what we term *money thresholds*, two rates that will play an important role in the characterization of the solution to the minimization problem (6) for $n = 3$. Also, we shall introduce some definitions that will facilitate the exposition of the aforementioned theorem.

For $i = 1, \ldots, n$, denote by m_i the slope of vector z_i, i.e., $m_i = \frac{w_i}{d_i}$. For convenience, let $\overline{m}_i$ and $\sigma^2_{m_i}$ denote the population mean and variance of all but the i-th slope. When the subindex $i \notin \mathscr{X}$, observe that the mean and variance are computed from all slopes. Accordingly, define the *money thresholds* μ_j as

$$\mu_j = \min_{i \neq 2j} \frac{(j+1)\, d_i\, \sigma^2_{m_{2j}}}{m_i - \overline{m}_{2j}}$$

for $j = 1, 2$.

Additionally, we define the *relative coefficient of variation* of the ratio w_i/d_i as

$$v_{i,j} = \frac{m_i - \overline{m}_j}{\sigma^2_{m_j}} \tag{11}$$

for $i, j = 1, \ldots, n$, which may be regarded as the inverse of the index of dispersion [49], a measure commonly utilized in statistics and probability theory to quantify the dispersion of a probability distribution. As we shall show in the following result, our coefficient of variation will determine the closed-form expression of the optimal disclosure strategy.

Theorem 8 (Case $n = 3$***and SED).*** *For* $n = 3$ *and the SED function, assume without loss of generality* $m_1 \geq m_2 \geq m_3$*. Either* $w_{j+1} \leqslant d_{j+1}\, \overline{m}_{j+1}$ *for* $j = 1$ *and* $m_1 > m_3$*, or* $w_j > d_j\, \overline{m}_j$ *for* $j = 2$*. For the corresponding index j and for any* $\mu \leq \mu_j$*, the optimal disclosure strategy is*

$$\delta_i^* = \begin{cases} \dfrac{v_{i,2j}}{(j+1)d_i}\, \mu, & i \neq 2j \\ 0, & i = 2j \end{cases},$$

and the corresponding, minimum SED yields the disclosure-money function

$$\mathcal{R}_{\mathrm{SED}}(\mu) = \frac{\mu^2}{(j+1)\, \sigma^2_{m_{2j}}}.$$

Proof. The proof is structured as follows. We shall begin by applying Lemma 4 and showing that a solution with only one positive component is infeasible. We shall derive the conditions for a solution to have two nonzero components and, to this end, we shall assume $\delta_2 = 0$. Afterwards, we shall prove that such a solution is possible only under certain conditions. Finally, we shall repeat the two previous steps but for a solution without nonzero components. For simplicity, we omit the subindex SED of the privacy function.

It is straightforward to verify that the SED function exposes the structure of the optimization problem addressed in Lemma 4. Note that, according to the lemma, the components of the solution such that $0 < \delta_i < 1$ for some $i = 1, 2, 3$ are given by the inverse of the privacy function and yield

$$f_i'^{-1}(\alpha d_i + \beta w_i) = \frac{\alpha}{2\, d_i} + \frac{w_i\, \beta}{2\, d_i^2}.$$

To check that a solution does not admit only one positive component, simply observe that the system of equations composed of the two primal equality conditions $\sum_i d_i\, \delta_i = 0$ and $\sum_i w_i \delta_i = \mu$ is inconsistent.

Having shown that there must be at least two positive components, we apply such primal equality conditions to a solution with $0 < \delta_1,\ \delta_3 < 1$. To verify these two equalities are met, first note that the former is equivalent to $\alpha + \beta\, \overline{m}_2 = 0$, and the latter can be written equivalently as

$$\alpha\, \overline{m}_2 + \frac{\beta}{2} \sum_{i=1,3} m_i^2 = \mu.$$

Then, observe that the condition $m_1 > m_3$ in the theorem ensures that the determinant of the homogeneous system is nonzero, and, accordingly, that the Lagrange multipliers that solve these two equations are

$$\alpha = -\frac{\overline{m}_2}{\sigma^2_{m_2}}\mu \text{ and } \beta = \frac{1}{\sigma^2_{m_2}}\, \mu. \tag{12}$$

Finally, it suffices to substitute the expressions of α and β into the function $f_i'^{-1}$, to obtain the solution with two nonzero optimal components claimed in the theorem.

Next, we derive the conditions under which this solution is defined. With this aim, just note that the inequalities $z_1^{\mathrm{T}}\gamma > f_1'(0)$ and $z_3^{\mathrm{T}}\gamma > f_3'(0)$ are equivalent to $d_1(m_1 - \overline{m}_2) > 0$ and $d_3(m_3 - \overline{m}_2) > 0$, respectively. On the other hand, $\delta_2 = 0$ if, and only if, $z_2^{\mathrm{T}}\gamma \leqslant f_2'(0)$, or equivalently, $d_2(m_2 - \overline{m}_2) \leqslant 0$.

We now show that when there are two components $0 < \delta_i,\ \delta_j < 1$, then $i = 1$ and $j = 3$. To this end, we shall examine the case $0 < \delta_2,\ \delta_3 < 1$ and $\delta_1 = 0$. The other possible case, $0 < \delta_1,\ \delta_2 < 1$ and $\delta_3 = 0$, proceeds along the same lines and is omitted.

First, though, we shall verify that $d_1 \geq 0$, a condition that will be used later on. We proceed by contradiction. Since $w_i > 0$ for all i, a negative d_1 implies, by the ordering assumption $m_1 \geq m_2 \geq m_3$, that $d_2,\ d_3 < 0$. But having $d_i < 0$ for $i = 1, 2, 3$ leads us to the contradiction $0 > \sum_i d_i = \sum_i q_i - \sum_i p_i = 0$. Consequently, d_1 is nonnegative, but by virtue of (3), it follows that $d_1 > 0$.

Having verified the positiveness of d_1, next we contemplate the case when $0 < \delta_2,\ \delta_3 < 1$ and $\delta_1 = 0$. Note that, in this case, the condition $\delta_1 = 0$ holds if, and only if, $d_1(m_1 - \overline{m}_1) \leqslant 0$. However, since $d_1 > 0$, we have that

$$m_1 \leqslant \frac{1}{2}(m_2 + m_3),$$

which contradicts the fact that $m_1 \geq m_2 \geq m_3$ and $m_1 > m_3$. Consequently, it is not possible to have $0 < \delta_2,\ \delta_3 < 1$ and $\delta_1 = 0$. The case when $0 < \delta_1,\ \delta_2 < 1$ and $\delta_3 = 0$ leads to another contradiction and thus to the conclusion that $0 < \delta_1,\ \delta_3 < 1$ and $\delta_2 = 0$.

Next, we check the validity of the conditions under which this solution is defined. Recall that these conditions are $d_1(m_1 - \overline{m}_2) > 0$, $d_3(m_3 - \overline{m}_2) > 0$ and $d_2(m_2 - \overline{m}_2) \leqslant 0$. It is easy to verify that the former two inequalities hold, since the arithmetic mean is strictly smaller (greater) than the extreme value m_1 (m_3); the strictness of the inequality is due to the assumption $m_1 > m_3$ in the statement. On the other hand, the latter inequality is the condition assumed in the statement of the theorem. Therefore, we have $0 < \delta_1,\ \delta_3 < 1$ and $\delta_2 = 0$ if, and only if, $w_2 \leqslant d_2\,\overline{m}_2$.

Next, we turn to the case when $0 < \delta_1,\ \delta_2,\ \delta_3 < 1$. By applying the two primal equality constraints of the optimization problem (6), we obtain the system of equations

$$\frac{3}{2}\begin{bmatrix} 1 & \overline{m}_0 \\ \overline{m}_0 & \frac{1}{3}\sum_{i=1}^{3} m_i^2 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 0 \\ \mu \end{bmatrix},$$

and note that the solution is unique on account of the fact that $\operatorname{sgn}(d_i) \neq \operatorname{sgn}(d_j)$ for some $i, j = 1, 2, 3$ and $i \neq j$, which implies that $\sigma_{m_0}^2 > 0$. Substituting the values

$$\alpha = -\frac{2\,\overline{m}_0}{3\,\sigma_{m_0}^2}\mu \text{ and } \beta = \frac{2}{3\,\sigma_{m_0}^2}\,\mu \tag{13}$$

into $f_i'^{-1}(z_i^{\mathrm{T}}\gamma)$ gives the expression of the optimal disclosure strategy stated in the theorem for $0 < \delta_1,\ \delta_2,\ \delta_3 < 1$.

Now, we examine the necessary and sufficient conditions for this optimal strategy to be possible, which, according to the lemma, are $0 < z_i^{\mathrm{T}}\gamma < 2\,d_i$ for $i = 1, 2, 3$. To this end, note that the left-hand inequalities can be recast as $d_i\,(m_i - \overline{m}_0) > 0$, for $i = 1, 2, 3$. We immediately check that the inequalities for $i = 1$ and $i = 3$ hold, as the mean is again strictly smaller (greater) than the extreme value m_1 (m_3). The strictness of these two inequalities is due to the fact that $\sum_{i=1}^{3} d_i = 0$ and the assumption (3). On the other hand, observe that

$$\operatorname{sgn}(m_2 - \overline{m}_0) = \operatorname{sgn}(m_2 - \overline{m}_2),$$

and therefore that the condition $d_2\,(m_2 - \overline{m}_0) > 0$ is equivalent to $d_2\,(m_2 - \overline{m}_2) > 0$. That said, note that $d_2\,(m_2 - \overline{m}_2) > 0$ is the negation of the condition for having a solution with two nonzero components smaller than one. Accordingly, we have either two or three components of this form, as stated in the theorem.

To show the validity of the solution in terms of μ, observe that, for $w_2 \leqslant d_2\,\overline{m}_2$, the parameterized line $(\alpha(\mu),\ \beta(\mu))$ moves within the space determined by the intersection of the slabs 1 and 3. To obtain the range of validity of a solution such that $0 < \delta_1,\ \delta_3 < 1$ and $\delta_2 = 0$, we need to find the closest point of intersection (to the origin) with either the upper hyperplane 1 or the upper hyperplane 3. Put differently, we require finding the minimum μ such that either $z_1^{\mathrm{T}}\gamma = f_1'(1)$ or $z_3^{\mathrm{T}}\gamma = f_3'(1)$. By plugging the values of α and β given in (12) into these two equalities, it is straightforward to derive the money threshold μ_1. We proceed similarly to show the interval of validity $[0,\ \mu_2]$ in the case when $w_2 > d_2\,\overline{m}_2$, bearing in mind that now α and β are given by (13).

To conclude the proof, it remains only to write the disclosure-money function in terms of the optimal apparent distribution, that is, $\mathcal{R}(\mu) = \sum_{i=1}^{n}(t_i - p_i)^2 = \sum_{i=1}^{n} d_i^2\,\delta_i^2$, and from this, it is routine to obtain the expression given at the end of the statement. □

Theorem 8 provides an explicit closed-form solution to the problem of optimal profile disclosure, and characterizes the corresponding trade-off between privacy and money. Although it rests on the assumption that $\mu < \mu_1,\ \mu_2$ and —for the sake of tractability and brevity— tackles only the case of SED, the provided results shed light on the understanding of the behavior of the solution and the trade-off, and enables us to establish interesting connections with concepts from statistics and estimation theory.

In particular, the most significant conclusion that follows from the theorem is the intuitive principle upon which the optimal disclosure strategy operates. On the one hand, in line with the results obtained in Theorem 7, the solution does not admit only one positive component: we must have either two or three active components, and never one alone. On the other hand, and more importantly, the optimal strategy is linear with the relative coefficient of variation of the ratio w_i/d_i, a quantity that is closely related to the index of dispersion, also known as Fano's factor[2].

The solution, however, does not only depend on $v_{i,\,j}$ but also on the difference between the interest value of the actual profile and that of the initial PMF. Essentially, the optimized disclosure works as follows. We consider the category i with the largest value w_i, which in practice may correspond to the most sensitive category. For that given category, if d_i is small and m_i is the ratio that deviates the most from the mean value —relative to the variance—, then the optimal strategy suggests disclosing the profile mostly in that given category. This conforms to intuition since, informally, revealing small differences $q_i - p_i$ when w_i is large may be sufficient to satisfy the broker's demand, i.e., the condition $\sum_i w_i \delta_i = \mu$, and this revelation may not have a significant impact on user privacy[3]. On the other hand, if d_i is comparable to w_i, and m_i is close to the mean value, then the optimal strategy recommends that the user give priority to other categories when unfolding their profile.

Also, from this theorem we deduce that the optimal trade-off depends quadratically on the offered money, exactly as with the case $n = 2$, and inversely on the variance of the ratios m_1, m_2, m_3.

Last but not least, we would like to remark that, although Theorem 8 does not completely[4] characterize the optimal disclosure strategy nor the corresponding trade-off for any q, p, w and μ for $n = 3$, the proof of this result does show how to systematize the analysis of the solution for any instance of those variables. Section 3.7 provides an example that illustrates this point.

3.6. Case n ≥ 3 and conical regular configurations

In this subsection, we analyze the disclosure-money trade-off for large values of n, starting from 3. To systematize this analysis, however, we shall restrict it to a particular configuration of the slabs layout, defined next. Then, Proposition 10 will show an interesting property of this configuration, which will allow us to derive an explicit closed-form expression of both the solution and trade-off for an arbitrarily large number of categories.

Definition 9. For a given q, p, w and $n \geq 3$, let $\mathscr{C}$ be the collection of slabs on the plane α–β that determines the corresponding solution to (6) stated in Lemma 4. Without loss of generality, assume $\frac{1}{m_1} > \cdots > \frac{1}{m_n}$. Define A_i, b_i and b'_i as

$$A_i = \begin{bmatrix} z_i^{\mathrm{T}} \\ z_{i-1}^{\mathrm{T}} \\ z_1^{\mathrm{T}} \end{bmatrix}, b_i = \begin{bmatrix} f'_i(0) \\ f'_{i-1}(1) \\ f'_1(1) \end{bmatrix} \text{and } b'_i = \begin{bmatrix} f'_i(1) \\ f'_{i-1}(1) \\ f'_1(0) \end{bmatrix}.$$

Then, $\mathscr{C}$ is called a *conical regular configuration* if each of the system of equations $A_i\,\gamma = b_i$ and $A_i\,\gamma = b'_i$ for $i = 3, \ldots, n$ has a unique solution.

Proposition 10. *Suppose that there exists a conical regular configuration $\mathscr{C}$ for some q, p, w and n. Denote by $\gamma_{i,j}^{a,b}$ the unique solution to*

$$\begin{cases} z_i^{\mathrm{T}}\,\gamma = f'_i(a) \\ z_j^{\mathrm{T}}\,\gamma = f'_j(b) \end{cases}$$

for $i, j = 1, \ldots, n$ with $i \neq j$, and $a, b \in \{0, 1\}$. Assume $f'_i(0) \neq f'_i(1)$ for all i. Then, except for $\gamma_{1,n}^{1,1}$, $\mathscr{C}$ satisfies

$$z_k^{\mathrm{T}}\,\gamma_{i,j}^{a,b} = f'_k(0) \tag{14}$$

for some $k = 1, \ldots, n$ and all $i \neq j$.

Proof. The existence and uniqueness of $\gamma_{i,j}^{a,b}$ is guaranteed by the fact that $\frac{1}{m_1} > \cdots > \frac{1}{m_n}$. The property stated in the proposition follows from the fact that the systems of equations $A_i\,\gamma = b_i$ and $A_i\,\gamma = b'_i$ for $i = 3, \ldots, n$ have a unique solution.

The systems of equations of the form $A_i\,\gamma = b_i$ ensure that $\gamma_{i,1}^{1,1} = \gamma_{i+1,1}^{0,1}$ for $i = 2, \ldots, n - 1$. Obviously, any $\gamma_{i,j}^{a,b}$ such that $a = 0$ or $b = 0$ with $i \neq j$ satisfies (14) for $k = i$ or $k = j$. Accordingly, we just need to prove the case $a = b = 1$.

Suppose $i > j$. Note that $A_i\,\gamma = b'_i$ implies, on the one hand, that

$$\gamma_{i,i-1}^{1,1} = \gamma_{i-1,1}^{1,0} = \gamma_{i-2,1}^{1,0} = \cdots = \gamma_{j,1}^{1,0},$$

[2] The difference with respect to the Fano factor is that our measure of dispersion inverses the ratio variance to mean, and also reflects the deviation with the particular value attained by a given component. Pearson's coefficient of skewness, another popular measure of dispersion, does not inverse the ratio but is further away from our definition of skewness since it considers the standard deviation and the mode instead of the variance and the instantaneous value m_i, respectively.

[3] Bear in mind that, when using f_{SED} to assess privacy, small values of d_i lead to quadratically smaller values of privacy risk.

[4] That is, for all values of μ.

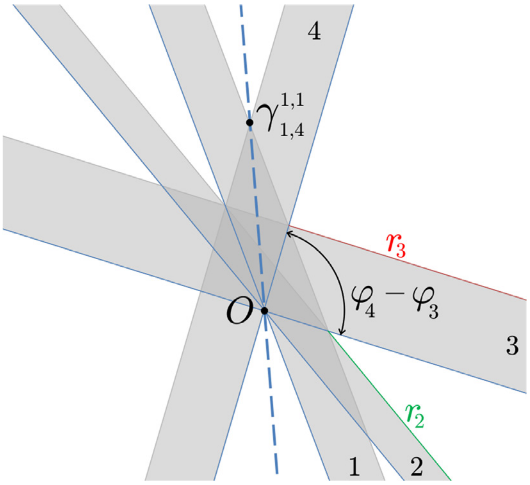


Fig. 5. A conical regular configuration for $n = 4$ on the α–β plane. In this figure, we show the segments of hyperplanes $r_2(\varphi)$ and $r_3(\varphi)$, given respectively by the angular coordinates $\varphi_2 \le \varphi \le \varphi_3$ and $\varphi_3 \le \varphi \le \varphi_4$. The cone defined by $r \ge 0$ and $\varphi_3 \le \varphi \le \varphi_4$ is intersected by the upper hyperplanes 1, 2 and 3. However, neither of these hyperplanes intersect among themselves on the interior of the cone in question.

and on the other hand, that $\gamma^{1,1}_{j,j-1} = \gamma^{1,0}_{j,1}$. Thus, $\gamma^{1,1}_{i,i-1} = \gamma^{1,1}_{j,j-1}$, from which it follows that $\gamma^{1,1}_{i,j} = \gamma^{1,0}_{j,1}$. The exception, i.e., $z_k^{\mathrm{T}} \gamma^{1,1}_{1,n} \neq f'_k(0)$ for all $k = 1, \ldots, n$, is justified by the conditions $f'_i(0) \neq f'_i(1)$ for all i, which guarantee that all slabs have nonempty interiors, and the strict ordering $\frac{1}{m_1} > \cdots > \frac{1}{m_n}$. □

The previous proposition shows a remarkable feature of the conical regular configuration: at a practical level, the fact that all intersections on the plane α–β (except $\gamma^{1,1}_{1,n}$) lie on lower hyperplanes suggests utilizing these hyperplanes, parameterized in polar coordinates with respect to the origin O, to efficiently delimit the solutions space. In other words, in our endeavor to systematize the study of the solution and trade-off, it may suffice to use a reduced number of cases, bounded by angles and segments of hyperplanes.

On the other hand and from a geometric point of view, any consecutive pair of lower hyperplanes defines a cone without intersections in its interior; hence the name of the configuration. Finally, because the slabs are sorted in increasing order of their slopes, we can go counter-clockwise from slab 1 to n, and start again at the line through O and $\gamma^{1,1}_{1,n}$, which serves as a reference axis.

Before we continue examining this concrete configuration, we shall introduce some notation. Let φ and r be the polar coordinates of γ. Define the angle thresholds φ_k as

$$\varphi_k = \begin{cases} \arctan -d_k/w_k, & k = 1, \ldots, n \\ \arctan \frac{d_1 f'_n(1) - d_n f'_1(1)}{w_n f'_1(1) - w_1 f'_n(1)}, & k = n+1 \\ \varphi_{k-n-1} + \pi, & k = n+2, \ldots, 2n+1 \end{cases},$$

and the segments of upper hyperplanes r_j as

$$r_j(\varphi) = \frac{f'_j(1)}{z_j^{\mathrm{T}} \begin{bmatrix} \cos\varphi \\ \sin\varphi \end{bmatrix}}$$

for $j = 1, \ldots, n$. Note that φ_{n+1} is the angular coordinate of $\gamma^{1,1}_{1,n}$. Occasionally, we shall omit the dependence of these line segments on the angular coordinate φ. Fig. 5 illustrates these coordinates and segments on a conical regular configuration for $n = 4$.

Our next result, Lemma 11, provides a parametric solution in the special case when the slabs layout exhibits such configuration. The solution is determined by the aforementioned thresholds and line segments, and is valid for any privacy function satisfying the properties stated in Lemma 4. As we shall show next, this result will be instrumental in proving Theorem 12.

Lemma 11 (Conical Regular Configurations)**.** *Under the conditions of Lemma 4, assume that there exists a conical regular configuration. Consider the following cases:*

(a) *$\varphi_k < \varphi \leqslant \varphi_{k+1}$ for $k = 1$ and, either $r < r_j$ for $j = 1$ or $r_{j-1} \leqslant r$ for $j = 2$; and $\varphi_k < \varphi \leqslant \varphi_{k+1}$ for $k = 2$ and, either $r < r_j$ for $j = 1$, or $r_{j-1} \leqslant r < r_j$ for $j = 2$, or $r \geqslant r_{j-1}$ for $j = 3$.*

(b) *$\varphi_k < \varphi \leqslant \varphi_{k+1}$ for some $k = 3, \ldots, n$ and, either $r < r_{j+1}$ for $j = 1$, or $r_j \leqslant r < r_{j+1}$ for some $j = 2, \ldots, k-2$, or $r_j \leqslant r < r_{j+2 \pmod k}$ for $j = k-1$, or $r_{j+1 \pmod k} \leqslant r < r_j$ for $j = k$, or $r \geqslant r_{j-1}$ for $j = k+1$.*

(c) *$\varphi_k < \varphi < \varphi_{k+1}$ for $k = n+1$ and, either $r < r_{j+1}$ for $j = 1$, or $r_j \leqslant r < r_{j+1}$ for some $j = 2, \ldots, n-1$, or $r_j \le r < r_1$ for $j = n$, or $r \geqslant r_{j-n}$ for $j = n+1$.*

(d) *$\varphi_k \leqslant \varphi < \varphi_{k+1}$ for some $k = n+2, \ldots, 2n$ and, either $r < r_{n-j+1}$ for $j = 1$, or $r_{n-j+2} \leqslant r < r_{n-j+1}$ for some $j = 2, \ldots, 2n-k+1$, or $r \geqslant r_{n-j+2}$ for $j = 2(n+1)-k$.*

Let δ^* be the solution to the optimization problem (6). Accordingly,

(i) *in cases (a) and (b), and for the corresponding indexes k and j,*

$$\delta_i^* = \begin{cases} 0, & i = k+1, \ldots, n \\ f_i'^{-1}\left(z_i^{\mathrm{T}}\gamma\right), & \begin{array}{ll} i = 1 \text{ and } i = j+1, \ldots, k & \text{if } j < k \\ i = j, \ldots, k & \text{if } j = k \end{array} \\ 1, & \begin{array}{ll} i = 2, \ldots, j & \text{if } j < k \\ i = 1, \ldots, j-1 & \text{if } j \geqslant k \end{array} \end{cases};$$

(ii) *in case (c), and for the corresponding indexes k and j, the solution is obtained by exchanging the indexes $i = 1$ and $i = n$ of the solution given for case (b) and $k = n$;*

(iii) *in case (d), and for the corresponding indexes k and j,*

$$\delta_i^* = \begin{cases} 0, & , \quad i = 1, \ldots, k-n-1 \\ f_i'^{-1}\left(z_i^{\mathrm{T}}\gamma\right), & i = k-n, \ldots, n-j+1 \\ 1, & , \quad i = n-j+2, \ldots, n \end{cases}.$$

Proof. From Proposition 10, we have that the conditions $r \ge 0$ and $\varphi_k \leqslant \varphi \leqslant \varphi_{k+1}$ for any single $k = 1, \ldots, n-1, n+2, \ldots, 2n$ yield a cone where no intersection of hyperplanes occurs in its interior. Clearly, we also note that each cone is bounded by two consecutive lower hyperplanes and intersected only by upper hyperplanes. It is easy to verify that the number of intersecting upper hyperplanes is k and $2n-k+1$, respectively for $k = 1, \ldots, n$ and $k = n+2, \ldots, 2n$.

That said, all cases stated in the lemma are an immediate consequence of Lemma 4. We only show statement (iii). With this aim, observe that, for any $k = n+2, \ldots, 2n$, the condition $\varphi_k \leqslant \varphi < \varphi_{k+1}$ is equivalent to $\varphi_{k-n-1} \leqslant \varphi + \pi < \varphi_{k-n}$, which means that, for a given k, the corresponding cone is bounded by the lower hyperplanes $k-n-1$ and $k-n$ and thus

$$z_{k-n-1}^{\mathrm{T}} \begin{bmatrix} r\cos\varphi \\ r\sin\varphi \end{bmatrix} \leqslant f_{k-n-1}'(0).$$

Since a conical regular configuration satisfies $\frac{1}{m_1} > \cdots > \frac{1}{m_n}$, then

$$f_1'^{-1}\left(z_1^{\mathrm{T}}\gamma\right), \ldots, f_{k-n-1}'^{-1}\left(z_{k-n-1}^{\mathrm{T}}\gamma\right) \leqslant 0, \tag{15}$$

and accordingly $\delta_1 = \cdots = \delta_{k-n-1} = 0$.

On the other hand, for a given $\varphi \in [\varphi_k, \varphi_{k+1}]$, note that the parameterized line $(r\cos\varphi,\ r\sin\varphi)$ intersects the sequence of line segments $r_n, r_{n-1}, \ldots, r_{k-n}$ when r goes from 0 to ∞. This shows the order of the line segments specified in case (d).

Having checked this, note that when $r_{n-j+2} \leqslant r < r_{n-j+1}$ for some $j = 2, \ldots, 2n-k+1$, we have

$$f_{n-j+2}'^{-1}\left(z_{n-j+2}^{\mathrm{T}}\gamma\right), \ldots, f_n'^{-1}\left(z_n^{\mathrm{T}}\gamma\right) \geqslant 1,$$

and thus $\delta_{n-j+2} = \cdots = \delta_n = 1$. From (15), it follows that $\delta_i = 0$ for $i = 1, \ldots, k-n-1$, and then that the rest of the components $i = k-n, \ldots, n-j+1$ must be of the form $f_i'^{-1}\left(z_i^{\mathrm{T}}\gamma\right)$. □

Our previous result, Lemma 11, shows that the specific arrangement of the lower and upper hyperplanes of a conical regular configuration makes polar coordinates particularly convenient for analyzing the solution to the optimization problem at hand. The lemma takes advantage of the regular structure of such configuration, and is used in Theorem 12 as a stepping stone to derive an explicit closed-form solution for $n \ge 3$. To be able to state our next result concisely, we introduce some auxiliary definitions.

Denote by $D_i = \sum_{k=i}^n d_k$ and $W_i = \sum_{k=i}^n w_k$ the complementary cumulative functions of d and w. For $k = n+2, \ldots, 2n$ and $j = 1, \ldots, 2(n+1)-k$, define the set $\mathcal{S}(k, j) = \{1, \ldots, k-n-1, n-j+2, \ldots, n\}$. In line with the definition given for case $n \le 3$ in Section 3.5, denote by $\overline{m}_{S(k,j)}$ and $\sigma^2_{m_{S(k,j)}}$ the arithmetic mean and variance of the sequence $(m_i)_{i \in \mathscr{X} \setminus \mathcal{S}(k,j)}$. Similarly to Section 3.5, we define a sequence of *money thresholds*

$$\mu_{k,j} = W_{n-j+2} - D_{n-j+2}\left(\overline{m}_{S(k,j)} + \frac{\sigma^2_{m_{S(k,j)}}}{\overline{m}_{S(k,j)} - m_{k-n-1}}\right),$$

for $k = n+2, \ldots, 2n$ and $j = 1, \ldots, 2(n+1)-k$.

Theorem 12. *Assume that there exists a conical regular configuration for some q, p, w and n. For any $k = n+2, \ldots, 2n$ and $j = 1, \ldots, 2(n+1) - k$ such that $\mu_{k+1,j} < \mu_{k,j}$, and for any $\mu \in (\mu_{k+1,j}, \mu_{k,j}]$, the optimal disclosure strategy for the SED function is $\delta_i^* = 0$ for $i = 1, \ldots, k-n-1$,*

$$\delta_i^* = \frac{1}{d_i\,(n - |S(k,j)|)}\Big(v_{i,S(k,j)}\big(\mu - W_{n-j+2} + D_{n-j+2}\,\overline{m}_{S(k,j)}\big) - D_{n-j+2}\Big)$$

for $i = k-n, \ldots, n-j+1$, and $\delta_i^* = 1$ for $n-j+2, \ldots, n$.

Proof. The proof parallels that of Theorem 8 and we sketch the essential points.

Observe that the range of values of the indexes k and j stated in the theorem corresponds to case (d) of Lemma 11. The direct application of this lemma in the special case of the SED function leads to the solution $\delta_i = \frac{\alpha}{2\,d_i} + \frac{w_i\,\beta}{2\,d_i^2}$ for $i = k-n, \ldots, n-j+1$, $\delta_i = 1$ for $i = n-j+2, \ldots, n$, and $\delta_i = 0$ for $i = 1, \ldots, k-n-1$.

The system of equations given by $\sum_i d_i \delta_i = 0$ and $\sum_i w_i \delta_i = \mu$ has a unique solution by dint of the fact that $D_1 = 0$ and $d_i \neq 0$ for all $i = 1, \ldots, n$. Routine calculation gives

$$\alpha = -\,\overline{m}_{S(k,j)}\,\beta + \frac{2\,D_{n-j+2}}{|S(k,j)| - n},$$

$$\beta = \frac{2\big(\mu - W_{n-j+2} + D_{n-j+2}\,\overline{m}_{S(k,j)}\big)}{(n - |S(k,j)|)\sigma^2_{m_{S(k,j)}}}.$$

By plugging these expressions into $\frac{\alpha}{2\,d_i} + \frac{w_i\,\beta}{2\,d_i^2}$, we derive the components $i = k-n, \ldots, n-j+1$ of the solution.

It remains to confirm the interval of values of μ in which this solution is defined. For this purpose, verify first that $\varphi = \arctan(\beta/\alpha)$ is a strictly monotonic function of μ. Then, note that the condition $\varphi_k \leq \varphi$ in Lemma 11, case (d), becomes

$$-\frac{1}{m_{k-n+1}} \leqslant -\frac{1}{\overline{m}_{S(k,j)}} + \frac{D_{n-j+2}}{\overline{m}_{S(k,j)}} \times \left(\frac{\overline{m}_{S(k,j)}}{\sigma^2_{m_{S(k,j)}}}\big(\mu - W_{n-j+2} + D_{n-j+2}\,\overline{m}_{S(k,j)}\big) + D_{n-j+2}\right)^{-1}$$

After simple algebraic manipulation, and on account of $\mu_{k+1,j} < \mu_{k,j}$ and the monotonicity of $\varphi(\mu)$, we conclude

$$\mu \leqslant W_{n-j+2} - D_{n-j+2}\left(\overline{m}_{S(k,j)} + \frac{\sigma^2_{m_{S(k,j)}}}{\overline{m}_{S(k,j)} - m_{k-n-1}}\right).$$

An analogous analysis on the upper bound condition $\varphi < \varphi_{k+1}$ determines the interval of values of μ where the solution is defined. □

Although the above theorem only covers the intervals $\mu_{k+1,j} < \mu_{k,j}$ for $k = n+2, \ldots, 2n$ and $j = 1, \ldots, 2(n+1) - k$, a number of important, intuitive consequences can be drawn from it. First and foremost, the components δ_i of the form $f_i'^{-1}(z_i^{\mathrm{T}}\gamma)$ are linear with the ratio $\frac{v_{i,S(k,j)}}{d_i}$, exactly as Theorem 8 showed for $n = 3$, which means that the optimal strategy follows the same intuitive principle described in Section 3.5. On the other hand, the coincidence of these two results suggests a similar behavior of the solution in a general case.

Another immediate consequence of Theorem 12 is the role of the money thresholds. In particular, we identify $\mu_{k,\,j}$ as the money (paid by a data broker) beyond which the components of δ_i for $i = k-n, \ldots, n$ are all positive. Conceptually, we may establish an interesting connection between these thresholds and the hyperplanes that determine the solutions space on the α–β plane. Lastly, although it has not been proved by Theorem 12, we immediately check the quadratic dependence of the trade-off function on μ, as shown also in Theorem 8 for $n = 3$.

3.7. Simple, conceptual example

In this section, we present a numerical example that illustrates the theoretical analysis conducted in the previous subsections. For simplicity, we shall assume the SED as privacy function.

In this example, we consider a user who wishes to sell their Google search profile to one of the new data-broker companies mentioned in Section 1. We represent their profile across $n = 3$ categories, namely, “health”, “others” and “religion”, as we assume they are concerned mainly with those search categories related to health and religion, whereas the rest of searches are not sensitive to them. We suppose that the user’s search profile is

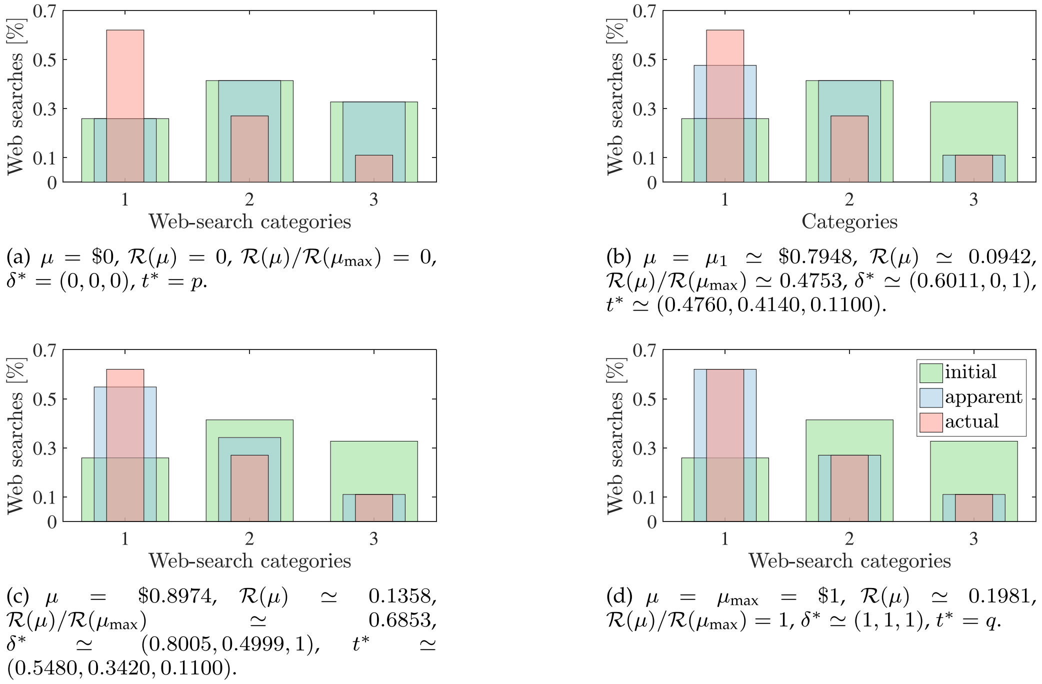
$$q = (0.620, 0.270, 0.110),$$

the initial distribution is

$$p = (0.259, 0.414, 0.327),$$

and the normalized category rates are

$$w = (0.404, 0.044, 0.552).$$



(a) $\mu = \$0$, $\mathcal{R}(\mu) = 0$, $\mathcal{R}(\mu)/\mathcal{R}(\mu_{\max}) = 0$, $\delta^* = (0, 0, 0)$, $t^* = p$.

(b) $\mu = \mu_1 \simeq \$0.7948$, $\mathcal{R}(\mu) \simeq 0.0942$, $\mathcal{R}(\mu)/\mathcal{R}(\mu_{\max}) \simeq 0.4753$, $\delta^* \simeq (0.6011, 0, 1)$, $t^* \simeq (0.4760, 0.4140, 0.1100)$.

(c) $\mu = \$0.8974$, $\mathcal{R}(\mu) \simeq 0.1358$, $\mathcal{R}(\mu)/\mathcal{R}(\mu_{\max}) \simeq 0.6853$, $\delta^* \simeq (0.8005, 0.4999, 1)$, $t^* \simeq (0.5480, 0.3420, 0.1100)$.

(d) $\mu = \mu_{\max} = \$1$, $\mathcal{R}(\mu) \simeq 0.1981$, $\mathcal{R}(\mu)/\mathcal{R}(\mu_{\max}) = 1$, $\delta^* \simeq (1, 1, 1)$, $t^* = q$.

Fig. 6. Actual, initial and apparent profiles of a particular user for different values of μ.

The choice of the initial profile and the category rates above may be interpreted from the perspective of a user who hypothetically wants to hide an excessive interest in health-related issues and, more importantly to them, wishes to conceal a lack of interest in religious topics. This is captured by the large differences between q_1 and p_1 on the one hand, and q_3 and p_3 on the other, and by the fact that $w_3 > w_1$.

First, we note that q and p satisfy the assumptions (2) and (3), and that $m_1 \geq m_2 \geq m_3$. Also, we verify that $w_2 \leqslant d_2 \overline{m}_2$, which, on account of Theorem 8, implies that the optimal disclosure strategy has just two positive components within the interval $\mu \in [0, \mu_1]$, in particular, the categories 1 and 3. Precisely, from Section 3.5, we easily obtain this money threshold $\mu_1 \simeq$ \$0.7948.

From Theorem 8, we also know that the optimal percentage of disclosure is proportional to the relative coefficient of variation of the ratio w_i/d_i, which in our example yields

$$\left(\frac{v_{i,2}}{d_i}\right)_i \simeq (1.513, -0.842, 2.516).$$

Accordingly, for $\mu \in [0, \mu_1]$ we expect higher disclosures for category 3, “religion”, than for category 1, “health”. This is illustrated in Fig. 6(b), where we plot the actual, initial and apparent profiles for the extreme case $\mu = \mu_1$. In this figure, we observe that the optimal strategy suggests revealing the user’s actual interest completely in category 3. For that economic reward, which accounts for roughly 79.48% of $\mu_{\max}$, interestingly the user sees how their privacy is reduced “just” 47.53%. Remarkably enough, this unbalanced yet desirable effect is even more pronounced for smaller rewards. For instance, for $\mu =$\$0.01, we note that the increase in privacy risk is only 0.0015% of the final privacy risk $\mathcal{R}(\mu_{\max}) \simeq 0.1981$.

Recall that γ is the parameter that configures the specific point of operation within the α–β plane in Lemma 4, and thus the specific form (i.e., either 0, 1 or $f_i'^{-1}(z_i^{\mathrm{T}}\gamma)$) of each of the components of the optimal disclosure strategy. In the interval of values $[0, \mu_1]$, the parameter γ lies in the closure of halfspaces 1 and 3, as we show in Fig. 7. An interesting observation that arises from this figure is, precisely, the correspondence between this parameter and μ, and how the latter (obviously together with q, p and w) determines the former through the primal equality conditions $\sum_i d_i \delta_i = 0$ and $\sum_i w_i \delta_i = \mu$. In particular, we observe that as μ increases, γ draws a straight line from the lower hyperplane 3 to the upper hyperplane 3, which helps us illustrate how economic rewards are mapped to the α–β plane. In addition, because we contemplate the SED function as privacy measure, we appreciate that the three lower hyperplanes intersect at (0, 0), as stated in Corollary 6.

To compute the solution to (1) for $\mu > \mu_1$, we follow the methodology of the proof of Theorem 8. With this aim, we first check that the only condition consistent with $\mu_1 < \mu < \mu_{\max}$ is that $0 < \delta_1$, $\delta_2 < 1$ and $\delta_3 = 1$. We verify this by noting that, when $\delta_2 = 0$, the system of equations given by the above two primal equality conditions is inconsistent. Then, we notice

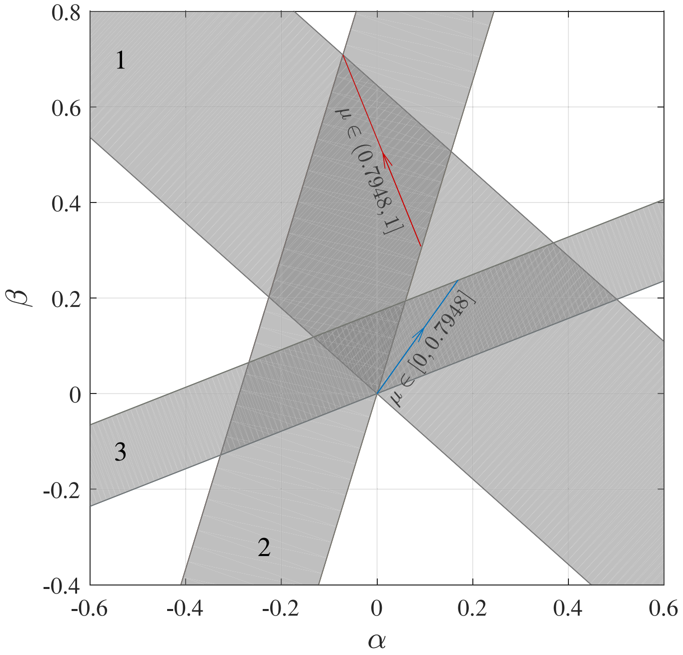


Fig. 7. Slabs layout on the α–β plane for the example considered in Section 3.7. The line segments plotted in blue and red show the dependence of the parameter γ on μ. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

that, if $0 < \delta_2 < 1$, these two conditions lead to the following system of equations,

$$\begin{bmatrix} 1 & \overline{m}_3 \\ \overline{m}_3 & \frac{1}{2}\sum_{i=1}^{2} m_i^2 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} -d_3 \\ \mu - w_3 \end{bmatrix},$$

which has a unique solution,

$$(\alpha, \beta) \simeq (-0.8017\,\mu + 0.7303,\ 1.9708\,\mu - 1.2619).$$

From this solution, it is immediate to obtain the optimal strategy $\delta_1^*(\mu) \simeq 1.9444\,\mu - 0.9445$ and $\delta_2^*(\mu) \simeq 4.8746\,\mu - 3.8746$. Following an analogous procedure, we find that its interval of validity is $(\mu_1, \mu_{\max}]$, where we note that $\mu_{\max}$ =\$1, owing to the fact that the category rates $(w_i)_{i=1}^3$ have been normalized for the sake of illustration.

From the expressions of δ_1 and δ_2 above, we observe that the optimal strategy reveals the actual interest values of both categories only when $\mu = \mu_{\max}$, in which case $t = q$. This is plotted in Fig. 6(d). An intermediate value of μ is assumed in Fig. 6(c) that allows us to show the distinct rates of disclosure for the category 1 between the cases $\mu \in [0, \mu_1]$ and $\mu \in (\mu_1, 1]$. In particular, the rate of profile disclosure is 0.7560 for the former interval, whereas the optimal strategy recommends a significantly larger rate for the latter interval (1.9444). The interval of operation $(\mu_1, 1]$, on the other hand, places γ on the intersection between slabs 1 and 2. Fig. 7 shows this and how γ approaches to the intersection between the upper hyperplanes 1 and 2 as μ gets close to \$1.

Finally, Fig. 8 depicts the disclosure-money function $\mathcal{R}(\mu)$, which characterizes the optimal exchange of money for privacy for the user in question. The results have been computed theoretically, as indicated above, and numerically[5], and confirm the monotonicity and convexity of the optimal trade-off, proved in Theorems 1 and 3.

4. Evaluation

Next, we conduct an extensive empirical evaluation of the mechanism investigated theoretically in the previous section. This experimental evaluation will explore a variety of aspects, ranging from the probability distributions of the money thresholds and the relative coefficients of variation of w_i/d_i, to the level of privacy lost and the amount of money gained when users sell brokers access to two kinds of personal accounts. In particular, the experiments will examine the case when brokers offer users money for accessing their banking accounts and their data at Foursquare[6]. With these experiments, we aim to demonstrate the technical feasibility of our mechanism and the benefits it would bring to users of Datacoup, CitizenMe, DataWallet and the like.

[5] The numerical method chosen is the interior-point optimization algorithm [10] implemented by the Matlab R2016a function `fmincon`.

[6] The type of data used in this empirical evaluation are fully in line with the user data which Datacoup and similar broker companies are disposed to purchase.

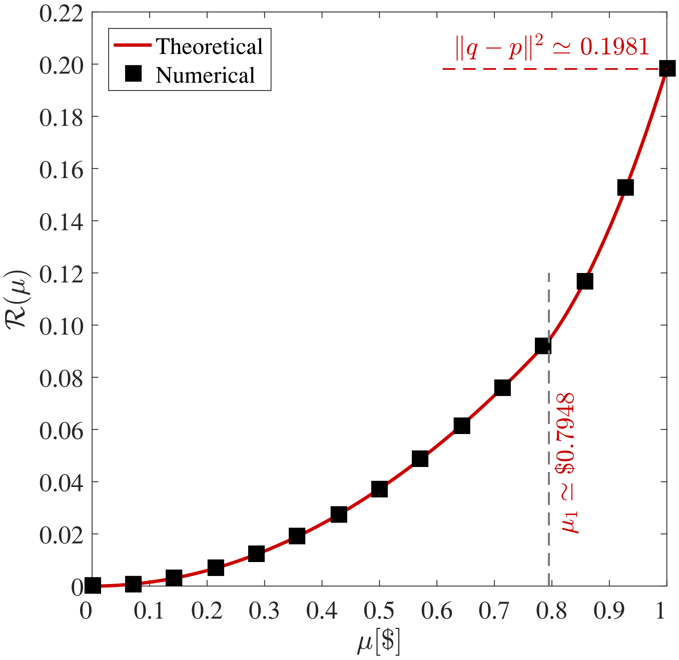


Fig. 8. Optimal trade-off between privacy and money, the former measured as the SED between the apparent and the initial profiles.

4.1. Data sets

The experimental evaluation has been conducted on the basis of two data sets. These represent real examples of user data the new brokers companies are interested in:

- the data set [55], which contains check-in information of the social network Foursquare[7];
- and the “Purchase Card Fiscal Year2015// data set [2], with information on the purchases made by public employees through the purchase card programs administered by the State of Oklahoma, U.S.

The former data set is composed of 227 428 check-ins (i.e., visits to a venue) logged in New York City from April 2012 to February 2013, and 1 083 users. The data is organized in the form of records, each one representing the visit of a user to a venue category (e.g., museum, library or medical center[8]. In an attempt to anonymize the data, [55] replaced usernames with numbers.

In our experiments, we removed those venues appearing lower than 2 000 times, which gave us a granularity level sufficiently aggregated as to avoid having user profiles with many empty categories. Also, we discarded those users with less than 100 check-ins. As a result of this preprocessing, the number of venue types and users reduced to 27 and 507, respectively. Fig 11 shows the categories used in our experiments with Foursquare.

The latter data set, on the other hand, contains 427 921 logs of the form (*user ID, purchase value*) and 3 906 users. We decided to divide the domain of the second attribute into three intervals: (0, 55.34], (55.34, 243.64], (243.64, 10 000]. The thresholds \$55.34 and \$243.64 were chosen to be the 33th and 66th percentile values. Similarly, we dropped users with an activity level lower than 100 purchases, since it would have been difficult to calculate a reliable estimate of their profiles with such a few transactions. Accordingly, the number of logs and users became 338 172 and 1 062 respectively.

Table 2
Overview of the data sets used in our experiments.

	Logs	Users	Data categories
Foursquare	105 384	507	27
Purchase Card	338 172	1 062	3

[7] https://foursquare.com

[8] The complete list of such categories is available at https://developer.foursquare.com/categorytree.)

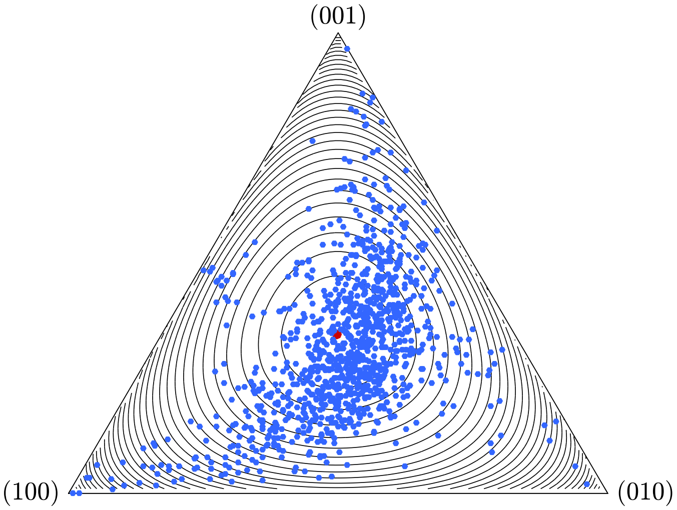


Fig. 9. Distribution of profiles over the simplex of probability in the Purchase Card data set, and average profile of the population $\bar{p}$ (in red). (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

4.2. Privacy models

To show the viability of our mechanism, we evaluate it for the two privacy models described in Section 2.3, individuation and classification. Accordingly, we consider the case when all users choose the former and wish their initial profiles to exhibit typical interests; and the case when these same users prefer a classification approach.

In the individuation scenario, we assume the KL divergence as privacy function. The KL divergence has been extensively used as a privacy metric [42,43] and as a classifier in image recognition, machine learning and in information security. Although the KL divergence is not a distance function, it provides a measure of discrepancy between distributions and may be construed as an indicator of the likelihood of a distribution within a population [31]. This latter property is consistent with the assumed individuation model, where we consider the attacker seeks users who deviate from the average profile of interests.

In the classification scenario, on the other hand, we rely on the SED function to quantify privacy risk. The SED function is not a proper metric, either. However, it has been used in a variety of fields, including data privacy [26] and statistics.

Regardless of the two privacy models assumed, our mechanism requires the definition of an initial profile for each user. In the individuation model, we assume all users select p as the average profile of the population $\bar{p}$. In the classification privacy, however, we first applied Lloyd's algorithm [37] to create 10 groups of users. This number of groups was chosen to achieve a level of granularity sufficiently large and thus avoid clusters with few profiles. According to this clustering, we consider a worst-case scenario for each user wishing to be classified into a different group, and assume the initial profile of each user is the centroid of the most distant group.

Fig. 9 shows the distribution of user profiles in the probability simplex for the Purchase Card data set. In this figure, we also represent the average profile and the contours of KL divergence between a point in the simplex and the average distribution $\bar{p}$, that is, $f_{\mathrm{KL}}(\cdot, \bar{p})$. On the other hand, Fig. 10 provides the number of users per cluster in the Foursquare data set, and Fig. 11 shows the centroid of the largest cluster as an example of user profile in this data set.

4.3. Category rates

In addition to an initial profile, our mechanism requires a tuple w of category rates. Recall that w_i is the amount of money a user would need to disclose their complete activity in the category i.

In the absence of a probability distribution model for those weights, we estimate them through the sensitivity of the data categories. In the Foursquare data set, we choose the categories “home”, “medical center”, “neighborhood” and “office” as sensitive and, accordingly, assume all users assign a same weight w_{s} to these sensitive categories, and a same weight to their other, non-sensitive ones. In these experiments, we consider $w_{\mathrm{s}} = 3\,w_{\mathrm{ns}}$ for all users. We hasten to stress, however, that each user would in principle be offered a different compensation in real practice.

We proceed similarly with the Purchase Card data set and assume that those categories including larger purchase values are more sensitive. Based on this criterion, we suppose $w_2 = 2w_1$ and $w_3 = 3w_1$ for all users. It is worth emphasizing that, in our experiments, we shall use a normalized reward $\bar{\mu} = \frac{\mu}{\mu_{\max}}$ to make our results independent of the particular values w_{ns} and w_1 might take on.

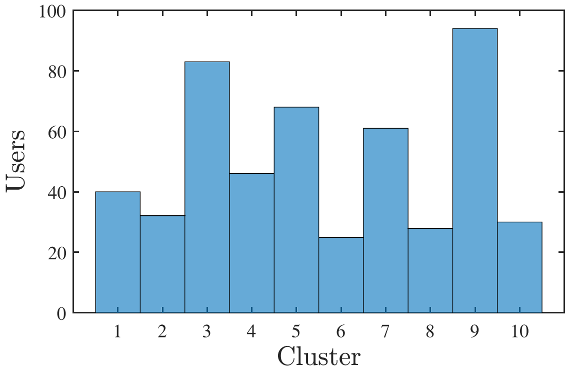


Fig. 10. Number of users per cluster in the Foursquare data set.

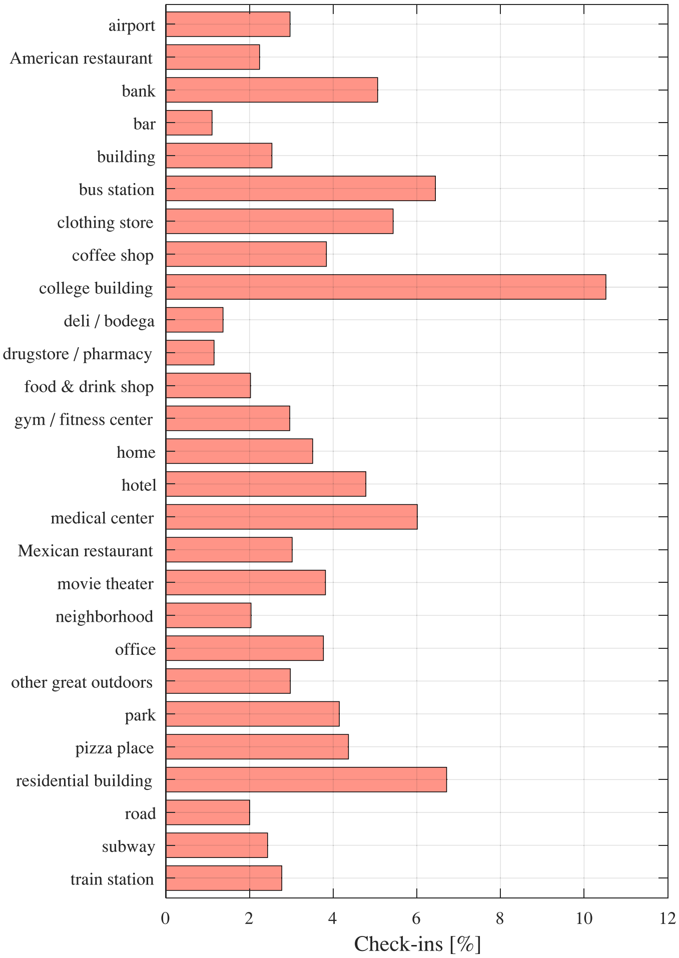


Fig. 11. Centroid of the largest group in the Foursquare data set.

4.4. Results

In our analysis of the disclosure-money trade-off for $n = 3$ in Section 3, we showed that the set of optimal disclosure strategies δ^* can be divided into two subsets: one where there exists a money threshold $\mu > 0$ below which δ^* has two positive components; and another subset where such threshold does not exist and all components are positive. We denoted the threshold of the former subset by μ_1. For the latter subset of optimal strategies, we also showed the existence of a money threshold μ_2 beyond which one of the components of δ^* is 1.

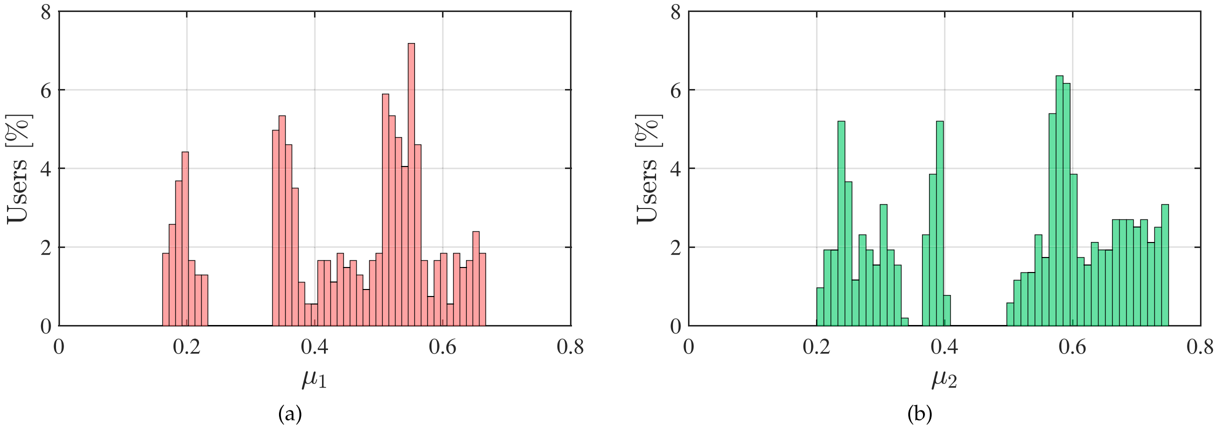


Fig. 12. Probability distributions of the money thresholds μ_1 and μ_2 in the Purchase Card data set.

In our first experiments, we examine the distribution of such thresholds in the Purchase Card data set with the aim of shedding some light on the form of the optimal strategy for a relatively large number of users. First, we note that the probability of having only two positive components is 51.13% —and thus the probability that all components be positive is 48.87%. In Fig. 12 we show those distributions and observe that the minimum, mean and maximum values are 0.1673, 0.4424 and 0.6633 for μ_1, and 0.2065, 0.4988 and 0.7483 for μ_2. In the case of the former threshold, these results indicate that, on average and for a compensation slightly smaller than half of $\mu_{\max}$, the optimal strategy only needs to disclose the two of the three categories by a percentage $\delta_i < 1$ to minimize privacy risk. Said otherwise, most users will not be required to reveal any percentage of purchasing activity in one of the money intervals for $\bar{\mu}$ smaller than 0.4424. An analogous, although conceptually different, conclusion can be drawn for μ_2. In particular, we appreciate that most users will experience the first complete disclosure of a purchasing category for roughly half of the reward they would accept for fully showing their actual profiles.

The relevance of the preliminary results above lies in that a quarter of our users would be able to earn $\mu \approx \mu_{\max}/2$, while leaving one-third of their profile fully obfuscated and hence disclosing two-thirds of it —although only partially; later on we shall see this balance will be tip more in favor of privacy, in the sense that much less disclosure will be required for compensations on that range. Our next result dives into the particular form of the obfuscated profile by exploring the probability distribution of the relative coefficient of variation $v_{i,\,j}$. As explained in Section 3, this coefficient plays a crucial role since the level of disclosure recommended by the optimal strategy is proportional to it.

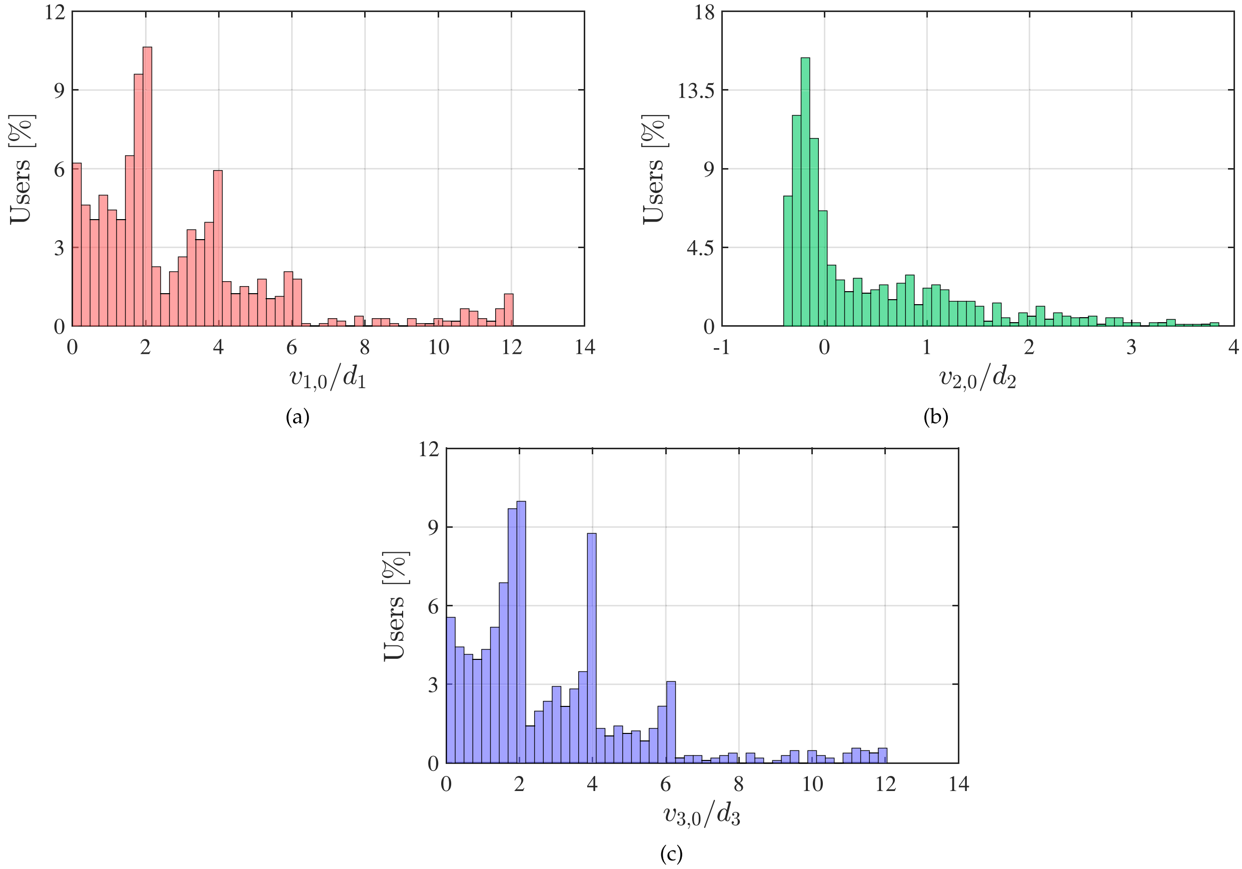
Fig. 13 plots the PMFs of the three components of this coefficient, which average 2.8756, 0.4118 and 2.9039. Several conclusions can be drawn from this figure. First and foremost, these mean values point out that the disclosure of purchasing habits is more frequent in the money intervals (0, 55.34] and (243.64, 10 000], than in the interval (55.34, 243.64]. From Fig. 13(b) we also note that 24.29% of users have a negative coefficient of variation. Because $v_{1,\,0}$ and $v_{3,\,0}$ were observed to be positive, a negative $v_{2,\,0}$ implies these users will not reveal their habits beyond the initial profile p_2, which appears to be in line with the observation that a quarter of the population would need to disclose up to two-thirds of their profile to get compensations of up to $\mu \approx \mu_{\max}/2$.

Figs. 13(a) and (c) show, on the other hand, a number of users with relatively large values of the coefficient of variation in the categories 1 and 3, which means that the optimal strategy will recommend them to disclose essentially the real value of their purchases in those categories. Not entirely unexpectedly, we notice this occurs for users with high (relative) activity in those categories.

Next, we turn to the Foursquare data set to examine the behavior of the optimal disclosure strategy for $\bar{\mu}$ close to 0. We are interested in this particular case as it may represent a frequent point of operation within the privacy-money trade-off, especially at the beginning of the technology adoption life cycle, where data purchasers might bid low prices. Under this assumption, we wonder how many components of their profile would be disclosed. Fig. 14 shows the probability distribution of the number of active components of δ^* for $\bar{\mu} = 1/25$. The minimum, mean and maximum values are 8, 23.03 and 27 respectively, which seems to reflect a behavior similar to the one observed for the Purchase Card data set: in this latter case, although the number of categories was 3, we noticed that roughly half of the population had 2 active components, whereas the rest had 3.

In our next series of experiments, we evaluate the extent to which our approach may help users protect their profiles while making money out of them.

We begin by examining the privacy risk that users in our data sets would experience when brokers offered them the maximum reward. Figs. 15(a) and (b) illustrate the PMFs of such final privacy risk, i.e., the distributions of the values of $f_{\mathrm{SED}}(t,\,p)$ and $f_{\mathrm{KL}}(t,\,p)$, where p is the average profile in the Purchase Card data set and the centroid of the most distant cluster in Foursquare. We observe that the minimum, mean and maximum values are respectively 0.0004, 0.1411 and 1.4572



(a)

(b)

(c)

Fig. 13. PMF of the relative coefficient of variation of the ratio w_i/d_i for $i = 1, 2, 3$ in the Purchase Card data set.

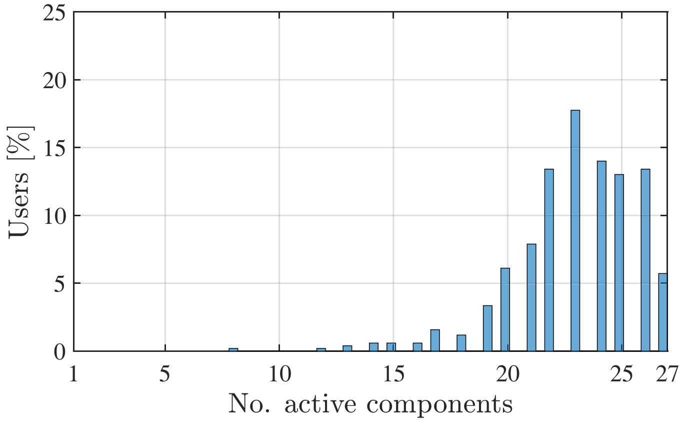


Fig. 14. Probability distribution of the number of active components of δ^* for $\bar{\mu} \simeq 0$ in the Foursquare data set.

bits for the former data set, and 0.0084, 0.0880 and 0.9254 for the latter. The main conclusion that can be drawn from these two figures is the difference in the number of users with zero, or near zero, final privacy risk. However, the fact that around 24% of users in the Purchase Card data set have less than 0.04 bits of privacy risk —whereas for that same privacy there are just 3% of users in Foursquare—, should come as no surprise since our experiments assume a different privacy model for each data set: while all users in the individuation model share a same initial profile (which might be close to their actual profile), the classification model forces users to choose the centroid which is farthest away from their cluster.

Our second set of experiments aims to analyze, for $\mu < \mu_{\max}$, the level of privacy lost in relation to the compensation offered by data brokers. To this end, recall that we assume a scenario where all users are rewarded a same $\bar{\mu}$. Under this assumption, Fig. 16 plots the relative privacy risk for the Purchase Card and Foursquare data sets, where we considered in-

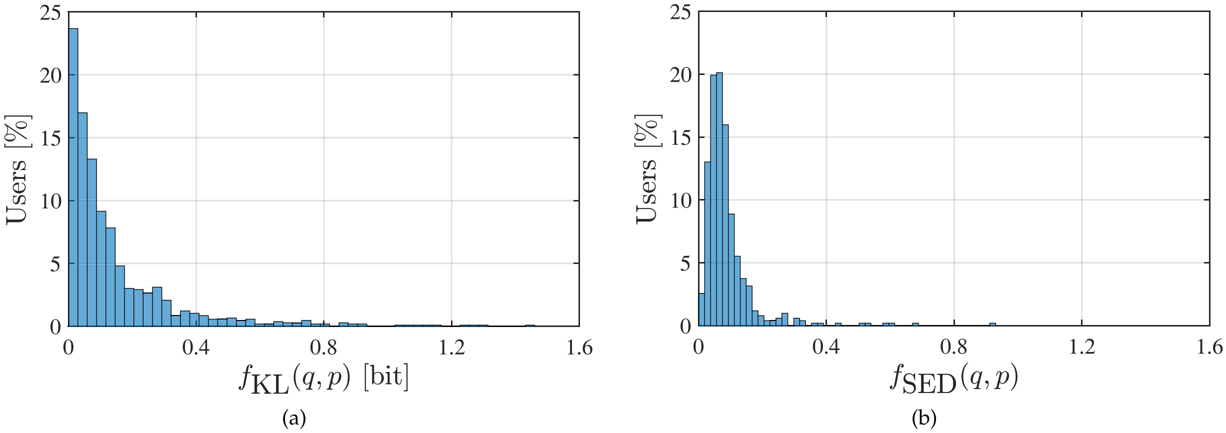


Fig. 15. PMF of the final privacy risk in the Purchase Card (a) and Foursquare (b) data sets.

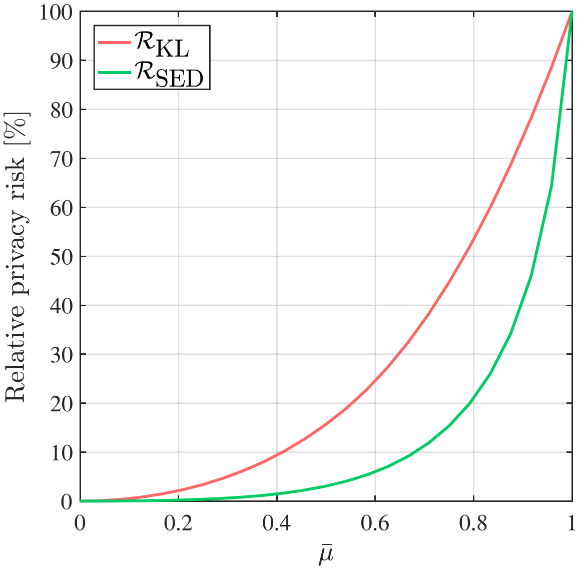


Fig. 16. Average relative privacy risk for different values of $\bar{\mu}$ in the Purchase Card and Foursquare data sets.

dividuation and classification as privacy models, respectively. The most relevant observation is that, for both privacy models, the average relative privacy risk is smaller than $\bar{\mu}$, which means that any given reward leads, on average, to an increase in relative privacy risk which does not exceed that reward. More specifically, we notice in the Purchase Card data set that the average user would obtain 60% of $\mu_{\max}$ for losing only 25% of their privacy. In the Foursquare data set, this effect is even more exacerbated: for that same reward, users would on average reduce their privacy by just 6.382%. In short, what these results point out is that the compensation offered to users far outweighs the average reduction in privacy risk.

Fig. 17 shows the protection achieved by these users in terms of percentile curves (10^{th}, 50^{th} and 90^{th}) of relative privacy risk. Two conclusions follow from this figure.

- First, for small to medium values of $\bar{\mu}$ (less than 40%), a vast majority of users exhibited a relatively low reduction in privacy risk. In quantitative terms, we observe in Fig. 17(a) that, for $\bar{\mu} = 0.4$, the 90% of users adhered to our mechanism obtained levels of relative privacy risk less than 15.72%. In the Foursquare data set (Fig. 17(b)), the 90^{th} percentile for that compensation value is just 3.13%.
- Secondly, the increase in relative privacy risk is relatively moderate for $\bar{\mu} < 0.5$ in the Purchase Card data set and $\bar{\mu} < 0.8$ in the Foursquare data set. In the former data set, we note that a reward of $\bar{\mu} = 0.5$ makes 90% of users experience a reduction in privacy risk of up to 63.04%, while in the latter data set, a $\bar{\mu} = 0.8$ leads this same fraction of the population to levels of relative privacy risk smaller than 32.87%.

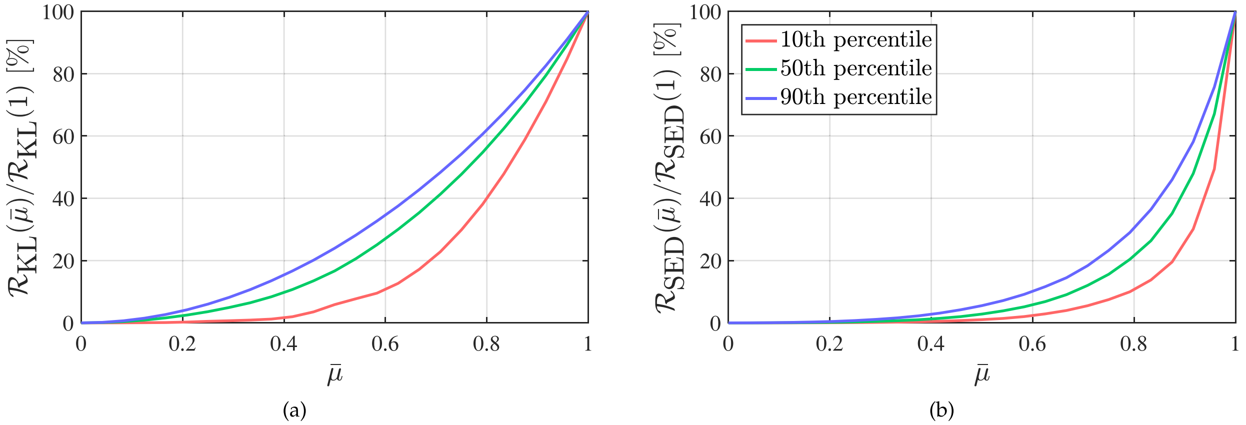


Fig. 17. Percentiles curves of privacy risk for a common $\bar{\mu}$ in the Purchase Card (a) and Foursquare (b) data sets.

In summary, the results provided in this section show how our mechanism would assist users in getting a good[9] deal on the sale of their private data. The results illustrate, besides, that this deal —in addition to being mathematically optimized— can be made without compromising users' privacy excessively. As a matter of fact, for medium values of compensation (e.g., $\bar{\mu} \leqslant 0.4$) we have checked that 90 percent of the populace would increase their privacy risk by at most 3.13 percent. To conclude, the results reported here provide evidence of the benefits of the proposed mechanism and may show the potential impact of a widespread adoption on the data industry. As a matter of fact, if users had access to fairer monetization services in which they had a more effective control over the sale of their data, this could have a pull effect on the demand, and then on supply, of such services, which might contribute to the growth of this industry.

5. Discussion and limitations

In recent years, we are witnessing a transition to an information economy in which information is the primary raw material and the basis for economic growth. Ignoring that any piece of data we generate online contributes to this economy, and at the same time, failing to claim ownership of said information, permit others to do so.

The current situation is a monopoly of the data markets by big technology companies —the classical data brokers— with important negative consequences in terms of market society and individual privacy. To address this situation, a new generation of data brokers have emerged that enable users to trade their data in directly with businesses. Nevertheless, the solution proposed by Datacoup, CitizenMe and DataWallet has not been designed with privacy in mind and still leads to abuse. Although this new monetization paradigm might mainly attract users who are not very concerned about their privacy, the fact is that users must trust the new brokers will fulfill their pledge to protect their data and make the best possible deal for them.

Our mechanism, in contrast, does not require users to trust any broker, but gives them control over their privacy and profits. In terms of privacy, since the hard-privacy model assumed in Section 2.1 delegates the protection of the data only to their owners, which contributes to the principle of data minimization. And in terms of profits, since users share their data only when they have an offer, and not the other way round.

Trying to foresee the actual implications of said control into the new data marketplaces, however, is a challenging task, and so is obtaining a rough estimate of the real-world impact of our mechanism on the data economy and society at large. Bearing this in mind, next we try to elaborate on such implications by splitting the discussion into purchasing model, and theoretical and experimental results.

5.1. Purchasing model

As mentioned above, our mechanism reverses the order in which transactions are made, thereby allowing users to control and value their data by themselves. However, one of the most important features of the proposed mechanism is that it enables a wide spectrum of choices with regard to privacy protection. In the literature of information privacy, some technologies based on access control and encryption offer the possibility of either fully delivering or completely obfuscating user information, by either providing or not a cryptographic key permitting its deciphering. This principle is precisely the one followed by the newly set up brokers, which allow users to sell their data, but permit just a binary choice: either selling full and *continuous* access to a data account, or not. In the case of Datacoup, for example, users are paid after the company

[9] By good, we actually mean the best possible exchange of money for privacy, since the mechanism under study is designed to attain the optimal trade-off between both aspects.

estimates how worthy they are from their data, with no further interaction. The more accounts a user allows access, the more money he/she earns.

In contrast, our purchasing model provides two key advantages to users. On the one hand, data prices are regulated by demand and supply, and on the other hand, users may sell portions of their data, instead of giving full/no access to a buying firm. We believe these two features may help deal with the current situation of abuse posed by the new brokers, which operate with unrestricted access once accounts are acquired.

Nonetheless, not only users may benefit from our model: advertisers and retailers —the other clients of the brokers—, may obtain more accurate data to whom direct offers and more users. This is especially topical for an industry that is trying to counter the growing adoption of ad-blocking and Web anti-tracking technologies [39].

5.2. Theoretical and experimental results

Our mathematical model proposes a formulation that is very flexible with regard to privacy assessment. Users can choose not only the attacker model (i.e., individuation or classification) most appropriate for their needs, but also how they wish to quantify privacy risk. This makes our theoretical results valid for a variety of models and privacy functions, which may facilitate the adoption of our mechanism by users with various privacy requirements.

In terms of design, the proposed mechanism is optimized to attain the minimum disclosure risk for a given compensation, which implies that users of data marketplaces are in the best position to negotiate with interested buyers. From a theoretical perspective, the fact that we find an analytical solution to the problem of optimized sale of data allows us to comprehend how the optimal strategy operates.

Among other theoretical results, the most relevant finding is precisely the principle the solution follows, which permits us to provide the following (informal) recommendations to users of such data brokerage services. If the difference between the actual and initial profiles is small for a category that is very sensitive to the user (in relative terms with such difference), then the disclosure should be made mainly in that category. However, if said difference is comparable to the category rate of some category, and the ratio category rate to profile difference for that category is similar to the mean ratio, then the user should avoid disclosing their profile on that category.

In the simple case when $n = 2$, a user might want to group all sensitive categories and all non-sensitive categories into two classes. In this case, Theorem 7 recommends that users disclose the same amount of information on either category. In the more general case $n > 3$, and under the assumption of a conic regular configuration, the closed-form expression of the optimal strategy follows the same intuitive principle described informally above.

The experiments conducted on two data sets in Section 4 aimed to find out to which extent our mechanism could enhance user privacy in practice. The theoretical analysis determined the key role of the money thresholds in the protection of privacy, but it remained to investigate how these thresholds were distributed in a real population.

The most important conclusion of our experiments is that the money gained by most users would compensate their privacy loss. Specifically, we observed in the Purchase Card data set that the average user would obtain 60% of its maximum compensation in exchange for losing only 25% of their privacy. In the Foursquare data set, the results are even more promising since, for the same reward, the same percentage of users would experience a increase in privacy risk of only 3.13%.

Unfortunately, these empirical results do not seem to be in line with the new data monetization services, which may be providing relatively low benefits to users. One example of these practices is a user of Datacoup reporting only four dollars after a month of data collection on all accounts but banking's [1]. This simply illustrates the abuses of the new model (i.e., all data in exchange for extremely small profits) and evidences the substantial benefits of an adoption of our mechanism by the new brokers. With our solution, users could protect their privacy more effectively (the best possible way) and also, according to our experimental findings, obtain medium values of $\bar{\mu}$ for little disclosure of their profiles. The result of this adoption could be a marked increase of the data industry growth; attracted by a fairer monetization of their personal data, more users could join these data-selling services and hence more companies would appear.

5.3. Limitations

In this section, we discuss potential limitations of our mechanism and alternative strategies. We shall begin with the purchasing model and then continue with the limitations of the mathematical assumptions and the experimental analysis.

As explained in Section 2.1, the proposed mechanism helps users reveal their profile when they have an offer from a buying company. If the offer is accepted, then users share their data with the company in question. This is, however, in contrast with the current practices of the new brokers, which ask for full access to the corresponding account, which implies they can obtain any new data the user generates on that account.

Our mechanism contemplates instead the sale of data in an offline manner[10], and this may regarded as a limitation for the adoption of our mechanism by those brokers. Allowing full access to, and hence continuous monitoring on, an account clearly implies revealing the actual user profile at any time. Similarly, renegotiating the sale of data pertaining to a same

[10] By offline, we mean that brokers and data buyers do not have online access to a user's data account.

account is an operation that is not permitted by our disclosure model. The reason is that renegotiation opens the possibility that data buyers and brokers might draw inferences from the set of apparent profiles available to them, which might reduce the space of possible candidate distributions of the real PMF.

On the other hand, closely related with our purchasing model is the communication protocol enabling the exchange of data for money. In this work, we assume users will follow the protocol honestly, but in practice they might try to deviate from its correct execution. The practical details of this data-transaction process and the analysis of incentives that may punish malicious behaviors are two of our main directions for future work.

In the introductory section, we mentioned that the sale of private data poses several fundamental concerns to users of data marketplaces. The mechanism investigated in this work helps users address such concerns by allowing optimal exchanges of personal data for economic rewards, in the sense of minimizing disclosure risk for an offered compensation. Specifically, the result of the optimization problem (1), which models this exchange, is a disclosure strategy that recommends users which percentage of their data should be disclosed in each category to minimize privacy risk. However, these recommendations, which are given in terms of data percentages as a result of our models of user profiles and profile disclosure, do not specify the concrete data elements of a user's given account that should be shared with the purchasing companies and brokers. In other words, our model assumes that all data elements within a given category count as being equally sensitive.

Since this assumption (i.e., that all data elements within a category are equally sensitive) might not be true for every user, we contemplate the splitting of data into a partition of subcategories where said assumption holds. For example, suppose there is a category with data elements that are clearly more sensitive than the rest of elements within such category. A solution could be considering two subcategories, one that includes the sensitive elements and another that encompasses the non-sensitive ones. The user in question could therefore assign different category rates to each subcategory, and reflect the different sensitiveness of the corresponding data.

As for the theoretical results, the analysis conducted in Section 3 found the solution to the problem of optimal sale of private data for any n. However, as already mentioned in Section 3.3, the derivation of an explicit closed-form expression for any $n > 3$ and any μ, q, p, w is hindered by the lack of regularity of the slabs layout posed by such variables. Specifically, for large n, a general closed-form expression and analysis of the underlying trade-off is intractable. For this reason, our analysis of the solution and the trade-off between privacy and economic reward examines some specific but interesting cases of slabs layouts. Future research will explore other configurations of slabs layouts that permit deriving a closed-form expression for large n.

Another potential limitation of our approach stems from the privacy functions assumed by our mathematical model. Although the theoretical analysis is restricted to dissimilarity functions that are non-negative, twice differentiable and convex in the pair, we would like to stress that some of the most popular dissimilarity and distance functions meet these properties. Examples of such functions include Bregman divergences, which have been extensively used to evaluate privacy [21,26,50,52,56]. From a practical perspective, the limited, albeit rich variety of privacy functions a user can choose from may ease the adoption of our mechanism by users with different requirements.

With regard to our experimental evaluation, the reported results depend on the categorization of the data elements and the choice of the initial profile of each user. In the Foursquare data set, we employed the taxonomy provided by the social network, although some preprocessing was necessary to eliminate the less popular categories and thus avoid user profiles with a large number of zero components. In the Purchase Card data set, on the contrary, logs were not categorized and our experimental methodology, which relied on a standard procedure to group them into three purchasing intervals, might have had an effect on the results. That said, the most promising results were not observed for this latter data set, but for the Foursquare one.

Finally, the choice of p in the classification model was made to allow for a worst-case scenario of users wishing to impersonate very distant profiles. We would like to emphasize that this design decision did not have any impact on the results reported in Section 4 since $\mu_{\max}$ depends only on w.

6. Related work

To the best of our knowledge, this work is the first to mathematically investigate a hard-privacy mechanism by which users themselves —without the need of any intermediary entity— can sell profile information and achieve serviceable points of operation within the optimal trade-off between disclosure risk and economic reward. As we shall elaborate next, quite a few works have investigated the general problem of sharing private data in exchange for an economic compensation. Nevertheless, they tackle different, albeit related, aspects of this problem: some assume an interactive, query-response data release model [7,15,24,35,46] and aim at assigning prices to noisy query answers [24,35,46]; most of them assume distinct purchasing models where data buyers are not interested in the private data of any particular user, but in aggregate statistics about a large population of users [7,15,24,35,46]; the majority of the proposals limit their analysis to differential privacy [18] as measure of privacy [15,24,35,46]; and some rely on a soft-privacy model whereby users entrust an external entity or trusted third party to safeguard and sell their data [7,15,24,35].

In this section we briefly examine several of those proposals, bearing in mind that none of them are user-centric and consider that data owners can sell their profile data directly to brokers. The theoretical analysis of the privacy-money trade-off posed by a mechanism like this is, precisely, the object of this work.

The study of the monetization of private data was first investigated formally in [24]. The authors tackled the particular problem of pricing private data [47] in a purchasing model composed of data owners, who contribute their private data; a data purchaser, which sends aggregate queries over many owners' data; and a data broker, which is entrusted those data, replies and charges the buyer, and ultimately compensates the owners. Accordingly, the problem consists in assigning prices to noisy answers, as a function of their accuracy, and how to distribute the money among data owners who deserve compensation for the privacy loss incurred. The operation of the monetization protocols may be described conceptually as follows: in response to a query, the data broker computes the true query answer, but adds random noise to protect the data owners' privacy. By adding perturbation to the query answer, the price can be lowered so that the more perturbation is introduced, the lower the price is charged. The data buyer may indicate to this end how much precision it is willing to pay for when issuing the query, similarly to our data-purchasing model where we assume buyers start bidding before any disclosure is made.

Various extensions and enhancements were introduced later in [14,22,35,36,48]. The most relevant is [35], which also capitalizes on differential privacy to quantify privacy, but differs in that it permits several queries and does not require that the minimum compensation users want to receive be public information (as we assume in this work). This approach, however, cannot be applied to the problem at hand since it relies on a distinct purchasing model where data buyers are not concerned with a single user's data, but aim to obtain aggregate statistics about a population through an interactive, query-response database. This is in stark contrast to our approach, which assumes buyers are interested in purchasing profile data of particular users, for example, to provide personalized, tailored services such as behavioral advertising [25]. In addition, our work leverages a hard-privacy model by which users take charge of protecting their profile data on their own before selling this information to data brokers.

Another related work is [7], which considers a rather simple mechanism to regulate the exchange of money for private data. The proposed setting permits a buyer to select the number of data owners to be involved in the response to its query. The mechanism is based on the assumption that a significant portion of data owners show risk-averse behaviors [29]. The operation of the mechanism, however, leaves users little control over their data: a market maker is the one deciding whether to disclose the whole data of an individual or to prevent any access to this information otherwise. Our data-buying model does not consider these two extremes, but the interesting continuum in between enabled by a disclosure mechanism designed to attain the optimal privacy-money trade-off. Interestingly, our approach may be used in combination with the mechanism proposed in the cited work.

7. Conclusions

In this work, we examine a mechanism that gives users control over the sale of their data. The mechanism relies on a variation of the purchasing model proposed by the new broker firms which is in line with the literature of pricing private data, and enables users themselves to respond directly to buyers' offers.

The objective of this paper is to investigate mathematically the disclosure-money trade-off posed by this mechanism. With this aim, we propose modeling profiles as PMFs, and quantifying privacy as a function of a user's disclosed profile and an initial profile they want to impersonate when no reward is offered for their data. Equipped with this function, we formulate a multiobjective optimization problem characterizing the trade-off between privacy risk on the one hand, and on the other economic reward.

Our theoretical analysis provides a general parametric solution to this problem and characterizes the optimal trade-off between profile disclosure and money. The solution is derived for additively separable, twice differentiable privacy functions, with strictly increasing derivatives; and although this limits our analysis of the trade-off, the fact is that a myriad of functions (such as some important Bregman divergences) satisfy these requirements.

We find that the optimal disclosure exhibits a maximin form, depends on the inverse of the derivative of the privacy function, and leads to a nondecreasing and convex trade-off. The particular form of each of the n components of the solution, however, is determined by the specific configuration of $2n$ halfspaces, which in turn depend on the particular values of q, p, w, μ and n.

To proceed towards an explicit closed-form solution, we study some examples of privacy functions and particular cases of those variables. Specifically, we derive riveting results for important examples of Bregman divergences, although special attention is given to the SED function for its mathematical tractability. Also, we split the analysis into two cases: a general configuration of slabs for $n \leq 3$, and a conic regular configuration for $n \geq 3$.

In our analysis, we show the existence of an origin of coordinates in the slabs layout that permits us to leverage certain regularities. One of the most relevant results is the dependence of the closed-form solution (essentially) on Fano's factor and the intuitive principle behind the optimal strategy, which recommends disclosing a profile mostly in those categories where d_i is small and m_i deviates the most from its mean value, compared to its variance.

Further, we investigate a concrete slabs layout that allows us to obtain an explicit closed-form expression of both the solution and trade-off for an arbitrarily large n. The configuration of slabs, which we call conical regular, permits parameterizing the solution with polar coordinates. The optimal strategy is also a piecewise linear function of the same index of dispersion, which may indicate a similar behavior of the solution in a general configuration. Our findings show that the particular form attained by each of the components of the solution is determined by a sequence of thresholds, which we interpret geometrically as lower hyperplanes.

Finally, the last section is devoted to the experimental evaluation of our mechanism in a real-world scenario of data brokerage. In particular, we study how the application of the proposed mechanism might help users make the best possible deal when selling access to their banking accounts and their data at Foursquare. The most relevant result is the reduced impact our mechanism would have on user privacy for relatively large values of $\bar{\mu}$.

Acknowledgment

We would also like to thank the anonymous reviewers for their immensely helpful suggestions to improve the readability and contents of this paper. This work was partly funded by the European Commission through the H2020 project "CLARUS", as well as by the Spanish Ministry of Economy and Competitiveness (MINECO) through the project "Sec-MCloud", ref. TIN2016-80250-R. J. Parra-Arnau is the recipient of a Juan de la Cierva postdoctoral fellowship, FJCI-2014-19703, from the MINECO.

Appendix A. Convexity in the Pairs of SED

This appendix shows that the SED privacy function satisfies the convexity property given in Definition 2.

Proposition 13. *The SED function* $f(t, p) = \sum_i (t_i - p_i)^2$ *is a convex function in the pair* (t, p).

Proof. It closely follows the proof of Theorem 7.2 of [13, Section 2]. Write the SED function as the sum of separable functions $f_i(t, p) = (t_i - p_i)^2$. We proceed by applying the left-hand side of (5) to $f_i(t, p)$:

$$\begin{aligned} f_i(\lambda t_{1_i} + (1-\lambda) t_{2_i}, \lambda p_{1_i} + (1-\lambda) p_{2_i}) &= \Big(\lambda\,(t_{1_i} - p_{1_i}) + (1-\lambda)\,(t_{2_i} - p_{2_i})\Big)^2 \\ &\leqslant \lambda\,(t_{1_i} - p_{1_i})^2 + (1-\lambda)\,(t_{2_i} - p_{2_i})^2 \\ &= \lambda f_i(t_{1_i}, p_{1_i}) + (1-\lambda) f_i(t_{2_i}, p_{2_i}), \end{aligned}$$

where the inequality follows from the fact that $f(x) = x^2$ is a convex function. Summing this all over i, we obtain the desired property for the SED. □

References

[1] "Data pays: Datacoup first month review," Panacea3, Tech. Rep., accessed on 2017-08-22. [Online]. Available: https://www.panacea3.com/datacoup/.
[2] Purchase card (pcard) fiscal year 2015.
[3] Adblock plus user survey results, part 3, Tech. rep., dec., Eyeo, 2011. Accessed on 2015-07-11. [Online]. Available: https://adblockplus.org/blog/adblock-plus-user-survey-results-part-3.
[4] Privacy and security in a connected life: A study of us, european and japanese consumers, Tech. rep., mar., Ponemon Institute, 2015. Accessed on 2016-05-14. [Online]. Available: http://www.trendmicro.com/vinfo/us/security/news/internet-of-things/internet-of-things-connected-life-security.
[5] State of privacy report 2015, Tech. rep., feb., Symantec, 2015. Accessed on 2015-05-10. [Online]. Available: https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf.
[6] The age of digital enlightenment, Tech. rep., mar., Logicalis, 2016. Accessed on 2016-05-17. [Online]. Available: http://www.uk.logicalis.com/globalassets/united-kingdom/microsites/real-time-generation/realtime-generation-2016-report.pdf.
[7] C. Aperjis, B.A. Huberman, A market for unbiased private data: paying individuals according to their privacy attitudes, First Sunday 17 (5) (2012).
[8] T.M. Apostol, Mathematical Analysis. A Modern Approach to Advanced Calculus, 2nd ed., Addison Wesley, 1974.
[9] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, D. Sicker, Low-resource routing attacks against anonymous systems, University of Colorado, 2007 Tech. rep..
[10] S. Boyd, L. Vandenberghe, Convex Optimization, Cambridge University Press, Cambridge, UK, 2004.
[11] L.M. Bregman, The relaxation method of finding the common point of convex sets and its application to the solution of problems in convex programming, USSR Comput. Math., Math. Phys. 7 (1967) 200–217.
[12] D. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, Commun. ACM 24 (2) (1981) 84–88.
[13] T.M. Cover, J.A. Thomas, Elements of Information Theory, 2nd ed., Wiley, New York, 2006.
[14] P. Dandekar, N. Fawaz, S. Ioannidis, Privacy Auctions for Inner Product Disclosures, CoRR, 2011. Abs/1111.2885, Nov.
[15] P. Dandekar, N. Fawaz, S. Ioannidis, Privacy auctions for recommender systems, ACM Trans. Econ., Comput. 2 (3) (2014).
[16] M. Deng, Privacy preserving content protection, Katholieke Univ. Leuven, Jun., 2010 Ph.d. dissertation.
[17] J. Domingo-Ferrer, U. González-Nicolás, Rational behavior in peer-to-peer profile obfuscation for anonymous keyword search, Inform. Sci. 185 (1) (2012) 191–204.
[18] C. Dwork, Differential Privacy, in: Proc. Int. Colloq. Automata, Lang., Program., 2006, pp. 1–12. Springer-Verlag
[19] Y. Elovici, B. Shapira, A. Maschiach, A new privacy model for hiding group interests while accessing the Web, in: Proc. Workshop Priv. Electron. Soc, 2002, pp. 63–70. Washington, DC: ACM.
[20] Y. Elovici, B. Shapira, A. Meshiach, Cluster-analysis attack against a private web solution (PRAW), Online Inform. Rev. 30 (2006) 624–643.
[21] A. Erola, J. Castellà-Roca, A. Viejo, J.M. Mateo-Sanz, Exploiting social networks to provide privacy in personalized web search, J. Syst., Softw. 84 (10) (2011). 1734–745. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0164121211001117.
[22] L.K. Fleischer, Y.-H. Lyu, Approximately optimal auctions for selling privacy when costs are correlated with data, in: Proc. ACM Conf. Electron. Commer. (EC). ACM, 2012, pp. 568–585.
[23] M. Fredrikson, B. Livshits, RePriv: Re-envisioning in-browser privacy, in: Proc. IEEE Symp. Secur., Priv. (SP), 2011, pp. 131–146.
[24] A. Ghosh, A. Roth, Selling privacy at auction, in: Proc. ACM Conf. Electron. Commer. (EC). ACM, 2011, pp. 199–208.
[25] A. Goldfarb, C.E. Tucker, Online advertising, behavioral targeting, and privacy, Commun. ACM 54 (5) (2011) 25–27.
[26] M. Halkidi, I. Koutsopoulos, A game theoretic framework for data privacy preservation in recommender systems, in: Proc. European Mach. Learn., Prin., Pract. Knowl. Disc. Databases (ECML PKDD), 2011, pp. 629–644. Springer-Verlag.
[27] M. Hildebrandt, J. Backhouse, V. Andronikou, E. Benoist, A. Canhoto, C. Diaz, M. Gasson, Z. Geradts, M. Meints, T. Nabeth, J.P.V. Bendegem, S.V.d. Hof, A. Vedder, A. Yannopoulos, Descriptive analysis and inventory of profiling practices – deliverable 7.2, Future Identity Inform. Soc. (FIDIS), 2005 Tech. rep..

[28] M. Hildebrandt, S. Gutwirth (Eds.), Profiling the European Citizen: Cross-Disciplinary Perspectives, Springer-Verlag, 2008.
[29] C.A. Holt, S.K. Laury, Risk aversion and incentive effects, J. Amer. Review 92 (2002) 1644–1655.
[30] F. Itakura, S. Saito, Analysis synthesis telephony based upon the maximum likelihood method, in: Proc. Int. Congr. Acoust., Tokyo, Japan, 1968. pp. 17-2
[31] E.T. Jaynes, On the rationale of maximum-entropy methods, Proc. IEEE 70 (9) (1982) 939–952.
[32] T. Kuflik, B. Shapira, Y. Elovici, A. Maschiach, Privacy preservation improvement by learning optimal profile generation rate, in: User Modeling, in: ser. Lecture Notes Comput. Sci. (LNCS), volume 2702, 2003, pp. 168–177. Springer-Verlag.
[33] S. Lang, Algebra, Menlo Park Cal: Addison Wesley, 1993.
[34] B.N. Levine, M.K. Reiter, C. Wang, M. Wright, Timing attacks in low-latency mix systems, in: Proc. Int. Financial Cryptogr. Conf., 2004, pp. 251–265. Springer-Verlag
[35] C. Li, D.Y. Li, G. Miklau, D. Suciu, A theory of pricing private data, in: Proc. ACM Int. Conf. Database Theory (ICDT). ACM, 2013, pp. 33–44.
[36] K. Ligett, A. Roth, Take it or leave it: running a survey when privacy comes at a cost, in: Proc. Int. Conf. Internet Netw. Econ. (WINE), 2012, pp. 378–391. Springer-Verlag.
[37] S.P. Lloyd, Least squares quantization in PCM, IEEE Trans. Inform. Theory IT-28 (1982) 129–137.
[38] S.J. Murdoch, G. Danezis, Low-cost traffic analysis of tor, Proc. IEEE Symp. Secur., Priv. (SP) (2005) 183–195.
[39] K. Murphy, The ad blocking wars, Feb. 2016, accessed on 2015-02-22. [Online]. Available: http://www.nytimes.com/2016/02/21/opinion/sunday/the-ad-blocking-wars.html.
[40] J. Parra-Arnau, J.P. Achara, C. Castelluccia, MyAdChoices: Bringing transparency and control to online advertising, ACM Trans. Web 11 (1) (2017). [Online]. Available: https://hal.inria.fr/hal-01270186/document.
[41] B. Pfitzmann, A. Pfitzmann, How to break the direct RSA implementation of mixes, in: Proc. Annual Int. Conf. Theory, Appl. of Cryptogr. Techniques (EUROCRYPT), 1990, pp. 373–381. Springer-Verlag, May
[42] S. Puglisi, D. Rebollo-Monedero, J. Forné, You never surf alone. ubiquitous tracking of users' browsing habits, in: Proc. Int. Workshop Data Priv. Manage. (DPM), 2015. Vienna, Austria, Sep.
[43] D. Rebollo-Monedero, J. Forné, Optimal query forgery for private information retrieval, IEEE Trans. Inform. Theory 56 (9) (2010) 4631–4642.
[44] D. Rebollo-Monedero, J. Forné, J. Domingo-Ferrer, Coprivate query profile obfuscation by means of optimal query exchange between users, IEEE Trans. Depend., Secure Comput. 9 (5) (2012) 641–654. [Online]. Available: http://doi.ieeecomputersociety.org/10.1109/TDSC.2012.16.
[45] M.G. Reed, P.F. Syverson, D.M. Goldschlag, Proxies for anonymous routing, in: Proc. Comput. Secur. Appl. Conf. (CSAC), 1996, pp. 9–13. San Diego, CA, Dec.
[46] C. Riederer, V. Erramilli, A. Chaintreau, B. Krishnamurthy, P. Rodriguez, For sale: your data: by: you, in: Proc. Hot Topics in Netw., 2011. Cambridge, Massachusetts, USA, Nov.
[47] A. Roth, Buying private data at auction: the sensitive surveyor's problem, ACM SIGecom Exchanges 11 (1) (2012) 1–8.
[48] A. Roth, G. Schoenebeck, Conducting truthful surveys, cheaply, in: Proc. ACM Conf. Electron. Commer. (EC). ACM, 2012, pp. 826–843.
[49] J. Shao, N. York, Mathematical statistics, Springer, 1999.
[50] R. Shokri, G. Theodorakopoulos, J.Y.L. Boudec, J.P. Hubaux, Quantifying location privacy, in: Proc. IEEE Symp. Secur., Priv. (SP), 2011, pp. 247–262. Washington, DC, USA: IEEE Comput. Soc.
[51] A.W. Sile, Privacy compromised? might as well monetize, 2015, Accessed on 2016-05-24. [Online]. Available: http://www.cnbc.com/2015/01/30/privacy-compromised-might-as-well-monetize.html.
[52] O. Tan, J. Gomez-Vilardebo, D. Gunduz, Privacy-cost trade-offs in demand-side management with storage, IEEE Trans. Inform. Forensics, Security 12 (2017) 1458–1469.
[53] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, S. Barocas, Adnostic: Privacy preserving targeted advertising, in: Proc. Symp. Netw. Distrib. Syst. Secur. (SNDSS), 2010, pp. 1–21.
[54] Y. Xu, K. Wang, B. Zhang, Z. Chen, Privacy-enhancing personalized Web search, in: Proc. Int. WWW Conf. ACM, 2007, pp. 591–600.
[55] D. Yang, D. Zhang, V.W. Zheng, Z. Yu, Modeling user activity preference by leveraging user spatial temporal characteristics in lbsns, IEEE Trans. Syst. Man, Cybern. 45 (1) (2015) 129–142.
[56] S. Ye, F. Wu, R. Pandey, H. Chen, Noise injection for search privacy protection, in: Proc. Int. Conf. Comput. Sci., Eng. IEEE Comput. Soc., 2009, pp. 1–8.