HDSR
HARVARD DATA SCIENCE REVIEW

Volume 0 Issue 0
DOI: 00.000
ISSN: 2644-2353

Making Data Markets more Fair and Transparent using Data Unions and Contextual Integrity

Raul Castro Fernandez[†,*]
[†] The University of Chicago

Abstract. Billions of individuals give their data to online platforms in exchange for search, social networks, health insights from wearables, and other online services. Platforms pool individuals' data together to create services from which they profit. Although the revenue stems from individuals' data, platforms benefit the most, sometimes at the expense of individuals' privacy. The consequence is a *data market* that is not fair (platforms benefit proportionally more than individuals) and is not transparent, affecting individuals' privacy.

In this paper, we: i) analytically study the effect of two mechanisms on data markets, *data unions* and *contextual integrity*; and ii) propose a software architecture to implement these mechanisms in current markets. Data unions are intermediaries that capture individuals' data to gain leverage with respect to platforms. Contextual integrity is a privacy philosophy where individuals control the *purpose* for which data is shared.

First, we show that data unions strictly improve individuals' utility by capturing some of the data value that only platforms capture today. We show that contextual integrity forces the market to be transparent and gives individuals more choice. Transparency and increased choice translate into better protection of individuals' privacy. Finally, to bridge the gap between theory and practice, we introduce a software architecture, called Data Station, to implement data unions and contextual integrity in data markets. This paper takes a step towards revamping today's data markets to make them fairer and more transparent.

Keywords: data market, data union, contextual integrity

Media Summary

Daily, billions of individuals give their data to online platforms in exchange for search, social networks, health insights from wearables, and other online services. Platforms group the data from every individual to create services from which they profit, e.g., to sell advertisements or consumer data. Although the revenue platforms raise stems from individuals' data, platforms benefit the most, sometimes at the expense of individuals' privacy. The consequence is a *data market* that is not fair (platforms benefit proportionally more than individuals) and is not transparent, affecting individuals' privacy.

[*] raulcf@uchicago.edu

In reaction to this situation, many have proposed to compensate individuals for their data. This compensation could be as a dividend of the revenue the platform raises, or proportional to the data contributions of individuals. In the spirit of these proposals, in our paper we study two alternative ways of taking some of the power platforms enjoy today, and giving it back into individuals. First, we study the effect of data unions. A data union combines data from individuals and then negotiates with platforms on their behalf, obtaining a better compensation for their data contribution. We also study a different privacy policy that benefits individuals: contextual integrity. We normally think of privacy as controlling access to our data. With contextual integrity, we specify not only who access our data, but for what purpose they are allowed to do so.

Looming regulations, and a society that is growing uneasy in the current climate of dominant platforms may force a change to how data is governed soon. And if change is coming, it is important to understand how to build fair and transparent data markets. Our study of how data unions and contextual integrity affect data markets contribute to understanding how to build better data markets.

1. Introduction

Daily, billions of individuals exchange personal data with online platforms for services such as search ("Google Data Collection Privacy", 2021), social platforms ("Facebook Data Collection Privacy", 2021; "Twitter Data Collection Privacy", 2021), health insights from wearables ("Oura Data Collection Privacy", 2021), and entertainment ("Spotify Data Collection Privacy", 2021), in what constitutes the largest data market in history ("Personal Data is worth billions, these startups want you to get a cut", 2021; Zuboff, 2019). A critical problem is that this data market is not transparent because individuals do not know how platforms use their data, and it is not fair because platforms benefit from individuals' data proportionally more than individuals themselves. Because it is not transparent, individuals do not know how their data is used, so they cannot decide if their privacy is respected. The market is not fair. Platforms exploit data's combinatorial power by correlating individuals' across groups and using that information to create revenue streams, such as advertising (Goldfarb, 2014). Individuals, on the other hand, do not benefit proportionally from the combinatorial power that stems from their own data. This lack of transparency and fairness leads to platforms exercising disproportionate power via the collection, usage, and exploitation of individuals' data.

Proposals such as data dividends ("Data Dividend, My data, my money", 2021), data trusts (Delacroix & Lawrence, 2019), data cooperatives ("Mozilla Research. Shifting power through data governance", 2021), and data-as-labor (Posner & Weyl, 2019) aim to correct the asymmetry between individuals and platforms. These proposals, which we refer to as *data unions*, appeal to the intuition that by pooling their data together, individuals gain leverage with respect to platforms. Despite the appeal of these ideas, it is not yet clear how they affect individual's and platform's welfare; most principled efforts focus on the legal challenges of implementing them (Delacroix & Lawrence, 2019). But understanding their impact empirically remains hard because current platforms have no incentives to change their market design and the strong network effects they generate makes it hard to attract individuals to alternative (fair and transparent) platforms. Despite the difficulties, change is possible. Looming regulations (Anderson & Mariniello, 2021), and a society that is growing uneasy in the current climate of dominant platforms may force such a change soon. And if change is coming, it is important to understand how to build fair and transparent data markets.

In this paper, we take three steps towards designing fair and transparent individual-platform data markets (IPDM). First, we use a data market model to understand whether *data unions* boost individuals' utility and overall social surplus, i.e., the combined utility of individuals and platform. We show that data unions let individuals capture some of the value generated from their data, making the market fairer. Second, we model the use of contextual integrity (Nissenbaum, 2004) in data markets. Contextual integrity is a privacy philosophy where in addition to control *what* data is shared, individuals control *how* it can be used, i.e., for what purposes. We show that *contextual integrity* forces data markets to become transparent, and show the benefits associated with this increased transparency. To demonstrate the impact of unions and contextual integrity we use a value of data model along with a game-theoretic model introduced in previous literature (Acemoglu et al., 2019). Third, we present the blueprint of a software system that implements unions and contextual integrity in IPDMs, paving the way towards the practical implementation of fair and transparent individual-platform data markets. In more detail:

Data Unions capture data externalities. When individuals share private data with a platform, they also share information about other individuals that are correlated with them. These correlations are leveraged, for example, by recommendation algorithms to power many Internet services such as Netflix, Amazon, Spotify, and the ad industry that makes the tech industry, among

others, profitable (Gomez-Uribe & Hunt, 2015; Sanna Passino et al., 2021; Smith & Linden, 2017; Varian, 2007). The excess information learned about others via an individual's data is called *data externality* (Acemoglu et al., 2019). While platforms exploit such externalities to monetize individuals' data, individuals only benefit indirectly, e.g., when platforms provide valuable content recommendations. In this paper, we show how data unions capture the externalities generated by the individuals' pooled data, and share with individuals benefits that stem from their data but that today are fully captured by platforms.

Contextual Integrity makes data usage transparent. In a transparent market, platforms tell individuals how they use their data, so individuals can decide whether to participate. Today, opaque terms of service make it hard for individuals to understand how their data is used. With contextual integrity, data flows are transparent and agreed upon by platform and individuals. This results in better privacy guarantees, as individuals decide whether to exchange their data having better information on how it will be used. A market with contextual integrity is more transparent, and we show how transparency benefits individuals.

Platform Blueprint. We present the blueprint of a software system called Data Station that implements data unions and contextual integrity. Data unions require an intermediary to pool data and contextual integrity requires enforcing that platforms use data for the pre-agreed purposes. Data Stations help implement both requirements. While we use mathematical models to demonstrate the value of unions and contextual integrity, Data Station is a first step towards bridging the gap between theory and practice. It illustrates how the above ideas can be implemented with today's technology.

We introduce preliminaries and the baseline data market model in Section 2. We present the model of data unions and contextual integrity in Sections 3 and 4, respectively. We present Data Stations in Section 5, followed by related work (Section 6) and conclusions in Section 7.

2. Value of Data Model and Individual-Platform Data Market Setup

In this section, we use the game-theoretic model of individual-platform data market model that was first introduced in Acemoglu et al. (2019) (IPDM model). However, we modify it using a model of the value of data which is based on information theory. The value of data model helps us simplify the IPDM model and extend it to study data unions and contextual integrity.

2.1. Preliminaries.

We present the platform's goal and scope of our analysis.

The Platform's Goal. An individual i has a type T_i which is a realization of the random variable. When individuals join the platform, they share data that contains information about their type. For example, location data (shared by the individual) may reveal that the individual frequents expensive restaurants and indicate food preferences and even annual income (Malmi & Weber, 2016). Platforms profit according to the degree to which they can predict the individual's type. For that, they use the individual's data to build an estimator of T_i, called A_i. We are not interested in how A_i is built from data, so from now on, we say individuals share A_i and skip the process platforms follow to obtain A_i from the shared data, which is specific to each platform's expertise and irrelevant to our analysis. In conclusion, platforms want individuals to join and share A_i so they can predict T_i.

We note that even when individuals try hard to conceal their data, even short and indirect interactions with a platform suffice to create a *shadow* profile (Debatin et al., 2009) of these individuals. As a consequence, platforms use these shadow profiles to predict every individual's type. When we

talk about individuals in the subsequent discussion, we assume individuals for whom the platform can predict their type.

Scope of the analysis. We concentrate on platforms that want to predict individuals' types at one point in time, i.e., we do not consider dynamic types. We also assume that when individuals join the platform, they provide their true data to access the service and so we do not model cases of "data poisoning". Finally, we do not consider in our analysis other forms of individual's data contributions, such as producing content (e.g., posts, videos) and other forms of data work, such as labeling training data for supervised machine learning tasks. Dynamic types, data poisoning, and other forms of data contributions are interesting avenues of future work but modeling them is not necessary to study the effects of data unions and contextual integrity in fairness and transparency, which are the target goals of our work.

2.2. **The Value of Data Model.** To analyze Individual-Platform Data Markets (IPDM) we need to value the asset exchanged. Valuing data is hard and depends on context and application. We do not fully characterize the economic value of data here. Instead, we use mutual information to express how much a platform learns about T_i when accessing data from the individual.

Individual's data and type. The entropy of T_i indicates the uncertainty of the individual's type, $H(T_i) = -\sum_{x \in X} p(x) * log_2(x)$[1]. The higher the value, the higher the uncertainty. Given two non-independent random variables, T_i and A_i (A_i is derived from the data shared by the individual), obtaining access to one provides some information (i.e., reduces uncertainty) about the other[2]. Mutual information determines the reduction of uncertainty on T_i given A_i, $I(T_i; A_i) = H(T_i) - H(T_i/A_i)$. An individual's data, A_i, is valuable to predict T_i and the platform can combine data from different individuals, that may be correlated among themselves, to reduce the uncertainty.

Data has combinatorial power. Consider two individuals share, A_1 and A_2. That data has combinatorial power means that if we had access to both A_1 and A_2 simultaneously, we would obtain more value (reduce uncertainty of T_i further) than from accessing them individually, i.e., that $I(T_i; A_1) + I(T_i; A_2) \leq I(T_i; A_1, A_2)$. We can show that this is true by expanding the expression into $H(T_i) - H(T_i/A_1) - H(T_i/A_2) \leq -H(T_i/A_1, A_2)$. Then, $H(T_i) \leq H(T_i/A_1) + H(T_i/A_2) - H(T_i/A_1, A_2)$. Since $H(T_i) \geq 0$, then $H(T_i/A_1, A_2) \leq H(T_i/A_1) + H(T_i/A_2)$. This confirms that simultaneous access to A_1 and A_2 is more valuable than access to each individually. This model of the value of data makes the expression "data's combinatorial power" concrete. We use this throughout the paper to reason about data externalities; how access to an individual's data *informs* the platform about other individuals' type.

2.3. **Individual-Platform Data Market Model Setup and Baseline Results.** In an Individual-Platform Data Market (IPDM) there are two kinds of players, individuals and online platforms (Acemoglu et al., 2019). Individuals exchange their data for services provided by platforms. Platforms use individuals' data to improve the services offered to those individuals as well as to raise revenue through various data-driven business models such as advertising, selling individuals data for customer segmentation, and other profitable data services.

2.3.1. *Preliminaries and Model Setup.* Consider n individuals, $V = 1, ..., n$, each with a type, T_i. An individual, i, who decides to join the platform shares A_i, and $I(T_i; A_i) \geq 0$. Because platforms profit according to how well they predict T_i, and they know A_i leaks information about T_i, they

[1]here we use X as the support of T_i

[2]Except when A_i and T_i are totally independent, but often in practice they are not, as evidenced by the numerous profitable data-driven platforms

are willing to compensate individuals to join their platform so they share A_i. As in the original model (Acemoglu et al., 2019), we use payment, p_i, as a convenient way of modeling the incentive the platform uses to attract individuals, i.e., it could be service quality, features, or money. We use money in the remainder to simplify the presentation. Individuals value their privacy according to a parameter $v_i \geq 0$. Higher values represent individuals with higher value for their privacy. In deciding whether to join a platform, individuals consider the incentive they gain and the privacy they lose by sharing A_i.

Leaked information and data externalities. Let $a_i = 1$ indicate individual i shares data with (i.e., joins) the platform, and $a_i = 0$ not sharing. Then, $\vec{a} = (a_1, ..., a_n)$ is the vector of sharing decisions. We use $\vec{a}_{-i}$ to indicate the sharing decisions that individuals other than i made. We use $D_{\vec{a}}$ to indicate the combination of data from individuals who shared according to the vector of sharing decisions $\vec{a}$. Then, the mutual information, $I(T_i; D_{\vec{a}})$ indicates how much a platform with access to $D_{\vec{a}}$ learns about T_i. Data externalities means that how much a platform knows about individual i depends not only on whether i shares, but on other individuals' sharing decisions as well. An unfortunate consequence of data externalities is that individuals have little power in enforcing their privacy preferences because their data leaks through others' sharing decisions, and platforms monetize access to this data.

Individual and Platform Utility Expressions. Given a price vector $\vec{p} = (p_1, ..., p_n)$, set by the platform, individuals' utility is defined as:

$$u_i(a_i, \vec{a}_{-i}, p_i) = \begin{cases} p_i - v_i * I(T_i; D_{\vec{a}}) & \text{if } a_i = 1, \\ -v_i * I(T_i; D_{\vec{a}_{-i}}) & \text{if } a_i = 0 \end{cases} \tag{2.1}$$

Individuals' utility is harmed according to i) how much externalities are produced by individuals who share, as given by the $I(T_i; D_{\vec{a}_{-i}})$ term, and; ii) by their own sharing decision. If they share, they receive a payment p_i and release A_i, so the platform learns more about them. This is reflected in the mutual information term, that changes from $D_{\vec{a}_{-i}}$ to $D_{\vec{a}}$ to reflect the own individual's data contribution when they share. Even if they do not share, they incur a privacy cost as the platform predicts their type: remember that even short interactions with a platform suffice to create shadow profiles that can be used for prediction.

The platform's utility consists of their ability to predict individuals' types minus the price of attracting individuals to the platform:

$$U(\vec{a}, \vec{p}) = \sum_{i \in V} I(T_i; D_{\vec{a}}) - \sum_{i \in V : a_i = 1} p_i \tag{2.2}$$

Data appears in both the individual and platform utility functions via the $I(T_i; D_{\vec{a}})$ term. Note that when $v_i < 1$ the platform values i's data more than the individual, because v_i is multiplying the exchanged term in the individual's utility function (2.1).

Equilibrium concept. In Acemoglu et al. (2019), this IPDM is modeled as a two-step Stackelberg game. First, platforms choose a price vector, $\vec{p}$. Second, individuals react to the price vector by deciding whether to join the platform. The platform chooses $\vec{p}$ to induce sharing actions from individuals in a way that maximizes its utility. In the equilibrium, neither individuals not platform can deviate (change joining decision or price) without harming their utility.

2.3.2. *Analyzing Equilibrium.* We find the sharing decision that maximizes social surplus as presented in Acemoglu et al. (2019), but we use the value of data model based on information theory

presented above because it helps simplify the proof and the presentation of subsequent sections. The social surplus is the combination of individuals' and platform's utility:

$$SS(\vec{a}) = U(\vec{a}, \vec{p}) + \sum_{i \in V} u_i(\vec{a}, \vec{p}) = \sum_{i \in V} (1 - v_i) * I(T_i; D_{\vec{a}}) \tag{2.3}$$

Now, we want to know when an individual's best action is to share $a_i = 1$ and when not.

Proposition 1. *To maximize social surplus, without accounting for externalities, individual i shares data ($a_i = 1$) when $v_i \leq 1$.*

Proof. We want to understand when sharing increases social surplus, $SS(\vec{a_{-i}}, a_i = 1) \geq SS(\vec{a_{-i}}, a_i = 0)$. If we replace the expression with the social surplus expression from (2.3), then we have:

$$\sum_{j \in V, j \neq i} (1 - v_j) I(T_j; D_{\vec{a}}) + (1 - v_i) I(T_i; D_{\vec{a}}) \geq \sum_{j \in V, j \neq i} (1 - v_j) I(T_j; D_{\vec{a_{-i}}}) + (1 - v_i) I(T_i; D_{\vec{a_{-i}}}) \tag{2.4}$$

Note that $(1 - v_i) I(T_i; D_{\vec{a}}) = (1 - v_i) \sum_{j \in V, j \neq i} I(T_i; A_j) + (1 - v_i) I(T_i; A_i)$. Then, if there were no externalities the expression above is equivalent to:

$$(1-v_i) \sum_{j \in V, j \neq i} I(T_j; A_j) + (1 - v_i) I(T_i; A_i) \geq (1-v_i) \sum_{j \in V, j \neq i} I(T_j; A_j) \Rightarrow (1-v_i) I(T_i; A_i) \geq 0 \tag{2.5}$$

and because $I(T_i; A_i) \geq 0$, then the expression is only true when $v_i < 1$. In other words, without externalities, in equilibrium, individuals share when $v_i < 1$ and they do not share when $v_i > 1$. When there are externalities, however, the best sharing decision depends on how much sharing affects other individuals, both in number and in magnitude.

□

2.3.3. *Consequences of data externalities: Inefficient equilibrium.* An individual's utility is affected by their sharing action and, crucially, by others' sharing actions as well. The externalities others create introduce a pathological problem. When an individual with a low privacy valuation, $j : v_j \leq 1, a_j = 1$, is correlated with an individual with a high privacy valuation, i, i.e., $I(T_i; A_j) \geq 0$, the equilibrium is inefficient (Acemoglu et al., 2019). This is because the externalities that j imposes on i by sharing makes i's data less valuable (as others have already revealed much of their data by their own sharing decisions) so they will tend to share, overlooking their original privacy preferences. There are other cases where the equilibrium is inefficient, the full analysis is in Acemoglu et al. (2019).

The next two sections do not solve this fundamental problem. Instead, they engage directly with the root cause, the existence of externalities, and offer alternative ways of implementing IPDM that are fairer and transparent.

3. Making Data Markets more Fair with Data Unions

In this section, we introduce data unions and study their effect in IPDMs.

3.1. **Introduction to Data Unions.** A data union is an intermediary between individuals and platforms. In an IPDM with unions, individuals never share their data with platforms directly, but with unions. Unions combine individuals' data and platforms pay data unions to access the data. After receiving the payment from the platform, unions redistribute the payment back to the individuals.

We claim that data unions, by capturing the externalities created by individual's sharing actions (by capturing data's combinatorial power) gain access to better data and thus obtain a higher payment from platforms. The net result is individuals receive a higher payment using unions than not. This is in stark contrast to today's data markets where the totality of data's combinatorial power is captured by platforms. We demonstrate the value of unions by finding the equilibrium price that platforms have to pay to obtain individuals' data when using Data Unions and comparing that price to the equilibrium price without unions.

3.2. **IPDM with Union: Analysis and Results.** **Setup.** There are n individuals partitioned into $U_1, U_2, ...U_u \in V$ unions; every individual is *represented* by one union. a_i is an individual's sharing decision. When $a_i = 1$ the individual shares with the union that represents them. a_u is a union's sharing decision. When a union shares data, it shares data from all individuals it represents with the platform. p_i is the price at which an individual shares in a IPDM without data unions, and p_u is the price at which a union shares, when considering IPDM with unions.

Platform's behavior. Whether with unions or without them, platforms' revenue streams depend on monetizing access to individuals' data (or services built off the data), to third-party organizations. It is not necessary to analyze how such monetization works in detail. However, we expect that platforms want to maintain their predictive power to continue monetizing access to that data, even when unions are introduced in the model. If they did not, their clients may move to other platforms with access to better predictive power. We show next that when the predictive power is the same, the social surplus, even with unions, is the same as well. This is an important insight that will let us analyze prices afterwards.

Claim 1: The social surplus with and without Data Unions is the same, i.e., $SS(\vec{a}) = SS_u(\vec{a})$. We use the following observation. Assume V individuals share data, with and without unions; this follows from the observation that platforms seek to maintain their predictive power to not lose clients. Then, after individuals share their data, the platform's predictive power is the same. In other words, in the social surplus expression (2.3), $SS(\vec{a}) = \sum_{i \in V} (1 - v_i) * I(T_i; D_{\vec{a}})$, the platform ends up with the same V's data with and without unions. Note that payments do not appear in the social surplus expression because they are an exchange between individuals and platform. This calls into question whether the prices change in a way that favors individuals or not. We turn our attention to analyze that question.

Equilibrium price with Unions. The price at which an individual shares *without* Data Unions is calculated by comparing the utility when an individual shares and when they do not (equation 2.1), and results in this expression:

$$p_i^{\vec{a}} = v_i(I(T_i; D_{\vec{a}}) - I(T_i; D_{\vec{a}_{-i}})) \tag{3.1}$$

The price reflects the marginal improvement in prediction performance the platform gains by having access to i's data scaled by the individual's privacy preference. The price is increasing with both v_i and with the marginal value of the individual's data[3], as per the difference of mutual information terms. In other words, the lower the information other individuals leak about an individual, the worse the prediction the platform will make and, consequently, the more valuable the individual's data becomes and the higher the platform will have to pay.

[3]We assume that platforms know v_i because we focus on the impact of unions and contextual integrity on IPDM; eliciting v_i is an orthogonal problem.

Let's use a_u to denote the union's sharing decision, analogously to an individuals'. In this case, if the union decides to share, it provides the platform with the data from every individual it represents. p_u is the price the platform pays the union to access that data and it is given by:

$$p_u = \sum_{k \in U} v_k * (I(T_k; D_{\vec{a}}) - I(T_k; D_{\vec{a}_{-u}}))$$

here we still consider each individual in the union, $k \in U$. When the union does not share, we discount the data contributed by all individuals in the union, which corresponds to the term $D_{\vec{a}_{-u}}$. Now we are ready to present the main result of this section.

Claim 2: Individuals receive a higher payment for their data when using Data Unions: $p_u \geq \sum_{i \in U} p_i$**.** Given a data union, U, we first calculate the total payments individuals represented by U would receive if they all shared their data *directly* with the platform instead of via the union, that is, if they all shared in an IPDM *without* data unions:

$$p_{i \in U} = \sum_{k \in U} v_k * (I(T_k; D_{\vec{a}}) - I(T_k; D_{\vec{a}_{-k}}))$$

Unlike in the p_u expression, here we discount the data each individual would share; this corresponds to the $I(T_k; D_{\vec{a}_{-k}})$ term. Then, to show that $p_u \geq \sum_{i \in U} p_i$, we use the expressions for p_u and p_i. Then, $I(T_k; D_{\vec{a}}) - I(T_k; D_{\vec{a}_{-u}}) \geq I(T_k; D_{\vec{a}}) - I(T_k; D_{\vec{a}_{-k}})$, which is equivalent to $I(T_k; D_{\vec{a}_{-u}}) \leq I(T_k; D_{\vec{a}_{-k}})$, where $D_{\vec{a}_{-u}}$ means the data from all individuals except for all individuals in the union and $D_{\vec{a}_{-k}}$ means all data except for one individual's data. Data's combinatorial value means that the combination of individuals' data is more valuable than the sum of each individual's data. The expression will only be equivalent when: i) the union represents only one individual k, or; ii) all individuals' represented by the union are uncorrelated with each other. Both conditions will be hard to find in practice: unions with only one individual do not make sense, and individuals' data is correlated. When those conditions are not true, platforms will have to pay a higher price to obtain data from a union than what they would pay to obtain data from each individual represented by that union, given they want to maintain their predictive power.

We now interpret the claim. Without unions, platforms capture all the externalities generated by individuals who share their data: platforms fully exploit data's combinatorial value. In contrast, when using unions, the union captures those externalities. Because the union captures data's combinatorial value, platforms need to pay higher to obtain that data, because it is more valuable than the sum of the individuals' data. Unions reallocate the price paid by the platform back to the individuals, and because that price is higher than what the individuals' would have obtained if they gave their data to platforms directly, they get a better deal when operating in IPDM markets with unions.

3.3. **Conclusion: Unions help Individuals Capture Data's Combinatorial Value.** Our analysis shows that the social surplus achieved in a IPDM with and without unions is the same. However, when using unions more of individuals' data is captured and the value derived (in the form of money in this case) is reallocated back to the individuals. This is in stark contrast with today's IPDM, where platforms capture and exploit the bulk of data's combinatorial power. Consequently, using unions make IPDMs fairer because individuals capture more of the value that stems from their data.

We note there are some downstream effects of using Unions that we do not analyze here. For example, if platforms' profit depends on services that require identifying concrete individuals (e.g., targeted advertising), then unions may reduce those gains as they sell a bundle of data from the

individuals they represent. When this individual targeting is necessary, the solution is to either let the union identify each individual's data, or let the platform target the union (e.g., customer segment), instead of specific individuals. Finally, unions may play diverse roles beyond capturing data's combinatorial value. For example, they could bundle individuals with similar v_i, or attempt to de-correlate certain individuals' data by using differential privacy (Dwork, 2006) and other techniques. These possible roles of unions are orthogonal to the main analysis of this paper and we do not discuss them further.

4. Making Data Markets transparent with Contextual Integrity

In this section, we study the implications of incorporating contextual integrity to IPDM.

4.1. The Role of Market Transparency on Individuals' Privacy and Primer on Contextual Integrity.

Today's IPDM markets adopt traditional definitions of privacy based on control or access over private data (Solove, 2005). Platforms communicate data collection practices to individuals via terms of service that indicate *what* data is retrieved. Empirical evidence suggests that individuals often ignore these terms of service (Obar & Oeldorf-Hirsch, 2020), not because they do not value privacy, but because of the large cost of interpreting the often inaccessible language (Strahilevitz & Kugler, 2016). Worse, even when individuals study the terms of service, they still have no way of telling whether platforms are honoring those because markets are not transparent: individuals cannot tell what platforms are doing with their data once they give it away. Finally, even if individuals could tell how their data is used, data externalities mean that one's privacy is not controlled exclusively by one's sharing decisions but by others' as well, as demonstrated earlier. With current definitions of privacy based on access or control IPDM markets cannot honor individuals' privacy.

Enter Contextual Integrity. A more adequate privacy definition is one that considers the *context* in which data is shared: *who* gets access to *what* data and *for what* purpose. The privacy theory of contextual integrity (CI) (Nissenbaum, 2004) determines that privacy is provided by *flows of information* that conform with *information norms*. The *information norms* depend on the context, which is determined by five parameters: i) *the data subject*, of whom the data refers to; ii) *sender*, who sends the subject's data iii) *receiver*, who receives the subject's data; iv) *information type*, that describes the data, and; v) *transmission principle*, that constrains the purpose and use of the data.

In an IPDM market, the data subject and sender correspond to the individual. The receiver corresponds to the platform and the information type is irrelevant. Next, we introduce transmission principles into the model, letting individuals choose how their data will be used by the platform.

Section Outline. We model IPDM if contextual integrity (`CI`) was implemented as the mechanism to handle privacy between individuals and platforms. We first analyze CI's effects on the model and then we conclude discussing when CI helps and interpreting the implications.

4.2. Model: IPDM Markets with Contextual Integrity.

In this section, we incorporate CI in the model (`CI`-IPDM) and present the main differences with Non-Contextual-Integrity IPDM, `NCI`-IPDM.

In a `CI`-IPDM, platforms declare a finite set of purposes for which they want to use individuals' data, $\mathcal{C}$. When individuals join the platform, they choose the purposes for which the platform is allowed to use the individual's data. For example, an individual joins a platform and decides to share data for purpose $c' \in \mathcal{C} : a^{c'} = 1$. Each purpose corresponds to a task or platform's internal goal, e.g., target advertising, recommending content, etc. Throughout this section, without loss of

generality, we will assume there are two purposes considered by the platform, c' and c''. This helps us simplify the expressions without sacrificing any insight.

4.2.1. *Effect of purposes on v_i, platform, and social surplus.* **Effect of purposes on individuals' v_i.** Individuals have different privacy preferences for each purpose, v_i^c, e.g., an individual i may be comfortable sharing data to receive better content recommendations, $v_i^{c'} = 0.5$ but may be uncomfortable if the platform sells their data to advertisers, $v_i^{c''} = 3$. This gained granularity of choice available in a `CI`-IPDM is not available without contextual integrity. Consider the individual of the example had to operate instead on a `NCI`-IPDM. This requires them to convey their privacy preferences ($v_i^{c'} = 0.5$, and $v_i^{c''} = 3$) into a single v_i. Averaging privacy preferences ensures the difference between the resulting v_i is closest to their true privacy preferences in the two underlying purposes. In this case, the individual's $v_i = (0.5 + 3)/2 = 1.75$, hence, they would decide not to join the platform, even though their true preference would be to join if the platform only used their data for purpose c', e.g., content recommendation.

Effect of purposes on the platform operation. Platforms aim to monetize access to data, as before. They try to predict the individual's type, T_i, with any data available to them. In particular, they can use individuals' data, $A_i^{c'}$, directly for purposes, $c' \in \mathcal{C} : a^{c'} = 1$, for which individuals shared. They cannot use the individual's data for other purposes, but they will leverage externalities caused by other sharing individuals to predict their type nevertheless, as before. Different purposes generate different revenue for the platform, e.g., advertising (c'') may be more profitable than engaging individuals with better recommendations (c'). We indicate the relative profitability of a purpose using the parameter $\delta^c \in [0, 1] \mid \sum_{c \in \mathcal{C}} \delta^c = 1$. Because of the different profitability, platforms will pay different prices to attract individuals to each purpose, $p_i = p_i^{c'} + p_i^{c''} = \delta^{c'} p_i + \delta^{c''} p_i$. Hence, with CI, the platform needs to buy the individual's data $|\mathcal{C}|$ times to match the prediction effect of NCI, i.e., to have access to the same individual's data on the same purposes. And the total price paid in that case is equivalent to what they would pay in `NCI`-IPDM, $\sum_{c \in C} p_i^c = p_i$.

Effect of purposes on the social surplus. If all individuals had the same sharing behavior in `NCI`-IPDM and `CI`-IPDM, then the social surplus would be the same, even though the contribution of each purpose may be different, $SS_{NCI} = SS_{CI} = \delta^{c'} SS_{CI}^{c'} + \delta^{c''} SS_{CI}^{c''}$. The parameter δ stems from the platform's ability to monetize data for a given purpose, and appears in the individual' and platform's utility functions, as we see next.

4.2.2. *Effect of CI on individual's utility and social surplus.* **Changes to individual's utility.** The individual's utility under CI is as follows:

$$u_i(a_i, \vec{a}^c_{-i}, \vec{p}) = \begin{cases} \sum_{c \in \mathcal{C}^+} \delta^c p_i - \sum_{c \in \mathcal{C}^+} \delta^c v_i^c I(T_i; D^c_{\vec{a}}) & \text{if } a_i = 1, \\ -\sum_{c \in \mathcal{C}^-} \delta^c v_i^c I(T_i; D^c_{\vec{a}_{-i}}) & \text{if } a_i = 0 \end{cases} \tag{4.1}$$

where $\mathcal{C}^+$ is the subset of $\mathcal{C}$ where individuals decide to share, i.e., $\mathcal{C}^+ = \{c \in \mathcal{C} \mid a_i^c = 1\}$, and $\mathcal{C}^-$ indicates those where they do not share. The price the platform pays an individual to share in all $c \in \mathcal{C}$, $p_i = \delta^{c'} p_i + \delta^{c''} p_i$, is as follows:

$$p_i^{\vec{a}} = \delta^{c'} v_i^{c'} [I(T_i; D^{c'}_{\vec{a}}) - I(T_i; D^{c'}_{\vec{a}_{-i}})] + \delta^{c''} v_i^{c''} [I(T_i; D^{c''}_{\vec{a}}) - I(T_i; D^{c''}_{\vec{a}_{-i}})] \tag{4.2}$$

We cannot compare the utility and price expressions between `CI` and `NCI` because the information leakage depends on individuals' sharing behavior, which in turn, is different in NCI than in CI. For example, an individual with $v_i = 0.8$ in `NCI` shares in equilibrium, but that privacy value may

correspond to $v_i^{c'} = 0.4, v_i^{c''} = 1.2$ in CI, which corresponds to sharing for one purpose but not for the other. Similarly, a strong preference for not sharing in CI may result in sharing for a purpose in NCI.

Changes to social surplus. Armed with the individual's and platform's utility (which we can derive as above), social surplus under CI is:

$$SS_{CI}(\vec{a}) = \delta^{c'} \sum_{i \in V} (1 - v_i^{c'}) I(T_i; D_{\vec{a}}^{c'}) + \delta^{c''} \sum_{i \in V} (1 - v_i^{c''}) I(T_i; D_{\vec{a}}^{c''}) \tag{4.3}$$

and then we can use a similar analysis to the one used in Proposition 1 to derive the expression that tells us, for an individual i, when the best action is sharing in CI. If we consider the case *without* externalities, then the inequality is:

$$(1 - v_i^{c'}) I(T_i; A_i^{c'}) + (1 - v_i^{c''}) I(T_i; A_i^{c''}) \geq 0 \tag{4.4}$$

In this case, the expression reflects both purposes. There is a subtle but important difference with respect to the NCI case. Even without externalities, an individual with $v_i^{c'} \geq 1$ may still share in equilibrium if the utility gained on c'' compensates the lost in c', and, similarly, an individual with $v_i^{c'} < 1$ may not want to share. In summary, individuals will not share when both $v_i^{c'}$ and $v_i^{c''}$ are larger than 1. Otherwise, their action will depend on the specific magnitude of the leak, which in turn depends on other individuals' sharing behavior. Finally, similar to the NCI case, when there are externalities, the optimal sharing behavior depends on the harm caused to others, so the equilibrium remains inefficient.

4.3. **When and How does Contextual Integrity help?** We concentrate on the three parameters that govern the equations for NCI and CI: δ, v_i, and the sharing behavior via its mutual information term, $I(T_i; D_{\vec{a}}^c)$. We pay attention to three pairs of equations, for social surplus, equilibrium payments, and sharing inequalities.

Claim 2: CI improves social surplus, or individuals obtain a better compensation for their data, or both social surplus and prices remain the same, but SS and prices cannot be simultaneously worse than in NCI.

We show the claim is true by contradiction. Assume $SS_{CI} < SS_{NCI}$ and $p_i^{CI} < p_i$ (we use equations 4.3, 2.3, 4.2 and 3.1, respectively). We know $v_i = 1/2(v_i^{c'} + v_i^{c''})$ and $\delta^{c'} = 1 - \delta^{c''}$. We start with social surplus. When $\delta^{c'} = 0.5$ or $v_i^{c'} = v_i^{c''} = v_i$, then both sides are weighted the same and $SS_{CI} = SS_{NCI}$. The inequality is true if $\delta^{c'} > 0.5$ and $v_i^{c'} > v_i$ or $\delta^{c''} > 0.5$ and $v_i^{c''} > v_i$. Now we consider the price expressions. The inequality is true when $\delta^{c'} \leq 0.5$ and $v_i^{c'} > v_i$ or $\delta^{c''} \leq 0.5$ and $v_i^{c''} > v_i$.

Hence, $SS_{CI} \leq SS_{NCI}$ only if $\delta^{c'} > 0.5$ and $v_i^{c'} > v_i$ and $p_i^{CI} \leq p_i$ only if $\delta^{c'} > 0.5$ and $v_i^{c'} < v_i$, i.e., this requires $v_i^{c'} > v_i$ and $v_i^{c'} < v_i$ simultaneously, thus exposing the contradiction.

Claim 3: Magnitude of error, $|v_i - v_i^c|$, accentuates the trends of claim 3. We know that $SS_{CI} \neq SS_{NCI}$ when $v_i^{c'} \neq v_i$, or $\delta^{c'} \neq 0.5$, or both. The difference in social surplus is related to $|v_i - v_i^{c'}|$, which we call the aggregation error as the larger it is, the worse the aggregation of privacy preferences in NCI represents the individual's real privacy preferences in CI. Showing this is the case is straightforward. Assume some $\delta^{c'} \neq 0.5$. In both the social surplus and price equations, $v_i^{c'}$ multiplies $\delta^{c'}$, which is fixed. The impact on those expressions will then grow according to $|v_i - v_i^{c'}|$.

4.4. **Summary and Broader Interpretation.** Claim 3 states that when using contextual integrity, the social surplus is higher than when not, or, at least, individuals are better compensated

for their privacy violation. Claim 4 explains that the difference between social surplus (prices) is proportional to the difference between the privacy preferences for a purpose and the average. That is, the higher the differences between individuals' preferences for different purposes, the higher the impact of using contextual integrity. To illustrate this, consider two individuals, i, j, with $v_i = v_j = 1$ in `NCI`, but with preferences $v_i^{c'} = 0.2, v_i^{c''} = 1.8$ and $v_j^{c'} = 0.9, v_j^{c''} = 1.1$, clearly individual i's decision is harder than j's from a privacy preservation perspective, and this shows in the IPDM market model.

Consider a population where most individuals are uncomfortable sharing data with a platform for the purposes of ad targeting, but are perfectly fine sharing data in exchange for the service. Say that, at the same time, the platform's main business model and revenue stream comes from ad targeting. To obtain data from individuals, the platform will have to pay high prices, reducing its revenue. A better alternative may be to find other business models that are aligned with the population's preferences. Contextual integrity requires the market to be transparent and, by providing individuals with more choice, gives them more power. The consequence is that platforms that wish to use individual's data to profit, must ensure the purposes for which they use that data are aligned with individual's preferences.

5. Towards Bridging the Practice-Theory Gap: The Data Station Architecture

In this section, we explore the requirements of a software platform that implements unions and contextual integrity. Then, we present a proposal, the Data Station, that fulfills those requirements. This section is our effort towards making the ideas presented in the model concrete and implementable in practice.

5.1. The Data Infrastructure Behind Today's Platforms.

Today's IPDMs use a variety of software to use individuals' data for profit and to provide services to those individuals. Although so far we have not explained what it means for a platform to have an individual's data, we must discuss this to make progress. We differentiate the *logical* and a *physical* view of data. The *logical* view corresponds to the conceptual attributes associated to each individual and the values for those attributes. The *physical* view corresponds to how are the values for those attributes represented, i.e., in what formats, and how they are stored. While there is only one *logical* view of an individual's data, there will be multiple *physical* views of the same data. There are many reasons for the multiplicity of *physical* views. For example, data may be replicated so it cannot be lost in case of a hardware failure. It exists in different formats and is stored in specialized systems that cater for different services and querying needs. Finally, it may be incorporated in machine learning models and other derived data products such as reports and aggregates.

We now explain the downsides of today's IPDMs from the software angle:

C1. Individuals have incomplete knowledge about what data platforms possess about them. Some attributes in the *logical* view of an individual's data are provided directly by them, e.g., email address and phone number for signing up, shared pictures, etc. Other attributes are collected by the platform in a way that is transparent to the individual, such as the IP address from where the individual connects[4], the time of day, locale, and more. Finally, other attributes are computed by platforms based on other individual's data and external knowledge, such as socioeconomic status (based on restaurants visited, products purchased, etc), movie preferences, and

[4]The Internet Protocol (IP) address reveals information about the location from where the connection is established

more. While individuals may know the data they provide directly, it is harder to be aware of all other attributes collected by the platform.

C2. Individuals cannot tell how platforms use their data. The myriad of *physical* view representations of data that organizations possess means that not even platforms have full control of an individual's data: no single individual will know in general the data's full lifecycle. Gathering all data corresponding to an individual when requested is a non-trivial task, as many efforts to support GDPR—that requires platforms to delete an individual's data on request—demonstrate (Politou et al., 2018). All this (many times necessary) complexity means that it is hard to determine how an individual's data is used at any given point in time, even when platforms are honest.

We now discuss the requirements of unions and contextual integrity.

5.2. **Requirements of Data Unions.** Individuals trust their data to the union and the union negotiates with platforms on behalf of individuals. This introduces several requirements of a software implementation of a data union as presented in this paper:

R1. Trustworthy intermediary. Individuals must trust the union's mission and that they will keep data (at least) as safe as platforms do today. Platforms must trust that the union is honest and that it trades real individual's data.

R2. Explicit Logical View. With unions, platforms cannot collect data directly from individuals. Instead, they must indicate concretely the *logical* dataset they need, so the union can collect that data on their behalf. And because the union works for individuals, they know precisely what attributes and data is being collected. This endows the market with transparency, addressing **C1**.

R3. Data Collection. Individuals need to explicitly share the logical dataset with the union, unlike today, where they only share a few attributes (e.g., email, password) and the rest is automatically collected. This may become cumbersome for some individuals. To workaround this issue, unions must have the same capacity to collect data that platforms have today. The difference is that unions work strictly on behalf of individuals' interests: only data that individuals explicitly allow is shared by the union with the platform.

5.3. **Requirements of Contextual Integrity.** We now turn our attention to the requirements induced by the integration of contextual integrity.

R4. Transparent purposes. Platforms must describe the purposes for which they will use individual's data. Individuals must be able to understand and choose among those.

R5. Enforce purpose execution. The main challenge is to enforce that platforms only use data for the purposes accepted by individuals. Consider a platform that declares two purposes, c_1 and c_2. Individuals agree on exchanging the data for a service in c_1. Once the data gets to the platform, what prevents the platform from using that data in c_2? Even if the platform is not trying to cheat, the complex data lifecyles in organizations mean data may leak from c_1 into c_2, making the enforcement of this contract between individual and platform hard. A requirement of a system implementing CI is that it can enforce platforms to use data only for the purposes allowed.

5.4. **Data Station: A System Architecture to Implement Unions and Contextual Integrity on IPDMs.** We present a system architecture to implement data unions and contextual integrity. We call systems that implement this architecture data stations. An diagram is shown in Figure 1 (right) in contrast to today's design (left).

First, to implement unions, data shared with the station is sealed by default and only the sharer can control, with fine-granularity, who can access the logical view of that data (addresses **C1** and **R2**). This guarantee means that individuals sharing data can think of the station as an extension of

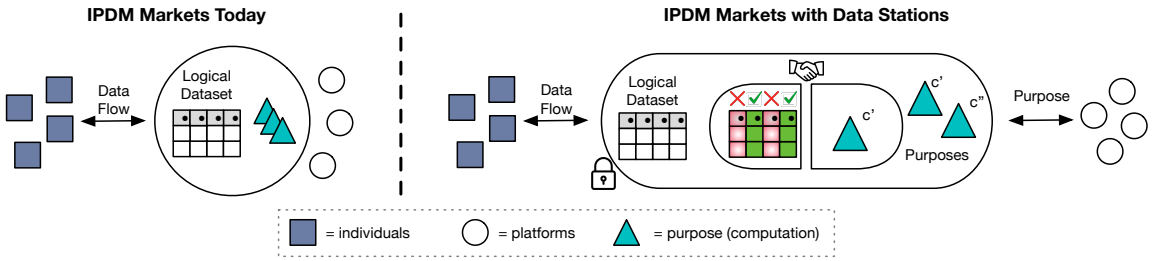

Figure 1. Illustration of data flow in IPDM markets today (left) and when using Data Stations (right).

their own infrastructure, and they can permit the station to collect data on their behalf (addresses **R3**).

Second, to implement contextual integrity, data stations must ensure that platforms only use data for the purposes agreed upon with individuals (as per **R5**). Data Stations achieve this by owning *data processing* and hence becoming responsible for executing programs on behalf of the platforms. What this means is that individuals' data never makes it into the platforms infrastructure. Instead, the platforms' programs are transferred to the data station where they execute. With this design, the data station can ensure that only programs representing purposes (e.g., a recommendation algorithm to provide better content) that individuals agreed on sharing the data with, run on that individual's data (addresses **R5**). Data Stations provide platforms with so-called *data-blind interfaces* that permit write computation without having to look at the data first. Data-blind interfaces may include techniques such as synthetic data generation, as well as inverted interfaces such as search and query-by-example (Zloof, 1977). This permits platforms to develop programs without requiring access to (real) individuals' data and declaring the purposes for which they plan to use individuals' data (addressing **C2** and **R4**).

For all this to work, data stations must be trustworthy (addressing **R1**). First, individuals trust their data to the station and must believe they fulfill the mission and that their data will be as secured as in today's platforms. Second, platforms share their oftentimes proprietary code. Confidential computing technology that includes secure hardware enclaves means that it becomes possible to work on private data while ensuring the customers their data is secure.

Finally, data stations bring additional benefits:

- Using data stations permits individuals and platforms to be aware of each data transaction, this may result in individuals adjusting their v_i with better information and platform calibrating their requests for individual data.
- Data stations incentivize all parties to standardize data to achieve portability, easing the transmission of data and ameliorating the challenging data integration problem (Doan et al., 2012).
- By logically centralizing data and compute, data stations are auditable. This helps individuals build more trust by ensuring the station is using their data in the pre-negotiated way. Crucially, this lets third parties inspect how data is being used and determine whether the transactions are appropriate.

Implementing a Data Station is a major research and development effort. But many academic communities are working on the challenges this involves, including confidential computing, data-blind interfaces, computing on synthetic and anonymized data—to permit platforms develop their programs—and more. Thus, although a major challenge, current technology suggests there is a path towards practical implementations of this platform.

6. Related Work

There are many efforts and initiatives that have explored similar problems and similar technologies to those presented in this paper. Next, we frame them in the context of our contributions.

Combating lack of fairness and transparency. Many efforts recognize the problems of fairness and lack of transparency of today's data-driven companies: i) balance platform-individual power, such as using "data strikes" (Vincent et al., 2021); ii) regulate the market to ensure increased transparency (Wagner et al., 2020); iii) react to the excessive data collection from platforms by poisoining or obfuscating the data delivered (Brunton & Nissenbaum, 2015). These efforts are aligned with the goals of this paper. First, we envision ways of incorporating "data strikes" in the context of the IPDM model we used to study unions and contextual integrity. Second, regulatory action may open up opportunities to enact some of the interventions we studied. Third, we could integrate obfuscation into our IPDM model by breaking the assumption that the data individuals provide is truthful. We believe that although orthogonal than our contribution, the model we present can be a starting point to study these otherwise goal-aligned initiatives.

Individual Platform Data Markets. Prior work has discussed the existence and consequences of data externalities generated by individuals' data (Acemoglu et al., 2019; Bergemann et al., 2020; Choi et al., 2019). We follow the structure of the IPDM model presented in Acemoglu et al. (2019), but using our formulation based on information theory to simplify the presentation and to extend our results to the analysis of unions and contextual integrity. In Bergemann et al. (2020) the authors present a data market model for the data broker industry. In that model, the intermediary is different than the one proposed in our paper: its role is to decide what data to buy from individuals and how to sell it to both the platform and to other consumers. The insights derived in this work are different and complementary.

Unions. Concepts similar to what we refer to as data unions in this paper are data cooperatives, commons, collaboratives, trust, fiduciary, and even marketplace and data futures ("Exploring legal mechanisms for data stewardship", 2021; "Mozilla Research. Shifting power through data governance", 2021). Most of these proposals focus on the governance of data in the context of IPDMs. Thedataunion.org ("The Data Union", 2022) proposes to treat data as labor to compensate individuals when their data is used. There are no technical details in their web, but the idea stems from Posner and Weyl (2019), where the authors explain how an intermediary could absorb the externalities produced by individuals and compensate them for their data. This is the insight we use in our paper. But we complement this idea by providing concrete analytical evidence of the benefits of unions. In datatrusts.uk ("Data Trusts", 2022; Delacroix & Lawrence, 2019) the authors detail how current (legal) contractual mechanisms lack the necessary features to enforce individual's data rights and propose a legal mechanism to enforce them, a data trust.. Our work is complementary and offers an analysis and technical justification of the benefits these ideas have in terms of utility and social welfare, and it paves the way towards their technical implementation.

Contextual Integrity. The theory of contextual integrity (Nissenbaum, 2004) "ties adequate protection for privacy to norms of specific contexts". We modeled these contexts as different purposes in this work, which correspond to the transmission principles the theory develops. Several studies have considered how to apply contextual integrity in practice (Benthall et al., 2017), including how to represent norms digitally (Barth et al., 2006), and how to incorporate the theory as part of already existing access control mechanisms used in computing systems (Ni et al., 2010). And more recently, some work focuses on potential uses of contextual integrity to permit organizations to use data hosted by large companies and extract value. This has been applied to, for example,

health research (Marelli et al., 2021; Winter & Davidson, 2019), and contact-tracing (Martens et al., 2021). We are not aware of studies that aim to understand the effect of contextual integrity on data markets.

Platforms to give individuals control of their data. In Hardjono and Pentland (2019), the authors propose using credit unions to implement data unions. Credit unions are non-profit organizations already trusted by millions of individuals, and already recognized in the legal system of many countries. The framework proposed in this work uses the idea of pushing algorithms to the platform, so the data does not need to leave the platform for it to yield value. Although similar in philosophy to our proposal, this one does not contain a list of requirements and challenges to solve, and the work does not focus on the value that such a union brings to individuals, or the benefits on transparency provided by CI.

Another effort is the Transportation Data Collaborative (Young et al., 2019) aimed to release synthetic datasets from which researchers can extract value even when the original data is proprietary and cannot be made transparent. The paper explains how centralization of data brings benefits to control how to release data. They explain a desiderata for such a platform, both technical, like ours, and legal, which we do not address in our work. Instead, we concentrate in the role that unions and contextual integrity play in the utility of individuals, the general social welfare, and in making data markets fairer and more transparent.

Orthogonal to the above, in the software systems community there is a plethora of work that focuses on providing secure access to data from remote platforms (Hu et al., 2020; Shafagh et al., 2017; Wang et al., 2016; Zheng et al., 2021). This is a requirement to implement Data Stations. This literature uses techniques from cryptography, hardware enclaves, and more to facilitate sharing. Sometimes, it provides some limited computation. As far as we know there is not a full solution to the problem presented here.

7. Discussion and Conclusions

In response to what the author considers a broken individual-platform data market, this paper makes 3 contributions. The first two are the analysis of data unions and contextual integrity that describe the advantages and impact of such ideas in data markets. Data unions make IPDM markets fairer because they capture data's externalities for individuals. Contextual integrity forces IPDM to be more transparent and permits individuals more fine-grained control over how their data is used, leading to better privacy guarantees. The third contribution of the paper is the blueprint of a system that brings those ideas a step closer to a practical implementation.

At a time where new antitrust law is actively discussed in the US where big tech companies have amassed a huge amount of power, this work brings attention to what makes many of these companies valuable, individual's data. If individuals' could share their data with multiple platforms and the platforms compete on the services offered, instead of today's hoarding and exploitation, it is conceivable that the result would be a more competitive environment. The converse is clear, platforms that first amass individuals' data acquire a disproportionate power that requires incumbent challengers to re-acquire that data to compete effectively. This brings an unnecessary loss in individuals' privacy.

This work is a first step towards redesigning IPDM markets in a way that is more respectful to individuals. There are many limitations. First, the model we use necessarily makes assumptions so we can analyze and provide insights. We believe the conclusions we observe are robust to the assumptions we made, but refinements on the model will be necessary to understand alternative designs before incurring large implementation costs. Data Stations are a step towards the technical

implementation of unions and contextual integrity, but many other technical problems remain. And technical problems are only a small part of a larger picture that requires legal mechanisms and perhaps new institutions. The related work presented current efforts on the design of legal institutions geared towards addressing similar problems presented here. The work we presented is the first to analyze the impact of unions and contextual integrity on individuals' and platforms' utility.

Disclosure Statement. The authors have no conflicts of interest to declare.

References

Acemoglu, D., Makhdoumi, A., Malekian, A., & Ozdaglar, A. (2019). *Too much data: Prices and inefficiencies in data markets* (tech. rep.). National Bureau of Economic Research.

Exploring legal mechanisms for data stewardship [https://www.adalovelaceinstitute.org/summary/exploring-legal-mechanisms-data-stewardship/]. (2021).

Anderson, J., & Mariniello, M. (2021). Regulating big tech: The digital markets act. *Bruegel-Blogs*.

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. *2006 IEEE symposium on security and privacy (S&P'06)*, 15–pp.

Benthall, S., Gürses, S., Nissenbaum, H., et al. (2017). *Contextual integrity through the lens of computer science*. Now Publishers.

Bergemann, D., Bonatti, A., & Gan, T. (2020). The economics of social data.

Brunton, F., & Nissenbaum, H. (2015). *Obfuscation: A user's guide for privacy and protest*. Mit Press.

Choi, J. P., Jeon, D.-S., & Kim, B.-C. (2019). Privacy and personal data collection with information externalities. *Journal of Public Economics*, *173*, 113–124.

Mozilla research. shifting power through data governance [https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/shifting-power-through-data-governance/]. (2021).

Data dividend, my data, my money [https://www.datadividendproject.com/]. (2021).

Data trusts [https://datatrusts.uk/]. (2022).

The data union [https://www.thedataunion.org/]. (2022).

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of computer-mediated communication*, *15*(1), 83–108.

Delacroix, S., & Lawrence, N. D. (2019). Bottom-up data trusts: Disturbing the 'one size fits all'approach to data governance. *International data privacy law*, *9*(4), 236–252.

Doan, A., Halevy, A., & Ives, Z. (2012). *Principles of data integration*. Elsevier.

Dwork, C. (2006). Differential privacy. In M. Bugliesi, B. Preneel, V. Sassone, & I. Wegener (Eds.), *Automata, languages and programming* (pp. 1–12). Springer Berlin Heidelberg.

Facebook data collection privacy [https://www.facebook.com/policy.php]. (2021).

Goldfarb, A. (2014). What is different about online advertising? *Review of Industrial Organization*, *44*(2), 115–129.

Gomez-Uribe, C. A., & Hunt, N. (2015). The netflix recommender system: Algorithms, business value, and innovation. *ACM Transactions on Management Information Systems (TMIS)*, *6*(4), 1–19.

Google data collection privacy [https://policies.google.com/privacy?hl=en-US]. (2021).

Hardjono, T., & Pentland, A. (2019). Data cooperatives: Towards a foundation for decentralized personal data management. *arXiv preprint arXiv:1905.08819*.

Hu, Y., Kumar, S., & Popa, R. A. (2020). Ghostor: Toward a secure data-sharing system from decentralized trust. *17th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 20)*, 851–877.

Malmi, E., & Weber, I. (2016). You are what apps you use: Demographic prediction based on user's apps. *Proceedings of the International AAAI Conference on Web and Social Media*, *10*(1).

Marelli, L., Testa, G., & Hoyweghen, I. v. (2021). Big tech platforms in health research: Re-purposing big data governance in light of the general data protection regulation's research exemption. *Big Data & Society*, *8*(1), 20539517211018783.

Martens, M., De Wolf, R., Vadendriessche, K., Evens, T., & De Marez, L. (2021). Applying contextual integrity to digital contact tracing and automated triage for hospitals during covid-19. *Technology in Society*, *67*, 101748.

Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C.-M., Karat, J., & Trombeta, A. (2010). Privacy-aware role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, *13*(3), 1–31.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, *79*, 119.

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128–147.

Oura data collection privacy [https://support.ouraring.com/hc/en-us/articles/360025586673-How-Oura-Protects-Your-Data]. (2021).

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the gdpr: An uneasy relationship. *Computer Law & Security Review*, *34*(6), 1247–1257.

Posner, E. A., & Weyl, E. G. (2019). *Radical markets*. Princeton University Press.

Sanna Passino, F., Maystre, L., Moor, D., Anderson, A., & Lalmas, M. (2021). Where to next? a dynamic model of user preferences. *Proceedings of the Web Conference 2021*, 3210–3220.

Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017). Towards blockchain-based auditable storage and sharing of iot data. *Proceedings of the 2017 on cloud computing security workshop*, 45–50.

Smith, B., & Linden, G. (2017). Two decades of recommender systems at amazon. com. *Ieee internet computing*, *21*(3), 12–18.

Solove, D. J. (2005). A taxonomy of privacy. *U. Pa. L. Rev.*, *154*, 477.

Spotify data collection privacy [https://www.spotify.com/us/privacy]. (2021).

Strahilevitz, L. J., & Kugler, M. B. (2016). Is privacy policy language irrelevant to consumers? *The Journal of Legal Studies*, *45*(S2), S69–S95.

Twitter data collection privacy [https://twitter.com/en/privacy]. (2021).

Varian, H. R. (2007). Position auctions. *international Journal of industrial Organization*, *25*(6), 1163–1178.

Vincent, N., Li, H., Tilly, N., Chancellor, S., & Hecht, B. (2021). Data leverage: A framework for empowering the public in its relationship with technology companies. *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 215–227.

Wagner, B., Rozgonyi, K., Sekwenz, M.-T., Cobbe, J., & Singh, J. (2020). Regulating transparency? facebook, twitter and the german network enforcement act. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 261–271.

Wang, F., Mickens, J., Zeldovich, N., & Vaikuntanathan, V. (2016). Sieve: Cryptographically enforced access control for user data in untrusted clouds. *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*, 611–626.

Winter, J. S., & Davidson, E. (2019). Big data governance of personal health information and challenges to contextual integrity. *The Information Society*, *35*(1), 36–51.

Personal data is worth billions, these startups want you to get a cut [https://www.wsj.com/articles/personal-data-is-worth-billions-these-startups-want-you-to-get-a-cut-11638633640?mod=foesummaries]. (2021).

Young, M., Rodriguez, L., Keller, E., Sun, F., Sa, B., Whittington, J., & Howe, B. (2019). Beyond open vs. closed: Balancing individual privacy and public accountability in data sharing. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 191–200.

Zheng, W., Deng, R., Chen, W., Popa, R. A., Panda, A., & Stoica, I. (2021). Cerebro: A platform for multi-party cryptographic collaborative learning. *30th {USENIX} Security Symposium ({USENIX} Security 21)*.

Zloof, M. M. (1977). Query-by-example: A data base language. *IBM systems Journal*, *16*(4), 324–343.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.