Data on Internet Platforms

Genaro Basulto
Ph.D Student
Tepper School of Business, Carnegie Mellon University
&
Aniko Öry
Associate Professor of Economics
Tepper School of Business, Carnegie Mellon University

1 Introduction.

Most markets involve two types of information asymmetries: consumers possess private information about their product preferences, while firms have private information about their products, such as quality or product uses. This information is valuable for the opposite party: product information helps consumers buy their preferred product, and knowing consumer preferences helps firms to develop better products and improve pricing strategies. Internet platforms, such as search engines, social networks, and retail marketplaces create value by collecting and aggregating growing volumes of consumer information, acting as information intermediaries.

Determining the social value of data and a "fair" allocation of surplus is challenging for several reasons. First, one consumer's data can have both positive and negative externalities on other consumers and market participants. Second, from a consumer's perspective, data collection oftentimes occurs in the background of a more prominent activity, and data intermediaries may not fully protect the privacy of consumers. Third, the surplus generated by data intermediaries does not benefit all market participants equally because the allocation of surplus is driven by market structure. In highly competitive markets, consumers might benefit more from enhanced information flow, whereas in markets dominated by a few large data intermediaries or firms, these entities might capture a larger share of the surplus. Importantly this affects the profitablity of internet platforms, for whom data is at the center of their business model. At the same time, market power of intermediaries results in consumers frequently bearing the costs of their data being shared, as they receive little or no compensation for it.

We identify three main problems within the current landscape of data in the platform economy. First, increasing market power of data intermediaries allows them to capture most of the surplus from data sharing, limiting the benefits for consumers and other participants such as advertisers. Second, consumers lack control over their personal information, and inadequate safeguarding measures lead to privacy concerns and potential data breaches. Third, small and medium-sized companies are struggling to keep up with the rapid pace of technological advancements, largely due to the fragmentation of consumer information from multiple intermediaries, which prevents them from fully leveraging the abundance of data available on the Internet.

Distributed Ledger Technologies (DLTs) can be used for the creation and operation of a database while ensuring anonymity of the people contributing to the database. Specifically, the data are replicated across multiple storage devices with equal rights using cryptography. This technology has the potential to address the previously mentioned problems with the current system. If consumer data generated from Internet activity is stored in a distributed ledger, market power of intermediaries may be reduced by giving consumers greater control over their information, and allowing them to get a fair price for it. Furthermore, the technology allows for anonymity, potentially lowering the risks of privacy breaches. Finally, a DLT might help small and medium-sized companies by providing access to a central data source with reliable and verifiable consumer information.

The remainder of the paper is organized as follows. In Section II, we explore the value of data, considering its dynamic characteristics and the externalities users impose on one another. In Section III, we delve deeper into the three identified problems, presenting both the relevant economic literature and real-world examples that illustrate how current data management schemes have been problematic. We analyze the economic implications of the increasing market power of data intermediaries, the lack of consumer control over personal information, and the challenges faced by small and medium-sized companies due to fragmented data sources. In Section IV, we explore the different methods of data storage, detailing the advantages and caveats of distributed ledger technologies (DLTs). We compare traditional centralized data storage methods with decentralized approaches, highlighting the potential benefits and limitations of DLTs in terms of security, transparency, and scalability. Section V proposes various ways in which DLTs could improve the current landscape of the market. We discuss potential solutions that DLTs could offer to mitigate the power of data intermediaries, enhance consumer control and data security, and provide small and medium-sized companies with more organized and accurate data sources. We conclude in Section VI.

2 The Value of Data

As stated in the introduction, asymmetric information makes various types of data valuable to different players: consumers typically have private information about their product preferences, and firms may have private information about their products. Consumers' willingness to disclose information in online markets hinges on a fundamental trade-off. On the one hand, providing precise product information or incorporating recommendation systems helps match consumers with better-suited products (4). On the other hand, this disclosure can enable sellers to extract more surplus by charging higher prices for all products, as consumers self-select to purchase the items they value most. So, data can allow firms to engage in third degree price discrimination (9).[1] Consider, for instance, an expecting parent searching for baby products on a retail platform. If the platform has sufficient information, it might recommend products that have been proven useful to other parents, which benefits the consumer. However, this same information also grants

[1]Third degree price discrimination is a pricing strategy where a firm charges different prices to different consumer segments based on information about consumer characteristics.

sellers the opportunity to potentially charge higher prices than they would otherwise, knowing that consumers who see the product are more likely to be interested in it.

One key insight from the former example is that the information captured by internet platforms facilitates better matching between consumers and products, enhancing overall market efficiency. However, it also redistributes the surplus generated during the transactions that occur between firms, consumers, and platforms, potentially leading to market distortions. The allocation of surplus is influenced by the market structure: In highly competitive markets, consumers might benefit more from enhanced information flow because firms cannot significantly increase prices. In contrast, in markets dominated by a few large firms or platforms, these entities might capture a larger share of the surplus due to increased market power. At the same time, positive data externalities and economies of scale might result in intermediaries effectively being natural monopolies. Ultimately, the balance of power in the market determines who reaps the benefits of reduced information asymmetry and the degree of market distortions.

In practice, placing a "fair" or efficient price on personal data is a complex issue because each market participant experiences different benefits and costs from sharing their data, which raises questions about its true value. For platforms, trading data is fundamental to their transactions. However, for users, exchanging personal data is often a secondary and invisible part of a more prominent transaction, such as conducting a search or interacting on a social network. The widespread collection of online data introduces significant externalities for consumers, as data from one set of users can provide insights about others (see e.g., (1, 11)). This implies that when platforms already have millions of observations of consumer behavior, the marginal contribution of a new user's data diminishes. Consequently, platforms only need to compensate consumers for their marginal contribution, which might result in near-zero compensation for individual users. Nonetheless, consumers should still assign a positive value to their data due to the potential for facing higher prices. Due to the central role of platforms, in practice, consumers often receive minimal compensation for their information (5).

Individuals may benefit from others sharing their information, such as through reviews, but they can also incur costs if the shared information is used to predict their own reservation price as shown by (10). Therefore, the personal costs and ability to protect one's information depend on the disclosure choices made by others. Furthermore, as more people reveal information about themselves, the cost of protecting one's data increases, while the potential compensation received for it decreases. Additionally, the value of information can change over time; what is valuable today may become obsolete tomorrow. For example, a user's purchase information from five years ago has no value to an advertiser compared to a purchase that happened a couple hours ago. The trade-offs involved in data sharing are often inter-temporal and blend tangible and intangible aspects, as the cost of sharing may be deferred to a distant future point, i.e. the moment of a purchase in the future (2).

The value of information is also not a straigthforward concept because data does not only play an instrumental role in economic transactions, but information and privacy is valued by customers for its own sake and personal reasons (4, 14, 21). This dual nature of privacy highlights its mul-

tifaceted importance in the digital age. The challenge lies in balancing the immediate benefits of sharing data with the potential long-term costs, both for individuals and for society as a whole when evaluating the true value of data.

3 Data in the Platform Economy.

3.1 Market Power of Platforms.

Given the current technology, data collection on the Internet has become increasingly cheaper, enabling large digital platforms such as Amazon, Google, and Facebook to effortlessly capture, aggregate, and capitalize on relevant information about consumers and firms. These mechanisms pose new challenges related to privacy, the market power of information intermediaries, and the potential for distortions in both the information and retail sectors (9). Data collection methods, such as tracking traffic flow, mining publicly available data, and monitoring social network activity, often operate obscurely, generating and capturing digital trails of personal activities that previously left little to no trace (2). Intermediaries profit by controlling access to and the quality of information, wielding significant market power, and influencing demand segmentation and welfare allocation (25, 8). They manage the tracking and linking of user behaviors across various platforms and services, often without the users' knowledge or consent.

Following the frameworks proposed by (4) and the (20), we can categorize two types of mechanisms for selling data: direct and indirect sales of information. In direct sales, data intermediaries grant direct access to a fraction of consumer information to interested parties. This means that buyers obtain raw data that they can analyze and use according to their needs. In indirect sales, the data itself is never transferred; instead, the data intermediary uses the information to make informed decisions on behalf of the interested party. For example, platforms often utilize indirect sales by selling advertising space to businesses targeting specific consumer demographics without actually sharing the raw data with these businesses. In this capacity, digital platforms act as market makers, overseeing the collection, aggregation, and dissemination of consumer information to advertisers and then feeding back the results to users. This intermediary role allows platforms to control the flow of information and maintain a central position as 'gatekeepers' in the data economy, which grants the platforms significant market power (7).

The tendency for data intermediaries to become natural monopolies arises from several other factors. First, data collection and processing involve significant fixed costs but relatively low marginal costs, creating economies of scale that favor large platforms. Once established, these platforms benefit from network effects: as more users join and generate data, the value of the platform increases, attracting even more users in a self-reinforcing cycle (30, 9). Additionally, data intermediaries benefit from economies of scope, as data collected for one purpose can often be repurposed for another, further enhancing their market power. Economic research suggests that platforms are capable of capturing most of the welfare generated by information sharing in these markets and that they can generate positive profits by selling information, even if this

reduces overall surplus (see, e.g., (24, 11, 1)). Furthermore, they can restrict access to information and introduce noise to increase their own surplus even if that decreases overall market efficiency (3, 10). The capture of all surplus by these platforms is not always guaranteed and can depend on several factors such as the degree of competition, regulatory environment, and technological changes. This is an area of ongoing research, and while some scholars argue that platforms tend to capture most of the surplus due to their market power and control over information (13, 16), others suggest that with appropriate regulation and competitive pressures, it is possible to mitigate these effects (34, 10).

Consumers also benefit from data collected by platforms, such as feedback and reviews left by other consumers on a product. For example, (29) find that having information such as review quantity, review quality, perceived symmetric product information, and responsiveness positively influences trust in the seller from the buyers. Therefore, the type and use of collected information greatly influence consumers' willingness to share it, and as awareness of data-sharing practices increases, users will likely demand compensation for their information. On the contrary, (23) investigate the motivations that drive consumers to voluntarily disclose their information to online retailers. Their findings reveal that consumers can incentivize sellers to offer lower prices by strategically withholding information about their most valued products. In equilibrium, sellers commit to refraining from using buyer information for price discrimination. In a similar setting, (21) demonstrate that information disclosure leads to equilibrium price discounts while in (24) it improves match quality but gives more market power to the platform relative to the merchants, which can reduce entry and consequently consumer welfare.

3.2 Privacy.

Privacy is a concept that involves the control and safeguarding of personal information, as defined by (32). It represents a boundary between oneself and others, and according to (2), privacy is not about avoiding sharing but about controlling how information is shared. Privacy is important because it affects the distribution of benefits in interactions, often altering the balance of information between parties. In online markets, while information about buyers helps sellers overcome informational asymmetries, it also creates uncertainty regarding the sellers' pricing and targeting strategies. Economic research suggests that privacy protection can both increase or decrease individual and societal welfare depending on the specific context, so privacy protection is neither absolutely beneficial nor detrimental in an economic context (for a survey, see (2)).

Yet, the increasing level of data collection and personalization in the platform economy has intensified privacy concerns. In the European Union, the General Data Protection Regulation (GDPR) mandates the anonymization of consumer data and its sharing only with explicit consent. In the United States, as early as 2015, the Federal Trade Commission advocated for greater consumer control over personal data collection and usage[2]. In addition, over the past year, interest in the use of analytical cookies has surged following complaints from None of Your Business (NOYB), an Austrian nonprofit dedicated to strengthening privacy rights. NOYB has filed complaints in

[2]FTC privacy report: see here.

all 30 EEA member states against 101 European companies, asserting that many tracking technologies used on EU websites are provided by US companies. This has led to several regulatory actions throughout the EU and scrutiny from regulators in several EU countries (26).

For platform users, the potential benefits of strategically sharing certain data while protecting other data are quite apparent. For example, users get reduced search costs and increased accuracy when searching for a product on a platform that has tracked their previous buying activity. The potential costs of having too much information disclosed to the wrong parties in the internet is also apparent when users might face price discrimination, and in worst cases stigma, blackmailing, identity theft, etc. Furthermore, it is difficult to prevent released data from being duplicated and accessed by third parties or to control its secondary users. However, there are also costs for information asymmetry between sellers and buyers and the optimal information sharing rule is one that takes into account the potential benefits and costs for all the parties involved.

3.3 Challenges for Businesses Under the Current Structure.

In principle, retailers now have access to real-time data that allows them to follow consumer behavior even before a purchase is made. (22) finds that a typical pre-purchase data of a consumer on an online retail platform might consist of bevahoiurs like entering a search query, filtering by product characteristics such as price or star rating, and finally visiting the product-detail pages for some products and purchasing one of them. However, the data collected by the platforms can also include browsing history, purchase history, search queries, items added to cart but not purchased, as well a demographic characteristics of the user such as age and gender. For the retailers, data on consumer behavior is valuable because it enables better decision making when pricing and advertising their products therefore a major problem arises when only a few players in the market have access and make use of the data.

(17) find that only major retailers like Amazon and Walmart effectively utilize state-of-the-art tools to leverage historical and real-time consumer data while a report by (15) reveals that leaders in digital transformation in the groceries industry are 83% more profitable than their lagging counterparts and account for over 90% of the sector's market capitalization gains. The dominance in data utilization by platforms and large businesses may lead to reduced market competition by potentially foreclosing rivals (16, 33). Furthermore, some studies indicate that platforms like Amazon use the collected data to engage in self-preferencing, where they rank their own products higher than those of third-party sellers when they identify a user with a higher propensity to buy the products (see, e.g. (19, 18)).

Lack of data and lack of adoption of new systems are major challenges for small and medium-sized retailers trying to make use of data analytics. (25) further highlight issues such as data fragmentation, inadequate data collection, and insufficient organization as obstacles for businesses trying to implement new technologies. Another significant issue is the lack of interoperability and verifiability among platforms, which ties individuals and companies to specific data service

providers, leading to market fragmentation and stifling innovation (28).

4 Data Structures.

Data can be stored in three types of databases: *centralized*, *decentralized*, and *distributed* (31). *Centralized databases* are those that are stored on a single physical device and therefore are easier to maintain and control than those stored in multiple devices. However, they have drawbacks in terms of availability and performance; for example, they can become a bottleneck if too many requests need to be processed during a specific period. *Decentralized databases* incorporate multiple hierarchically organized centralized databases. They increase the availability of the data, but might still have performance issues because the changes need to be communicated and processed through the hierarchy of the system.

A *distributed database* is a type of database where data are replicated across multiple storage devices (nodes) with equal rights (31). *Distributed databases* help increase availability and avoid performance issues because if a node fails or cannot be accessed in time, requests can be channeled to another node and provide the same result. In fact, one key characteristic of distributed databases that makes them more complex than centralized databases is that an operation should always return the same results on every node. When the database is synchronized, it is said that the database is in a *consistent state*. In order for a distributed database to reach a consistent state, it needs a consensus mechanism. Think of consensus mechanisms as ways in which the nodes vote on which version of the database is the correct one.

If some nodes have malicious intentions, such as trying to store incorrect data, the consensus mechanism has to be more complex, usually relying on cryptography and game theory ((27)), to ensure the malicious nodes cannot corrupt the stored data. A **distributed ledger** is a type of distributed database that assumes the presence of nodes with malicious intentions and in which the data can only be appended or read, but not deleted. A **Distributed Ledger Technology (DLT)** enables the realization and operation of distributed ledgers, which allow benign nodes, through a shared consensus mechanism, to agree on an (almost) immutable record of transactions (31). The use of cryptography in DLTs and the fact that nodes do not need to verify their identity to participate in the network enable, in many cases, the anonymity (12) or pseudo-anonymity (27) of the people contributing to the ledgers and their data.

A major application of distributed ledger technology are *smart contracts*: computer programs that allow secure transaction issuance without the need for third parties, transactions are traceable and immutable. The purpose of smart contracts is to reduce the transaction costs associated with contracting and to increase transparency between the parties. Furthermore, smart contracts are not restricted to data stored on the same distributed ledger (on-chain), but can also communicate with external (off-chain) services, such as APIs. In healthcare, for example, MedRec (6) is a decentralized record management system that uses DLT and aims to reduce the efforts required to obtain a complete representation of the medical records of a particular patient. MedRec stores the patient's digital signature on a blockchain and patients are ultimately in control of who views

their data and in doing so shifts the focus of control from the institution (e.g., a hospital) to the patient.

5 Distributed Ledgers as an Alternative to Data Intermediaries.

Distributed Ledger Technologies offer an alternative structure to the internet data market by replacing data intermediaries, such as platforms, with a decentralized system of data collection and sharing. Adopting a DLT would require internet users to voluntarily record their internet activity across multiple sites, such as retail platforms and social networks, on the database. An advantage for users is that, on a DLT, they can choose the level of anonymity they prefer, releasing only the information they deem appropriate. Businesses can then offer compensation to users to access their data in a direct sale through the type of *smart contracts* explained in Section IV. This compensation need not be monetary; it can also include discounts or access to specific sales from a retailer.

A distributed ledger could offer solutions and advantages over the current intermediation system. It reduces the platform's market power by providing an alternative for buyers and sellers to exchange information and allowing the price of information to be determined solely by the interested parties without the need for intermediaries. A sufficiently large distributed ledger might also facilitate access to data for small and medium-sized businesses, as it becomes a central and reliable source of consumer information, eliminating the current fragmentation problem businesses face when choosing data providers. Consumers might benefit from receiving a fair price for sharing their information. In contrast to the current system, firms would need to compensate for the flow value of information to users, rather than the marginal value they receive from platforms. This poses the question of who would capture the surplus in the case that DLTs replace information intermediaries as the redistribution of surplus would still depend on the competitiveness of the market and the market power of each participant.

DLTs make information verifiable without disclosing the real identity of the database users. This implies that the user identity is protected, while businesses still have access to relevant information from a reliable source. The encryption technology allows for the protection of information from unwanted uses and manipulation by third parties. Additionally, the need to ensure truthful reporting from users incentivizes an allocation that compensates users for honesty. Furthermore, not only can we store information about users, but reviews and opinions of products can also be recorded on a distributed ledger where they cannot be altered, addressing some of the trust issues buyers have with retailers.

These ideas are not far-fetched; in fact, some startups are already trying to implement blockchain technology within this context with moderate success (see, for example, Datacoup at https://datacoup.com/). However, there are various challenges with implementing this technology. The first challenge is generating enough momentum to build a large enough dataset that can actually compete with the billions of observations controlled by the main data intermediaries.

Additionally, as the owners of the most popular platforms, social networks, or search engines, data intermediaries can restrict the interaction of DLTs with their sites, making data collection difficult. Furthermore, all technologies have flaws and there will still be privacy breach risks associated with having personal data stored on a DLT, even if these risks are less significant than in the current system. For instance, even with DLTs preventing all users from sharing the information that they acquire.

6 Conclusion.

Consumer data collected by internet platforms is valuable for retailers, as it helps develop better pricing and marketing strategies for their products. The current system allows platforms to control large datasets containing personal consumer information, capitalizing on it through indirect sales of information. Data externalities and the economies of scale of data collection have granted internet platforms significant market power, leading to the surplus from information sharing not being distributed across all participants and small retailers and advertisers lagging behind due to fragmentation in the data market. Users of the platforms typically bear the costs when the platforms collect and sell their data, often without their knowledge or consent. They face risks of price discrimination and loss of privacy, while receiving no tangible compensation for it.

We propose the use of Distributed Ledger Technologies (DLTs) as an alternative to data intermediaries on the Internet. DLTs present a way for users to gain control over their information, potentially enabling optimal information sharing between consumers and firms via *smart contracts*, eliminating the need for intermediaries. The cryptography inherent in DLTs ensures the privacy protection of users while guaranteeing that the information comes from a reliable source. The challenges in implementing this technology include the dominance of the current system and the immense quantity of data needed to compete with the main intermediaries. Further measures are necessary to guarantee the safeguarding of people's personal information on a DLT as data breaches can still occur once many parties have accessed the information. However, this technology presents a compelling alternative to the current landscape.

References

[1] Daron Acemoglu, Ali Makhdoumi, Azarakhsh Malekian, and Asu Ozdaglar. Too much data: Prices and inefficiencies in data markets. *American Economic Journal: Microeconomics*, 14(4):218–256, 2022.

[2] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. The economics of privacy. *Journal of economic Literature*, 54(2):442–492, 2016.

[3] Anat R Admati and Paul Pfleiderer. A monopolistic market for information. *Journal of Economic Theory*, 39(2):400–438, 1986.

[4] Anat R Admati and Paul Pfleiderer. Direct and indirect sale of information. *Econometrica: Journal of the Econometric Society*, pages 901–928, 1990.

[5] Susan Athey, Christian Catalini, and Catherine Tucker. The digital privacy paradox: Small money, small costs, small talk. Technical report, National Bureau of Economic Research, 2017.

[6] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. Medrec: Using blockchain for medical data access and permission management. In *2016 2nd international conference on open and big data (OBD)*, pages 25–30. IEEE, 2016.

[7] Michael R Baye and John Morgan. Information gatekeepers on the internet and the competitiveness of homogeneous product markets. *American Economic Review*, 91(3):454–474, 2001.

[8] Matthew Bellringer. Worthy of trust: Protecting minority privacy in diversity reporting. *Journal of Data Protection & Privacy*, 5(2):173–182, 2022.

[9] Dirk Bergemann and Alessandro Bonatti. Markets for information: An introduction. *Annual Review of Economics*, 11:85–107, 2019.

[10] Dirk Bergemann and Alessandro Bonatti. Data, competition, and digital platforms. *arXiv preprint arXiv:2304.07653*, 2023.

[11] Dirk Bergemann, Alessandro Bonatti, and Tan Gan. The economics of social data. *The RAND Journal of Economics*, 53(2):263–296, 2022.

[12] David Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of Crypto 82*, pages 199–203. Springer, 1983.

[13] Jay Pil Choi and Doh-Shin Jeon. A leverage theory of tying in two-sided markets. 2016.

[14] Jay Pil Choi, Doh-Shin Jeon, and Byung-Cheol Kim. Privacy and personal data collection with information externalities. *Journal of Public Economics*, 173:113–124, 2019.

[15] Gemma D'Auria, Andreas Ess, Holger Hürtgen, Gereon Sommer, and Alex Sukharevsky. Grocers can fuel growth with advanced analytics. *McKinsey.com*, 2021. Available at: https://www.mckinsey.com/industries/retail/our-insights/grocers-can-fuel-growth-with-advanced-analytics#.

[16] Alexandre De Cornière and Greg Taylor. Upstream bundling and leverage of market power. *The Economic Journal*, 131(640):3122–3144, 2021.

[17] Nicole DeHoratius, Andrés Musalem, and Robert Rooderkerk. Why retailers fail to adopt advanced data analytics. *Harvard Business Review Online*, 2023.

[18] Jean-Pierre Dubé. Amazon private brands: Self-preferencing vs traditional retailing. *Available at SSRN 4205988*, 2022.

[19] Chiara Farronato, Andrey Fradkin, and Alexander MacKay. Self-preferencing at amazon: evidence from search rankings. Technical report, National Bureau of Economic Research, 2023.

[20] Federal Trade Commission FTC. Data brokers: A call for transparency and accountability. *Washington, DC*, 20, 2014.

[21] Sinem Hidir and Nikhil Vellodi. Privacy, personalization, and price discrimination. *Journal of the European Economic Association*, 19(2):1342–1363, 2021.

[22] Elisabeth Honka, Stephan Seiler, and Raluca Ursu. Consumer search: What can we learn from pre-purchase data? *Journal of Retailing*, 2024.

[23] Shota Ichihashi. Online privacy and information disclosure by consumers. *American Economic Review*, 110(2):569–595, 2020.

[24] Rishabh Kirpalani and Thomas Philippon. Data sharing and market power with two-sided platforms. Technical report, National Bureau of Economic Research, 2020.

[25] Lien Lamey and Katrijn Gielens. (new) data sources in retailing: Opportunities and challenges. *Journal Of Retailing*, 100(1):1–4, 2024.

[26] Morgan Lewis. Navigating the global data privacy landscape. Technical report, Morgan Lewis, 2023. Available at: https://www.morganlewis.com/-/media/files/publication/morgan-lewis-title/white-paper/2023/navigating-the-global-data-privacy-landscape.pdf?rev=cb2a5acaf3a54583abd990c86a90d129&hash=C117E1C103A33A875DC388BD69699D41.

[27] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[28] Antti Poikola, Kai Kuikkaniemi, and Harri Honko. Mydata. *Finland: liikenne-ja viestintäministeriö*, 2014.

[29] Madugoda Gunaratnege Senali, Mohammad Iranmanesh, Morteza Ghobakhloo, Behzad Foroughi, Shahla Asadi, and Abderahman Rejeb. Determinants of trust and purchase intention in social commerce: Perceived price fairness and trust disposition as moderators. *Electronic Commerce Research and Applications*, page 101370, 2024.

[30] Carl Shapiro and Hal R Varian. *Information rules: A strategic guide to the network economy*. Harvard Business Press, 1999.

[31] Ali Sunyaev. Distributed ledger technology. *Internet computing: Principles of distributed systems and emerging internet-based technologies*, pages 265–299, 2020.

[32] Alan F Westin. Privacy and freedom. *Washington and Lee Law Review*, 25(1):166, 1968.

[33] Feng Zhu. Friends or foes? examining platform owners' entry into complementors' spaces. *Journal of Economics & Management Strategy*, 28(1):23–28, 2019.

[34] Ruizhi Zhu, Sridhar Moorthy, and Xianwen Shi. Advertising platforms and privacy. *Rotman School of Management Working Paper*, (4248339), 2022.