10

Data Commons, Data Oligopolies, and Consumer Financial Data Trusts

Alberto R. Salazar and Andi Rezda Rezal

10.1 INTRODUCTION

The rapid digitalization of capital markets and the expansion of financial technology have significantly enhanced the efficiency of the financial sector. However, this progress has also introduced new risks, particularly concerning financial data concentration. Financial companies are increasingly leveraging advanced technologies to consolidate control over public-generated financial data, leading to the rise of financial data oligopolies. This is part of a concerning trend. For instance, reports in recent years indicated that Google, Microsoft, and Yahoo together dominated 98 percent of the US search engine market, whereas Amazon accounted for 43 percent of US online retail sales and Facebook and Google controlled 73 percent of all digital advertising in the US (Shkabatur 2019, 358). This growing data concentration problem exposes the serious limitations of the prevailing individual consent model of data protection. Even in jurisdictions such as the European Union, where data subjects have greater protection and rights, most users accept cookies automatically to gain access to websites (Houser and Bagby 2023, 122). Neither the General Data Protection Regulation (GDPR) nor the California Consumer Privacy Act (CCPA), widely considered the two strongest privacy laws, has resulted in meaningful improvements in citizen's privacy protection and legal compliance by companies (Lancieri 2022).

This is largely due to information asymmetries, consumer rationality failures, and market power in data markets (Blankertz 2020, 6, 8; Solove 2021, 5; Lancieri 2022), as well as poor enforcement that relies on consumers' abilities to bring complaints and is often underfunded (Fisher and Streinz 2022, 902; Houser and Bagby 2023, 127). In fact, it appears that data concentration by big tech companies has increased after the introduction of robust privacy laws such as the GDPR (Blankertz 2020, 12; Johnson et al. 2023). Furthermore, while focusing on individual data rights, current data protection laws often overlook the negative impact of concentrated control over data and data-generating infrastructures (Fisher and Streinz 2022, 833, 906), including the internet, search engines, cloud services, operating systems, platforms, data

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

centers, and other emerging technologies. As a small number of entities amass vast quantities of data, ostensibly to maximize profits and enhance their societal influence, it becomes imperative to critically examine the consequences of this data concentration.

The data concentration problem is evident in the financial sector. BlackRock's Aladdin platform serves as a potential example of the data oligopoly problem. BlackRock Inc., the world's biggest asset management company, to a significant extent owes its success to its operating system, Aladdin. This centralized platform collects and analyzes data on client portfolios, trades, risks, operations, performance, compliance, and accounting worldwide to predict market behavior and provide optimal information for effective investing decisions.[1] However, like other data-driven technologies, Aladdin must continue to scale the amount of data it collects and analyzes to maintain its competitive advantage. This expansion raises troubling concerns about the limits of BlackRock's access to data and the types of data it should be allowed to acquire. A critical concern with the emergence of financial data oligopolies such as Aladdin relates to their negative impact on financial consumers. Financial companies concentrating vast amount of data – including consumer behavior data – and empowered by financial technologies may facilitate financial exclusion and exploitation, including predatory and discriminatory lending, in addition to privacy breaches. While Aladdin mainly serves investors, it may enable or facilitate investors' decisions to engage in such problematic practices.

The Governing Knowledge Commons (GKC) framework (Frischmann et al. 2014; Madison 2024) provides a valuable lens through which to analyze the policy response to the emergence of financial data oligopolies. Viewed through this framework, financial data can be considered a shared resource that *could* be governed by a community of members. From this perspective, the monopolization of financial data by a select few entities may be viewed as eroding the fundamental principles of community governance that underpins the concept of data as commons. This process not only excludes important community members or stakeholders who contribute to the data ecosystem but also distorts the rules-in-use (Crawford and Ostrom 1995; Sanfilippo et al. 2018) that govern data sharing and utilization. The outcome is a system that disproportionately benefits a small group of actors while potentially undermining the broader societal benefits that could be derived from a more equitable and participatory approach to financial data management. Financial consumers, as important members of the governing community, are vulnerable to potential abuses by data oligopolies. However, they also have the capacity to act collectively to protect their data rights and interests and actively participate in the governance of *financial data commons*. One effective strategy involves consumer associations' activism, which can serve as a form of collective action to co-govern their financial data. This approach is akin to the concept of

[1] www.blackrock.com/aladdin.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

consumer data trusts, where consumers band together to manage and safeguard their data collectively (Blankertz 2020).

Drawing on insights from the data commons approach (Shkabatur 2019), this chapter posits that consumer associations, acting as data trusts, can play a crucial role in overseeing financial data oligopolies while fostering the development of a community governance of data commons. In doing so, these associations can promote the attainment of valuable outcomes beyond addressing privacy harms, notably preventing predatory and discriminatory lending, mitigating financial exploitation, and expanding access to financial capital. By leveraging and shaping both formal and informal rules-in-use to facilitate these efforts, consumer associations or consumer data trusts contribute to *reinstitutionalizing* community governance that ultimately enhances the legitimacy of financial data commons.

This argument is discussed in the context of a case study, namely, BlackRock's Aladdin platform. Drawing on secondary sources, the analysis hypothesizes that Aladdin's massive financial data collection in various action situations may lead to the formation of data oligopolies that primarily benefit elite investors and potentially facilitate consumer financial exclusion and exploitation. Furthermore, by adopting a polycentric view of financial data governance and exploring the potential of consumer-led activism, this chapter discusses how consumer associations acting like data trusts can aggregate consumer data rights, enhance collective bargaining power, and negotiate more equitable terms with data oligopolies. Drawing on recent legal developments in Europe, particularly a case involving a German consumer association's action against Meta-Facebook, the chapter highlights the potential of such associations to address not only data privacy and value distribution concerns but also issues of financial exclusion and exploitation amid the emergence of financial data oligopolies.

10.2 A DATA COMMONS APPROACH TO FINANCIAL DATA AND FINTECH

Knowledge commons is the community governance of shared knowledge, information, and data resources (Madison 2024). Governance, whether the product of design or path-dependent accidents, consists of systems of formal and informal rules – ranging from law to social norms that may be mediated through sociotechnical devices – by which members of that community achieve their goals and resolve problems and disputes. The GKC framework identifies instances of shared knowledge resources, highlights the problems or social dilemmas arising from the shared character of such resources – "conflicts between self-interested individual behavior and social or collective interests" (Madison 2024, 309) – and analyzes the rules communities can adopt to mitigate these problems. The important point is that the rules-in-use govern the production, contribution, sharing, use, appropriation, preservation, and even destruction of the shared resource (Madison 2024, 307–8).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

A *data commons* can form around "a collection of data that is shared as a common resource" (Houser and Bagby 2023, 140). As a valuable knowledge resource, data is produced by market participants and can be considered a shared resource (Madison 2024: 308). These stakeholders – namely, companies, investors, consumers, employees, the environment, local communities, and governments – are involved in the creation, collection, management, and use of data. They can be part of a data commons (Shkabatur 2019: 383, 385) and often participate in the community governance of data. Rules-in-use – formal regulations, social norms, market practices, compliance strategies, and enforcement mechanisms, including those at the societal level (Crawford and Ostrom 1995; Sanfilippo et al. 2018) – affect their interactions in various practical action situations. For instance, the "transmission principles" that define the terms for information transfer and various informal norms regarding commercial sharing of information are examples of rules-in-use applied to specific interaction situations (Sanfilippo et al. 2018, 139). A data commons approach to financial data and fintech offers a nuanced framework for understanding and developing different mechanisms governing data. It addresses both top-down regulations and bottom-up practices and strategies, capturing the complexities of financial data creation, sharing, and management.

10.2.1 *The Monopolization of Financial Data*

Community governance of data is becoming an imperative. Community members are increasingly demanding not only protection of their interests, notably privacy, voice, and profit-sharing associated with data commercialization, but also *data sovereignty*. Data, from this perspective, should benefit not only companies that often provide the infrastructure for data collection and management but also all stakeholders involved and the public (Shkabatur 2019, 383). Such demands are growing, as current privacy laws are failing to provide significant protection of data subjects' rights, largely due to information asymmetries, rationality failures, and market power in data markets (Lancieri 2022), not to mention concentrated control over data infrastructures. These problems are compounded by poor enforcement that relies on consumers' abilities to bring complaints and is often underfunded (Houser and Bagby 2023, 127). Furthermore, the environmental cost of data governance imposed on community members and society at large provides additional reasons for the collective governance of data as shared resource. Data governance, including the use of financial technology, requires increasing consumption of energy and water, which worsens the ongoing climate crisis, affecting community members and the public in general. Recognizing this problem further warrants not only community members' entitlement to the benefits of data but also to participating in its collective governance.

Applying the GKC framework to financial data and fintech reveals several critical considerations. The community involved in creating, collecting, managing, and

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

using shared financial data includes financial companies, investors, creditors, financial consumers, local communities, regulators, and other stakeholders. While these community members appear to somewhat participate in the collective governance of financial data, their involvement in financial data commons is limited in practice. The nature of the resource is such that financial data is non-rivalrous but excludable (Jones and Tonetti 2020; Purtova and van Maanen 2024). While it can be duplicated and shared at minimal marginal cost, access can be restricted through technical and legal measures, as well as by social norms and practices (Frischmann et al. 2014, 1–2). And notable power imbalances and information asymmetries exist among community members.

Specifically, financial and fintech companies are increasingly *monopolizing* the collection, storage, use, and commercialization of financial data to the detriment of other members of the governing community (McIntosh 2019; Chakravortl 2021; Houser and Bagby 2023). This situation gives rise to a critical social dilemma. Thanks to their control of financial technologies or infrastructures, financial companies absorb ever-growing amounts of financial data, while relying on formal and informal rules to largely exclude data subjects – notably small investors, creditors, and companies as well as financial consumers – from its governance (Sanfilippo et al. 2021, 268, 278; Fisher and Streinz 2022, 832). Consumer data is overshared with some and undershared with others (Houser and Bagby 2023, 116). Excluded community members have limited influence over how their data is collected, managed, and used, and are often excluded from governance (Sanfilippo et al. 2021, 268). This can be viewed as data subjects' involuntary contribution, which questions the legitimacy of data commons (Sanfilippo et al. 2021, 285–86). Interactions in this context are predominantly transactional, with, for instance, consumers exchanging data for services with minimal transparency or collective decision-making regarding data practices. Such practices by data oligopolies are often driven by commercial interests rather than public benefit. The primary benefits from financial data exploitation accrue mainly to financial and fintech companies, whereas several risks and harms fall on powerless community members such as consumers. While financial data is produced by all, it is largely under private control and mainly serves to maximize the benefits of private data controllers (Fan 2021, 1444), sometimes to the detriment of data subjects (MacCarthy 2011; Houser and Bagby 2023, 115). For instance, financial companies may use collected financial data to facilitate predatory and discriminatory lending practices.

These data oligopoly practices undermine the potential for a community governance of financial data. Concentrations of power prevent community governance, as the political economy of commons suggests (Madison 2024, 323–24). The GKC framework can thus reveal both the oligopolistic tendencies of financial companies and the need to heed community members' neglected interests and voices. Otherwise, data commons governance may be deemed ineffective and illegitimate (Sanfilippo et al. 2021, 268, 283). Furthermore, financial data oligopolies can erode

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

the attainment of outcomes (Martens 2018; Houser and Bagby 2023, 116) that data commons can favor and that community members may value. These include preventing privacy harms, cybersecurity risks, and financial exclusion and exploitation; expanding access to credit and funding; sharing profits from data commercialization; stimulating financial innovation and enabling collaborative development of solutions; enhancing financial competition and facilitating the rise of new competitors; and reducing barriers to financial data access.

The nature of financial data as a shared resource, community members' involvement in financial data production and dissemination, and the desired outcomes may call for the need to both address the financial data oligopoly problem and seek the building of effective and legitimate community governance of financial data commons. Barriers to implementation include resistance from financial companies prioritizing profit maximization and proprietary technological platforms that limit community members' participation in financial data governance. Among other things, it seems imperative to encourage the development of rules that may facilitate the effective involvement of community members in creating financial data commons.

10.2.2 *The Promise of Consumer Data Trusts*

The activism of community members may play a crucial role in developing financial data commons, challenging the dominance of data oligopolies, and implementing a community governance of financial data. Specifically, financial consumer groups, as one important community member, can actively foster a collective governance of financial data. These groups can represent consumers or evolve into consumer data trusts (e.g., Zarkadakis 2020), serving the interests of consumer data subjects. *Data trusts* can be defined as governance devices that place an independent fiduciary intermediary between companies and data subjects (Houser and Bagby 2023). They can be viewed as a form of data commons (Scassa 2020; Madison 2024, 328), wherein consumers pool their data, assert their voice as data subjects, and govern it as shared resource. In this capacity, these trusts can play a crucial role in overseeing financial data oligopolies (Delacroix and Lawrence 2019; Houser and Bagby 2023), thus revealing the polycentricity of financial data governance (Sanfilippo et al. 2021, 270). These contestation efforts can lead to the development of more legitimate new rules-in-use (Sanfilippo et al. 2021, 281).

By aggregating consumer data rights and enhancing collective bargaining power, consumer data trusts and trustees acting on behalf of consumers can negotiate more equitable terms, enforce robust privacy safeguards (Delacroix and Lawrence 2019; Blankertz 2020; Ruhaak 2021; Fisher and Streinz 2022, 835; Houser and Bagby 2023, 140, 144, 152), and ensure a fair distribution of the economic value derived from financial data. Key features of consumer data trusts may include pooled data rights, democratic governance, professional management, and stringent privacy and ethical

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

standards. Taken together, these elements offer greater negotiating power, stricter data protections, and a platform for collaborative decision-making on data policies, including efforts to attain valuable outcomes (Houser and Bagby 2023, 174). The emergence of such trusts represents a paradigm shift in data governance, addressing the limitations of individual consent models (MacCarthy 2011; Delacroix and Lawrence 2019) and potentially rebalancing power dynamics between individual consumers and data oligopolies (Van Geuns and Brandusescu 2020; Houser and Bagby 2023, 140). This model not only tackles immediate concerns about data privacy and value distribution but also lays the groundwork for a more participatory and equitable data commons.

Consumer data trusts may be enabled by formal rules and in turn help develop and implement informal rules to pursue outcomes that consumers deem valuable, including social norms, strategies, and practices seeking to protect consumers' interests and to undo data oligopolies' rules that are not conducive to building data commons. This combination of data subjects' participation and voice with legal regulation may address the governance failures of illegitimate and socially problematic commons governance (Sanfilippo et al. 2021, 283). For instance, granting a consumer association a right to bring a representative action, utilizing consumers' right to an explanation of companies' use of data or financial algorithms or to data portability, and embracing emerging open banking laws and policies legally empower these associations to oversee data oligopolies, including preventing discriminatory or exploitative lending practices (Anidjar and Mizrahi-Borohovich 2019, 201), and help build a community governance of data commons. By consolidating the data rights of numerous consumers and enhancing their collective bargaining power, consumer data trusts can negotiate with financial companies to oversee the development and implementation of new informal and formal rules. These rules, while fostering community governance, also safeguard consumers' interests. This is particularly important as financial companies are likely to resist external oversight and accountability, for instance by opposing financial algorithm and data disclosure and audits.

Data trusts can develop *strategies* to push for more favorable terms concerning data collection, usage, monetization, and access, including privacy and transparency (Houser and Bagby 2023: 144, 160). This is consistent with the idea that consumers have some ownership over their financial data and accessing it serves to attain positively valued outcomes (Fracassi and Magnuson 2021: 330, 346; Jurcys et al. 2021). For instance, trusts can develop and promote the enforcement of ethical guidelines for the use of financial data. These guidelines may include prohibiting the use of consumer data for predatory lending practices, ensuring that data is not used to unfairly discriminate in financial decision-making, and requiring transparency about the extent to which consumer data influences investment recommendations. Similarly, data trusts could promote data portability and interoperability standards. Trusts could advocate for standards that make it easier for consumers to

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

transfer their data between different platforms. This could involve requiring financial companies to provide data in standardized, machine-readable formats, ensuring that consumers can easily move their financial data to competing platforms. Additionally, trusts could promote the development of open application programming interfaces (APIs) that foster greater competition within the financial technology sector. These standards could reduce the lock-in effects that help entrench data oligopolies. All these strategies by data trusts can help ensure that powerful financial companies and their financial technology also operate in the best interests of consumers and smaller companies.

Furthermore, consumer data trusts may provide *oversight* of financial companies, and in particular their financial technologies and data. Financial companies rely heavily on complex algorithms to analyze data and make decisions. Data trusts could demand transparency of how algorithms use consumer data, review them for potential biases or unfair practices, and require human oversight for certain types of algorithmic decisions. This oversight can help prevent algorithmic bias and discrimination (Shkabatur 2019, 383), ensure fair treatment of consumers, and exemplify the power of data trusts to "reveal 'black box' algorithms that leading technology firms use to concentrate their power and perpetuate injustices" (Houser and Bagby 2023, 118). Consumer data trusts could also conduct regular audits of financial and fintech companies' access and use of consumer financial data (Blankertz 2020; Houser and Bagby 2023, 179). These audits may involve reviewing data sharing agreements between financial companies and data users, analyzing data flows to ensure they comply with agreed-upon terms, and verifying that data access is limited to authorized purposes (Blankertz 2020, 16–17). By performing these audits, trusts can help ensure that financial data oligopolies are not overstepping bounds or misusing consumer data. Furthermore, consumer data trusts can set and enforce stricter privacy and security standards than individual consumers or regulators might be able to achieve. This could mean mandating specific encryption and data protection protocols, requiring regular third-party security audits and imposing penalties for data breaches or unauthorized access. The trust's ability to terminate agreements with companies and withhold access to member data gives it leverage to enforce these standards (Blankertz 2020, 17).

In terms of value distribution and compensation, consumer data trusts could negotiate for more equitable sharing of profits generated from consumer financial data (Mulgan and Straub 2019; Houser and Bagby 2023, 175). They could, for instance, require financial and fintech companies to share a portion of revenues derived from consumer data analysis, negotiate reduced fees or improved services for trust members, and ensure that insights from aggregated data are made available to consumers. This approach ensures that consumers receive a fairer share of the benefits generated by their data, rather than allowing large financial institutions to monopolize those gains. This aligns with the growth of data marketplace organizations that assist consumers in collecting and selling their data (Blankertz 2020, 11).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

Moreover, consumer data trusts can establish mechanisms for resolving disputes related to data use and for sanctioning violations (Houser and Bagby 2023, 179). For financial companies, this might involve creating independent arbitration panels to handle complaints, establishing escalating penalties for repeated violations of agreed-upon terms, and providing consumers with the ability to challenge decisions made using their data. These processes offer consumers recourse if they believe their data has been misused.

While the implementation of such strategies and practices will likely face challenges, including resistance from financial companies and technical complexities, they offer a promising path forward. By *empowering consumers* collectively, consumer data trusts could provide a much-needed counterbalance to the growing power of financial data oligopolies, promoting fairer, more transparent, and more equitable use of consumer financial data. This can help build an effective community governance of financial data that could achieve important social goods such as privacy, quality, security, and innovation while enhancing competition. Collaborative data governance may spur innovation, improve access to financial services, and facilitate the emergence of new market players. Achieving these benefits, however, requires the cooperation of financial companies, regulators, and consumers to address challenges effectively.

Despite their potential, consumer data trusts face practical obstacles, such as achieving the necessary scale, developing effective engagement and internal governance among consumer members, having sustainable funding models, accessing appropriate technologies to manage shared consumer data, protecting against security risks associated with centralizing data within trusts, and navigating technical and regulatory landscapes. In particular, the legal status of consumer data trusts remains uncertain, and trusts' above-mentioned strategies and practices are likely to require facilitative laws and policies. Nonetheless, consumer data trusts offer a promising avenue for experimenting with participatory and equitable data governance models. Ultimately, consumer data trusts should be viewed as part of a broader data governance ecosystem. Data commons are part of polycentric data governance systems or multiple different governance centers (Sanfilippo et al. 2021, 270; Madison 2024, 325). Consumer data trusts' effectiveness could be enhanced when combined with community members' cooperative practices, thoughtful regulation, technical standards, and efforts to improve data literacy. As financial companies expand their data practices, novel governance approaches like data trusts will be crucial. Further research and pilot projects are necessary to refine these models and assess their long-term impact.

10.3 BLACKROCK AND ALADDIN: A CASE STUDY

There are two things that make *data-opoly* (Fisher 2021; Stucke 2022) possible under BlackRock: motive and capability. In the new digital age of finance, BlackRock must

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

remain proactive in beating competitors to not suffer the same fate as other big players, such as Eastman Kodak or Blockbuster (Baxter et al. 2023). New financial technology used by the likes of Robinhood Markets Inc. can be a threat to BlackRock, as fintech makes investment more accessible to a more diverse population of investors.[2] According to Ananth Madhavan, the Global Head Research for ETFs and Index Investing at BlackRock, the best way to remain competitive is by investing in artificial intelligence (AI) and data technology, whose quality output depends on the amount of data available.[3] Better information output regarding risk management and investment will ensure the security of investors and the continuance of business. Better service also attracts more clients, who aid in further advancing BlackRock in the financial industry. Hence the key to survival and success is data collection – and this makes data-opoly a very attractive goal for BlackRock to achieve.

Not only is data-opoly desirable, but it is also achievable for BlackRock. Thanks to Aladdin, BlackRock has become the default option in the financial marketplace. According to BlackRock, "approximately 55,000 investment professionals around the world" from almost all industries rely on the Aladdin platform.[4] These investors include Google, Apple, Facebook, and Amazon (otherwise known as GAFA) – whose dominance over the information market is undeniable (Chakravortl 2021) – they all depend on BlackRock to manage their investment portfolios.[5] Furthermore, BlackRock is a major shareholder in 18,000 companies, banks, and financial services firms around the world.[6] As one executive of a large European insurer commented: "if you are looking to buy anything, or sell anything, or invest anything, it's very difficult to get around BlackRock."[7] Therefore, BlackRock can clearly use its position to gain virtually unlimited access to data – including to the databases of other dominant players in the data market – and to generate and exploit network effects to achieve data-opoly. At BlackRock's AI Labs, leading researchers, data scientists, and engineers are preparing for the processing and analysis of the ever-growing data the company is planning to accumulate.[8] This strategy may enable BlackRock to become the ultimate data-opoly. The next section elaborates on the direct and indirect methods BlackRock employs to collect different kinds of big data.

[2] "The Four Biggest Ways That Robinhood Changed Investing," *Bloomberg Businessweek*, July 29, 2021.

[3] "MIT AI Conference 2018: Staying Competitive in the World of AI in Finance." May 15, 2019. www.youtube.com/watch?v=0583lIm428A at 0'50"-2'06" and 10'50"-12':42".

[4] www.blackrock.com/aladdin/offerings/aladdin-overview.

[5] "BlackRock's Black Box: The Technology Hub of Modern Finance," *Financial Times*, February 23, 2023; "In Aladdin We Trust." *Queens Business Review*, September 18, 2023.

[6] BlackRock, *Investor Stewardship Annual Report* 2023. www.blackrock.com/corporate/literature/publication/annual-stewardship-report-2023-summary.pdf.

[7] "Aladdin and the Genius that is Larry Fink", *Cognitive Finance*, October 2020. www.cognitivefinance.ai/single-post/aladdin-and-the-genius-that-is-larry-fink.

[8] www.blackrock.com/corporate/ai.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

10.3.1 *BlackRock's Data Collection Capabilities*

BlackRock can acquire data through its massive client base via its Aladdin platform without needing countless permissions from clients to hand over various forms of data (Zetzsche et al. 2023). The ease of such data retrieval supports BlackRock's AI and machine learning technologies. Machine learning is an inductive approach to computing, in which AI systems analyze data to find the best solution to a problem, as opposed to following strict instructions coded by the programmers beforehand (Armour and Eidnmuller 2020). Machine learning is possible if the AI systems can act as a central nervous system and form a neural network with other information technologies and computers to communicate and deliver data between densely interconnected processing nodes, where the data is analyzed and an output created. In order for AI to work effectively, it must have access to as much relevant and accurate information as it can from one centralized database. Since any type of data may have the potential to be relevant in the long run, AI is designed to not be restrictive in data collection.

Similarly, Aladdin is designed to store, centralize, and convert various unstructured data – data mined from numerous sources – into readable data that is easier to analyze and utilize to make effective decisions concerning portfolios, risks, trades, operations, performance, compliance, and accounting management. In other words, it is the central nervous system that is equipped with the ability to connect with other data technologies and extract as much information from them as possible. BlackRock simply needs to obtain permission to initiate data collection from clients' information databases via the terms and conditions clients must consent to when signing up to use Aladdin. The terms include conforming to Aladdin's privacy policy, which covers the collection of personal information, including identification data, contact data, electronic monitoring data, financial data, and even sensitive personal information data (information regarding dietary restrictions, sexual orientation, disabilities, and political affiliation, among other things, taken from public sources such as social media or other third parties such as credit card providers). GAFA privacy notices confirm this by stating that third parties are able to gain access to their users' personal information collected by them; this is part of their own terms and conditions. Hence, the sharing of data between BlackRock and GAFA is inevitable because upon agreeing to Aladdin's privacy policies, users also consent to the sharing of their GAFA information with BlackRock. Users who consent to data sharing when using GAFA services may unknowingly authorize these companies to provide data to third parties, potentially including BlackRock when GAFA companies engage it for institutional investment services or analytics. GAFA companies themselves are clients of Aladdin, subjecting them to the same data-collecting terms and conditions as other clients, thus providing BlackRock access to even more data (Steele 2020, 23).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

In addition, the upgrade to Aladdin Data Cloud – an investment platform developed in partnership with SnowFlake – further exacerbates BlackRock's collection capability by enabling Aladdin to "host all of the [clients'] data – from both inside and outside Aladdin."[9] This feature is heavily supported by clients who tend to pull "their own data sources from other places" to centralize their data for convenience and to maximize their use of the platform.[10] As clients of BlackRock, it is plausible that GAFA provides BlackRock with additional data not initially collected by Aladdin at registration in order to receive better results. When combined with the sheer volume of public market data – global economic data stock quotes, climate data, government decisions, alternative data like geolocation and consumer activity – it is clear that the data BlackRock has access to make investment decisions far exceeds the type of data outlined in Aladdin's privacy policy. While this can benefit clients, who now have all their information in one place, by enabling them to make more accurate and successful investment decisions, it is also very profitable for BlackRock, which effectively now has all of GAFA's information in one system.

Thanks to its partnership with Snowflake, the system can now integrate external data into its platform by using Snowflake's data technology, which can process unstructured and raw data at a rapid speed, converting that raw data into structured data that can be integrated and read by Aladdin.[11] As part of the agreement, BlackRock has access to Snowflake's Data Cloud, which can be used in Aladdin's analysis. This is not the first partnership BlackRock entered into with a view to improving Aladdin Data Cloud. In 2020, BlackRock and Microsoft formed a strategic partnership to host Aladdin on Microsoft's Azure cloud platform, providing BlackRock with access to Microsoft's data centers around the world.[12] BlackRock was also able to leverage Microsoft's scale in computing and expertise in cloud computing and data analytics, as part of the collaboration. While the partnership did not give BlackRrock access to other Azure users' data, BlackRrock can use Microsoft's computers to collect new data globally. Aladdin's main cloud partner, Amazon's AWS, provides another access point into Amazon's database, including users' purchasing behavior and other data provided by Amazon's Internet of Things devices.[13] Being the top e-commerce company in the world that is also advancing into many lines of business, Amazon is providing BlackRock access to a plethora of information (Khan 2017, 754–767).

[9] www.blackrock.com/aladdin/products/aladdin-data-cloud.

[10] "Snowflake Inc. (SNOW) Q4 2020 Earnings Call Transcript." March 2021. www.fool.com/earnings/call-transcripts/2021/03/04/snowflake-inc-snow-q4-2020-earnings-call-transcrip/

[11] www.snowflake.com/blog/blackrock-and-snowflake-partner-to-unlock-the-value-of-data-for-the-investment-management-industry/?utm_source=blackrock&utm_medium=referral&utm_campaign=powered-by-snowflake-blackrock.

[12] "https://news.microsoft.com/2020/04/07/blackrock-and-microsoft-form-strategic-partnership-to-host-aladdin-on-azure-as-blackrock-readies-aladdin-for-next-chapter-of-innovation/.

[13] https://aws.amazon.com/what-is-aws/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

Aladdin can acquire even more data from portfolio companies through BlackRock's investments. This starts even before the purchase of any shares, when BlackRock is given access to prospective companies' information, which may include all types of information that can be used to assess the opportunities and risks of investing in those companies.[14] When applied to GAFA, this can include any type of users' information. As the head of the product group for Aladdin, Jody Kochansky noted almost a decade ago, given that untapped data – such as GPS locations, customers' online behavior, and transaction histories – is tremendously valuable for quality investment analysis, the strategy is to access as much untapped data as possible.[15] BlackRock's Aladdin can thus collect increasing amounts of data from all the four platforms before and after investing in them.

While BlackRock has utilized its Aladdin platform to collect data directly from GAFA in new and unconventional ways in order to optimize its AI technology and big data collection capacities, it also employs an indirect method of data collection: the exploitation of shareholder power to control corporate decisions and push for joint ventures, which ultimately aid its direct data collection. BlackRock's investments across vast segments of the market – it is among a small group of institutional investors that own large stakes in most US corporations (Azar et al 2018; Backus et al 2021) – allow it to influence the way companies manage their data. Aladdin's success has largely expanded BlackRock's client base, which has increased the capital at its disposal, and enables it to invest massively in GAFA shares: BlackRock is one of the largest institutional shareholders in Google, Amazon, Facebook (Meta), and Apple.[16] This position means that its voting power and voice in corporate decisions is significant. For example, Larry Fink convinced Mark Zuckerberg to change Facebook's platform design to be more "purpose-driven," namely, to focus more on promoting posts from friends than from advertisers (Serafeim 2018). This was a costly move for Facebook, whose main revenue relies on its advertising model.

10.3.2 *Caveats*

The considerations in the previous section provide insights into the technical, legal, and managerial rules-in-use that underpin BlackRock's unparalleled data collection capabilities. The difficulty in collecting evidence is compounded by the fact that the precise data management procedures employed by BlackRock and GAFA are kept under seal, thanks to intellectual property law, trade secrets, out of court settlements, not to mention the considerable complexity of the software (Pasquale 2015, 67,

[14] "BlackRock's Black Box: The Technology Hub of Modern Finance," *Financial Times*, February 24, 2020.

[15] "Blackrock Is Making Big Data Bigger." *Institutional Investor*, November 1, 2016.

[16] See www.nasdaq.com/market-activity/stocks/goog/institutional-holdings; www.nasdaq.com/market-activity/stocks/amzn/institutional-holdings; www.nasdaq.com/market-activity/stocks/meta/institutional-holdings; www.nasdaq.com/market-activity/stocks/aapl/institutional-holdings.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

103).[17] The public cannot investigate the contractual terms of joint ventures, nor can they criticize how the companies' algorithm collect and analyze data, even if companies provide public disclosure in "plain language" to comply with consumer protection law (Pasquale 2015, 7–8, 51, 103). Even internal stakeholders, who may be aware of BlackRock's business practices, and thus are great sources of information, are unable to share their observations with the public due to their contractual obligations to BlackRock. For example, BlackRock required departing employees to sign separation agreements to receive severance payments that included provisions waiving rights to whistleblower compensation for disclosing wrongdoings. This discourages whistleblowers, as it waives any right to recovery of incentives for reporting of misconduct.[18] Even though the Securities and Exchange Commission successfully removed this particular clause in a 2017 lawsuit against BlackRock, the terms of the agreement suggested that BlackRock may have been conducting acts that it wanted to stay behind closed doors, and there certainly is no guarantee that it will stop trying to prevent whistleblowers from speaking out in the future. Hence, the opacity surrounding the operations of powerful companies such as BlackRock, and its attempts to maintain a black box, makes it almost impossible to gather empirical evidence to prove BlackRock's strategy of creating a data monopoly. Aladdin's lack of transparency highlights the need for public accountability and raises concerns about potential risks and harmful impacts on stakeholders, including financial consumers.

10.4 BLACKROCK'S ALADDIN AND FINANCIAL CONSUMERS

Financial data oligopolies like BlackRock's Aladdin have emerged as dominant players in the financial market infrastructure, controlling critical data flows and analytical tools used by a vast number of investors. These platforms offer powerful solutions for risk management and investment decision-making, but their centralized nature also creates significant risks. These include the concentration of financial data and analytics in a few hands and the spread and reinforcement of similar data management models, potentially exacerbating herd behavior and amplifying market volatility in times of stress. Aladdin's global adoption across major financial institutions thus poses a systemic risk, as the investors who rely on the same financial risk management system can make and propagate the same mistakes (Zook and Spangler 2023, 119). Similarly, the dominance of these platforms raises concerns about overreliance on centralized models, the potential for overlooking idiosyncratic risks, and the creation of feedback loops that could destabilize markets. For creditors, the concentration of risk assessment tools in a few platforms may lead to

[17] "CNPD vs. Amazon, the largest GDPR fine on record – what do we know so far?" August 13, 2021. www.passwordprotectedlaw.com/2021/08/amazon-largest-gdpr-fine/.

[18] "BlackRock Charged with Removing Whistleblower Incentives in Separation Agreements." US Securities and Exchange Commission, Press Release, January 17, 2017. www.sec.gov/news/pressrelease/2017-14.html.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

blind spots in credit evaluation and coordinated tightening of lending conditions. Additionally, the role of data oligopolies in complex financial instruments like securitized assets echoes concerns from past financial crises. While these platforms offer undeniable benefits, their growing influence necessitates careful consideration of the potential risks to market stability, diversity of investment strategies, and overall financial system resilience.

10.4.1 *Potential Harms to Financial Consumers*

One of the most important concerns with financial data oligopolies like BlackRock's Aladdin is their potential impact on financial consumers – ordinary individuals who use financial services, invest their savings, or rely on credit. These retail consumers often have little awareness of the extent to which their financial well-being is affected by the operations of powerful data platforms behind the scenes. The first obvious concern relates to data privacy and surveillance. Aladdin appears to collect vast amounts of data about consumer activity to identify patterns and trends in consumer consumption.[19] Aladdin must continue to scale not just the amount of data but also the types of data it collects and analyzes to maintain its competitive advantage (Zetzsche et al. 2020).[20] The more BlackRock collects nonfinancial data, such as GPS locations and online behavior, the greater the risk to consumers that their information is being misused, for commercial purposes or other harmful objectives. The massive centralization of data within a small number of platforms also makes them lucrative targets for cyberattacks or any other form of data breach, potentially exposing consumers to identity theft or financial fraud. Any failures of Aladdin can cause severe harm to consumers (Fraser 2022).

Furthermore, pervasive data surveillance enabled by financial platforms could lead to discriminatory practices. For instance, financial companies may use insights from these platforms to engage in "digital redlining," where certain consumers or even smaller companies are excluded from financial services based on data-driven risk assessments (Friedline and Chen 2021). Digital redlining occurs when lenders use algorithmic models based on data analytics to exclude specific groups of consumers from financial products, often based on factors like zip codes, income levels, race, or even social media activity. While such practices may not be explicitly illegal, they can result in discriminatory outcomes that disproportionately affect minority or low-income communities. Platforms like Aladdin, which consolidate vast amounts of consumer data and apply sophisticated algorithms, could inadvertently reinforce these biases if not carefully monitored. If data models incorporate biased assumptions or historical data that reflects past discriminatory practices, they may perpetuate exclusionary patterns in lending. This can lead to financial

[19] "When Aladdin Meets Ambani: What JV with BlackRock means for Jio Financial Services," *Economic Times*, July 28, 2023.

[20] "Blackrock Is Making Big Data Bigger," *Institutional Investor*, November 1, 2016.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

exclusion and exploitation, as marginalized groups are either denied access to fair financial products or steered toward higher-cost, riskier alternatives. Over time, this exacerbates the wealth gap and deepens systemic financial inequalities.

Moreover, there is the risk that financial data oligopolies may facilitate financial exploitation of consumers (Das 2016, 27; Reynolds 2017, 18–21), including predatory lending (US Senate 2018, 51; US Congress 2019, 2). Abusive loan terms can be imposed on borrowers, often targeting vulnerable individuals such as low-income consumers, those with poor credit histories, or minority communities. Financial data platforms like BlackRock's Aladdin, which aggregate vast amounts of consumer financial data, may indirectly contribute to such exploitative practices, if their insights are misused or if the centralization of data leads to greater disparities in how consumers are treated by financial institutions. Financial data oligopolies may enable the exploitation of consumer data by identifying financially vulnerable individuals (US Congress 2019, 16–17). With access to granular data on consumers' spending patterns, credit history, income, and even social behaviors, financial companies using platforms like Aladdin can build detailed profiles of potential borrowers. While this data can be used to assess creditworthiness and manage risk, it can also be used to target consumers with exploitative loan products. For example, lenders might use data insights to offer high-interest payday loans or subprime mortgages to individuals who are unlikely to qualify for traditional credit and can least afford such predatory products, but must accept them due to lack of alternatives.

Companies using platforms like Aladdin may develop highly optimized pricing strategies based on consumer data, allowing them to extract maximum profit from specific segments of the population. This can lead to the proliferation of high-fee financial products such as payday loans, subprime credit cards, or predatory auto loans, which impose significant costs on consumers, including hidden costs. Financial companies may employ data-driven marketing strategies that specifically target low-income consumers with unfavorable terms, taking advantage of their limited access to competitive loan products. The use of sophisticated data analytics makes it easier for lenders to prey on financially vulnerable individuals, further exacerbating financial inequalities. Financial companies may leverage data insights to identify consumers who are less financially literate or more likely to overlook the fine print in loan agreements. These consumers may be saddled with loans that come with hidden fees, balloon payments, or punitive interest rates, making it difficult for them to repay their debts and trapping them in cycles of debt. In this way, financial data oligopolies may enable the use of data to exploit the most financially vulnerable consumers (US Congress 2019, 9, 16–17; Bartlett et al. 2022), undermining their financial well-being.

Additionally, financial data oligopolies may facilitate reduced competition and consumers' loss of autonomy and choice in the financial market (US Congress 2019, 8). Aladdin and similar platforms wield enormous influence over how financial companies evaluate risk and allocate capital. This concentration of power can lead to reduced competition in the financial services industry, as smaller firms struggle to

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

compete with the data analytics capabilities of larger companies using Aladdin. Consumers may have fewer choices when it comes to where they invest or borrow, as market concentration reduces the number of available financial products tailored to their needs.

The centralization of financial data also risks creating pricing and access disparities for financial consumers (US Senate 2018, 51; Bartlett et al. 2022). Large financial companies using Aladdin's platform benefit from economies of scale and superior data analytics, allowing them to optimize their operations and pricing strategies. Smaller financial companies without access to such powerful tools may struggle to compete, leading to higher costs for consumers in certain sectors. This can create a financial landscape where large, well-capitalized companies offer better rates or products, while smaller players may charge more for less competitive services. Wealthier consumers who are more likely to engage with larger companies may enjoy better financial products, while low-income consumers or those in underserved markets may be forced to pay higher prices, leading to worsen financial inequalities (Bartlett et al. 2022, 55–56).

To illustrate how financial data platforms like BlackRock's Aladdin can undermine the position of financial consumers as a community member, erode the community governance of financial data commons, and hinder the attainment of outcomes that community members may value, consider Jio BlackRock, a 50:50 joint venture that combines BlackRock's expertise with data provided by Jio Financial Services (JFS). While this partnership aims to deliver tech-enabled access to investment solutions for millions of investors in India (BlackRock 2023), it will also harness vast amounts of data to assist JFS in expanding its lending business to consumers.[21] Yet, this effort to democratize financial services may pose risks. Reliance Jio, India's telecom giant and the parent company of JFS, has an extensive digital footprint in India, managing data from telecom, retail, and digital services. Integrating this data with financial data and insights from BlackRock's Aladdin creates immense potential for personalized services, but also raises significant concerns about privacy, data sharing, and profiling. As JFS plans to use advanced data analytics as a basis for consumer lending, leveraging information from credit bureaus, account aggregators, and consumer patterns,[22] this comprehensive data ecosystem may help develop detailed consumer profiling and surveillance, which can lead to concerns about targeted advertising, overreach, and misuse. These partnerships could exploit combined consumer data to push high-risk financial products, create opaque credit-scoring mechanisms, implement price discrimination, or engage in other unfair practices that can harm consumers' interests (Pandit

[21] "BlackRock and Jio Financial Services Agree to Form Joint Venture to Enter India's Asset Management Industry." BlackRock, Press release, July 26, 2023; "The BlackRock and Jio Financial Services Mutual Fund Joint Venture: All You Need to Know." *Economic Times*, October 18, 2024.

[22] When Aladdin Meets Ambani: What JV with BlackRock means for Jio Financial Services." *Economic Times*, July 28, 2023.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

and Javed 2021, 215–216). Moreover, the reliance on technology and data-driven models may unintentionally exclude populations with limited digital literacy or access to reliable internet.

For example, in rural areas where smartphone penetration remains low, the digital-first approach of the joint venture could marginalize less tech-savvy consumers. Furthermore, data-driven credit scoring could lead to biased assessments. For instance, individuals lacking substantial digital footprints or with limited formal financial histories might face higher interest rates or outright rejection of financial products. This perpetuates existing inequities rather than addressing them. The BlackRock-JFS venture combines extensive consumer data with AI for decision-making. If not carefully designed, these systems may encode biases, leading to discriminatory practices. Algorithms might prioritize customers in urban centers or specific socioeconomic brackets, creating systemic inequalities. There is also the risk of unfair terms and predatory practices. The competitive advantages of BlackRock's financial expertise and Jio's expansive consumer base could pressure smaller financial institutions, potentially reducing competition. A monopolistic or oligopolistic environment might allow JFS to dictate unfavorable terms to consumers, such as high fees or restrictive product conditions. The partnership's promise of "low-cost" financial products could also obscure hidden costs or cross-selling practices that burden consumers.

The history of numerous consumer complaints against the Reliance Jio group suggests that concerns about potential unfair practices facilitated by BlackRock's Aladdin platform in partnership with JFS may have merit. For instance, there have been documented cases of service deficiencies, such as slow internet speeds and connectivity issues, excessive charges, price hikes, delayed refunding, and poor service to rural consumers, which have led to consumer dissatisfaction and legal complaints against Reliance group.[23] These instances highlight a possible pattern of unfair practices harming consumers' interests that could extend into the financial services domain if not addressed. While the regulatory framework in Western countries is stronger than in India, the likelihood of unfair practices that harm financial consumers is nonetheless real.

10.4.2 *Consumer Data Trusts and the Building of Data Commons*

As we have seen, financial consumers, as stakeholders in the governance of financial data commons, have the potential to play a pivotal role in overseeing financial data oligopolies and contributing to the development of the community governance of financial data commons. This engagement can represent a shift toward more participatory models of data governance, aligning with emerging concepts of data

[23] "Flipkart #1 in Consumer Complaints Followed by Jio, Amazon; Ecommerce #1 in Complaints!?" Trak.in, November 18, 2019; "Delay in Refunding 3,536 Costs Telecom Firm 15,000," *Times of India*, February 12, 2024.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

stewardship and digital citizenship and departing from disclosure–individual consent models. Specifically, consumer associations can evolve into more formalized entities, such as consumer data trusts (Delacroix and Lawrence 2019; Blankertz 2020), which may act as intermediaries aggregating and representing consumer interests vis-à-vis data oligopolies. These trusts can leverage technical and legal expertise, as well as enhanced bargaining power, to oversee financial data oligopolies, including negotiating more favorable terms of data use on behalf of consumers. This approach addresses the power imbalance between individual consumers and financial companies.

The potential of consumer data trusts in *commonizing* and governing financial data, and holding financial data oligopolies to account, is exemplified by a recent court decision that underscores the growing recognition of collective consumer rights and the legal standing of entities representing these collective interests. The decision in *Meta v Federation of German Consumer Associations* (2024)[24] illustrates the role that consumer associations can play in overseeing companies, including data oligopolies and their financial technologies. The ruling clarified the legal standing of entities that may bring a complaint for data privacy breaches, and established that authorized entities, such as consumer associations, can bring representative actions on behalf of data subjects when their rights are infringed during data processing. In reaching this conclusion, the court interpreted Article 80(2) of the GDPR and broadened the scope of representative actions.

The ruling enabled consumer associations to challenge not only data breaches but also the inadequate provision of information, expanding the oversight that such entities can exercise. This gives consumer associations the ability to play a proactive role in shaping data practices, rather than merely reacting to data breaches. Moreover, by establishing clearer standards for transparency in data processing, this case sets a benchmark for the quality and accessibility of information that companies must provide to consumers. The decision reaffirmed Meta's obligation to provide clear, concise, and easily accessible information about the purposes of data processing and the recipients of the data. The case also carries significant cross-border implications. Although it involves a German consumer association challenging a global company like Meta, the case highlights how consumer associations or similar entities can operate across borders to protect consumer rights in a globalized digital economy. By lowering barriers for individuals, the ruling makes it easier for consumers to have their rights protected through consumer associations' representative action without needing to bring complex legal challenges themselves.

This decision of the European court provides some basis to suggest that representation may allow for the gradual creation of data trusts (Ruhaak 2020, 17). Consumer associations such as the German one can potentially act similarly to a consumer data

[24] Meta Platforms Ireland Ltd v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV (Case C-757/22).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

trust by aggregating the interests of individual consumers to bring a representative action against giant tech companies, such as Meta. While the existing legal framework, including Article 80 of the GDPR and this court decision, needs to be expanded to clearly permit data trusts (Ruhaak 2020, 17; Blankertz 2020, 26; Iwan-Sojka 2024; Ruhaak 2020, 17), these formal rules may provide some initial legal basis for empowering consumer associations to act as data trusts with a view to holding tech giants accountable. Collective action by consumer associations to oversee financial companies, including data oligopolies, may help address the information and power asymmetries between consumers and tech companies. The court's decision does not go far enough in detailing or legalizing consumer associations' powers and oversight role, but it may enable such associations to develop strategies or practices, or informal rules, aiming at supervising financial companies and their financial technologies, including eventually BlackRock's Aladdin.

Formal rules grounded in the court's decision empower consumer associations acting like consumer data trusts to contribute to building a community governance of financial data, overcoming barriers to data commons created by data oligopolies. Consumer associations or consumer data trusts can, for instance, help curb data oligopolies' self-serving rules, such as partnerships with tech companies and data-related liability exclusion agreements. Ultimately, consumer associations can rebalance power dynamics, enhance transparency, and protect consumers' interests. These associations or trusts can go far in promoting the development of formal and informal rules that favor the attainment of important social goods – such as preventing financial exclusion, exploitation, surveillance and privacy invasion – that the governing community values. Recent developments in open banking laws and policies, which grant financial consumers greater legal powers (rights to access, transparency, data portability, switching, and protection against the misuse of their data), expand the formal rules governing financial data. These advancements reinforce consumers' potential to engage in the community governance of financial data commons and further empower consumer associations or consumer data trusts to hold data oligopolies accountable.

It will be important to explore the feasibility and effectiveness of this potential of consumer associations acting as data trusts. It will be critical to think about internal governance structures and trustees' duties, and other facilitative formal and informal rules-in-use. Addressing questions pertaining to the use of technology to manage shared consumer data and implement their oversight practices (e.g., enforcement technologies) will be crucial, especially in the fact of data oligopolies' opposing strategies and control over data infrastructures.

10.5 CONCLUSION

This research has examined the growing trend of financial companies leveraging fintech to monopolize financial data, and its implications for the concept of

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

financial data as a shared resource. Relying on the lens of the GKC framework, the chapter explored how this trend prevents the community governance of financial data, excludes important stakeholders, and disproportionately benefits a select few. The case study of BlackRock's Aladdin platform illustrated the potential for massive financial data collection that leads to the formation of data oligopolies. This example underscores the risks of financial exclusion, exploitation, and worsening wealth concentration that can result from such concentrated control over financial data.

The analysis also revealed a promising counterforce to this trend: consumer associations acting as data trusts. These entities have the potential to play a crucial role in overseeing financial data oligopolies while fostering the development of community-governed data commons. The recent European court decision allowing a German consumer association to bring a representative action against Meta-Facebook demonstrates the growing legal recognition of this potential. Furthermore, the emergence of open banking laws and policies provides additional tools for consumer empowerment, reinforcing the capacity for consumer-led activism in shaping financial data governance. The transformative potential of consumer-led activism suggests a paradigm shift away from individual consent models toward a more collective, community-oriented approach to data governance. Looking forward, further research is needed to explore the practical implementation of consumer associations as data trusts, including the development of appropriate legal frameworks, technological infrastructures, and governance models. Additionally, investigating the potential synergies between open banking initiatives and consumer data trusts could yield valuable insights for policymakers and practitioners alike.

REFERENCES

Anidjar, Leon Y., and Inbar Mizrahi-Borohovich. 2019. "Reinventing Credit Data Sharing Regulation." *Southern California Interdisciplinary Law Journal* 29(2): 177–225.

Armour, John, and Horst Eidenmuller. 2020. "Self-Driving Corporations?" *Harvard Business Law Review* 10(1): 87–116.

Azar, José, Martin C. Schmalz, and Isabel Tecu. 2018. "Anti-Competitive Effects of Common Ownership." *Journal of Finance* 73(4): 1513–1565.

Backus, Matthew, Christopher Conlon, and Michael Sinkinson. "Common Ownership in America: 1980–2017." *American Economic Journal: Microeconomics* 13(3): 273–308.

Bartlett, Robert, Adair Morse, Richard Stanton, and Nancy Wallace. 2022. "Consumer-Lending Discrimination in the FinTech Era." *Journal of Financial Economics* 143(1): 30–56.

Baxter, David, Paul Trott, and Paul Ellwood. 2023. "Reconceptualising Innovation Failure." *Research Policy* 52(7): 104811.

Blankertz, Aline. 2020. *Designing Data Trusts: Why We Need to Test Consumer Data Trusts Now*. Stiftung Neue Verantwortung. www.interface-eu.org/storage/archive/files/designing_data_trusts_e.pdf.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

Chakravortl, Bhaskar. 2021. "Big Tech's Stranglehold on Artificial Intelligence Must Be Regulated." *Foreign Policy*, August 11, 2021. https://foreignpolicy.com/2021/08/11/artificial-intelligence-big-tech-regulation-monopoly-antitrust-google-apple-amazon-facebook/

Crawford, Sue E., and Elinor Ostrom. 1995. "A Grammar of Institutions." *American Political Science Review* 89(3): 582–600.

Das, Sanjiv Ranjan. 2016. "Big Data's Big Muscle." *Finance & Development* 53(3): 26–28.

Delacroix, Sylvie, and Neil D. Lawrence. 2019. "Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance." *International Data Privacy Law* 9(4): 236–252.

Fan, Mary D. 2021. "The Right to Benefit from Big Data as a Public Resource." *New York University Law Review* 96(5): 1438–1444.

Fischer, Benjamin. 2021. "The Rise of the Data-Opoly: Consumer Harm in the Digital Economy." *Washington University Law Review* 99(2): 729–750.

Fisher, Angelina, and Thomas Streinz. 2022. "Confronting Data Inequality." *Columbia Journal of Transnational Law* 60(3): 829–956.

Fracassi, Cesare, and William J. Magnuson. 2021. "Data Autonomy." *Vanderbilt Law Review* 74(2): 327–383.

Fraser, Max. 2022. "Biden and BlackRock." *New Labor Forum* 31(2): 105–108.

Friedline, Terry, and Zibei Chen. 2021. "Digital Redlining and the Fintech Marketplace: Evidence from US Zip Codes." *Journal of Consumer Affairs* 55(2): 366–388.

Frischmann, Brett M., Michael J. Madison, and Katherine J. Strandburg. 2014. "Governing Knowledge Commons." In *Governing Knowledge Commons*, ed. Brett M. Frischmann, Michael J. Madison, and Katherine J. Strandburg, 1–43. New York: Oxford University Press.

Houser, Kimberly A., and John W. Bagby. 2023. "The Data Trust Solution to Data Sharing Problems." *Vanderbilt Journal of Entertainment & Technology Law* 25(1): 113–180.

Iwan-Sojka, Dominika. 2024. "The Inclusive Data Governance Models for Algorithms – A Dream of the Already Convinced or a Realistic Way of Action?" *Information & Communications Technology Law* 34(1): 1–14.

Johnson, Garrett A., Scott K. Shriver, and Samuel G. Goldberg. 2023. "Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR." *Management Science* 69(10): 5695–5721.

Jones, Charles I., and Christopher Tonetti. 2020. "Nonrivalry and Economics of Data." *American Economic Review* 110(9): 2819–2858.

Jurcys, Paulius, Christopher Donewald, Mark Fenwick, et al. 2021. "Ownership of User-Held Data: Why Property Law Is the Right Approach." *Harvard Journal of Law & Technology Digest*, September 21, 2021. https://jolt.law.harvard.edu/digest/ownership-of-user-held-data-why-property-law-is-the-right-approach

Khan, Lina M. 2017. "Amazon's Antitrust Paradox." *Yale Law Journal* 126(3): 710–805.

Lancieri, Filippo. 2022. "Narrowing Data Protection's Enforcement Gap." *Maine Law Review* 74(1): 15–72.

MacCarthy, Mark. 2011. "New Directions in Privacy: Disclosure, Unfairness, and Externalities." *I/S: A Journal of Law and Policy for the Information Society* 6: 425–456.

Madison, Michael J. 2019. "Biobanks as Knowledge Institutions." In *Global Genes, Local Concerns*, ed. Timo Minssen, Janne Rothmar Herrman, and Jens Schovsbo, 22–40. Cheltenham: Edward Elgar.

Madison, Michael J. 2014. "Commons at the Intersection of Peer Production, Citizen Science, and Big Data: Galaxy Zoo." In *Governing Knowledge Commons*, ed. Brett M. Frischmann, Michael J. Madison, and Katherine J. Strandburg, 209–254. New York: Oxford University Press.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

Madison, Michael J. 2024. "Knowledge Commons Past, Present, and Future." *Lewis & Clark Law Review* 28(2): 303–331.
Martens, Bertin. 2018. "The Importance of Data Access Regimes for Artificial Intelligence and Machine Learning." JRC Digital Economy Working Paper 2018–09. https://ssrn.com/abstract=3357652.
McIntosh, Daniel. 2019. "We Need to Talk About Data: How Digital Monopolies Arise and Why They Have Power and Influence." *Journal of Technology Law and Policy* 23(2): 185–213.
Mulgan, Geoff, and Vincent Straub. 2019. "The New Ecosystem of Data Trusts." Medium, February 26, 2019. https://medium.com/@vincejstraub/the-new-ecosystem-of-data-trusts-36901fc59010.
Pandit, Urshila, and Sanah Javed. 2021. "Antitrust and Privacy Concerns: A Dilemma across Jurisdictions." *RGNUL Financial and Mercantile Law Review* 8(2): 203–246.
Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.
Purtova, Nadya, and Gijs van Maanen. 2024. "Data as an Economic Good, Data as a Commons, and Data Governance." *Law, Innovation and Technology* 16(1): 1–42.
Reynolds, Faith. 2017. *Open Banking: A Consumer Perspective*. London: Barclays.
Ruhaak, Anouk. 2020. "Data Trusts in Germany and Under the GDPR." *Algorithm Watch*, December 6, 2020. https://algorithmwatch.org/en/wp-content/uploads/2020/12/Data-trusts-in-Germany-and-under-the-GDPR-Anouk-Ruhaak-AlgorithmWatch-2020.pdf.
Ruhaak, Anouk. 2021. "How Data Trusts Can Protect Privacy." *MIT Technology Review*, February 24, 2021. www.technologyreview.com/2021/02/24/1017801/data-trust-cybersecurity-big-tech-privacy/.
Sanfilippo, Madelyn R., Brett M. Frischmann, and Katherine J. Strandburg, eds. 2021. *Governing Privacy in Knowledge Commons*. Cambridge: Cambridge University Press.
Sanfilippo, Madelyn R., Brett M. Frischmann, and Katherine J. Strandburg. 2018. "Privacy as Commons: Case Evaluation through the Governing Knowledge Commons Framework." *Journal of Information Policy* 8: 116–166.
Scassa, Teresa. 2020. "Designing Data Governance for Data Sharing: Lessons from Sidewalk Toronto." *Technology and Regulation* 2020: 44–56.
Serafeim, George. 2018. "Facebook, BlackRock, and the Case for Purpose-Driven Companies." *Harvard Business Review*, January 16, 2018. https://hbr.org/2018/01/facebook-blackrock-and-the-case-for-purpose-driven-companies.
Shkabatur, Jennifer. 2019. "The Global Commons of Data." *Stanford Technology Law Review* 22(2): 354–411.
Solove, Daniel J. 2021. "The Myth of the Privacy Paradox." *George Washington Law Review* 89(1): 1–51.
Steele, Graham. 2020. *The New Money Trust: How Large Money Managers Control Our Economy and What We Can Do About It*. American Economic Liberties Project. www.economicliberties.us/wp-content/uploads/2020/11/Working-Paper-Series-on-Corporate-Power_8_FINAL.pdf.
Stucke, Maurice E. 2022. *Breaking Away: How to Regain Control Over Our Data, Privacy and Autonomy*. New York: Oxford University Press.
US Congress, House, Committee on Financial Services, *Banking on Your Data: The Role of Big Data in Financial Services: Hearing Before the House Committee on Financial Services*. 116., 1st sess., November 21, 2019, written testimony of Lauren Saunders, Associate Director of the National Consumer Law Center, https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-wstate-saundersl-20191121.pdf.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010

US Senate, Committee on Banking, Housing, and Urban Affairs. *Fintech: Examining Digitization, Data, and Technology*. 115th Cong., 2nd sess., September 18, 2018. Prepared Statement of Saule T. Omarova, Professor of Law at Cornell University, www.congress.gov/115/chrg/CHRG-115shrg32753/CHRG-115shrg32753.pdf.

Van Geuns, Jochai, and Ana Brandusescu. 2020. "Shifting Power through Data Governance." Mozilla Foundation, September 16, 2020. https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/shifting-power-through-data-governance/.

Zarkadakis, George. 2020. "Data Trusts Could Be the Key to Better AI." *Harvard Business Review*, November 10, 2020. https://hbr.org/2020/11/data-trusts-could-be-the-key-to-better-ai.

Zetzsche, Dirk A., William A. Birdthisle, Douglas W. Arner, and Ross P. Buckley. 2020. "Digital Finance Platforms: Toward a New Regulatory Paradigm." *University of Pennsylvania Journal of Business Law* 23(1): 273–339.

Zetzsche, Dirk A., Douglas Arner, and Ross Buckley. 2023. "Sustainability, Financial Inclusion and Efficiency: A Trilemma or a Trifecta for the Regulation of Digital Finance?" *Banking and Finance Law Review* 39(3): 445–466.

Zook, Matthew, and Ian Spangler. 2023. "A Crisis of Data? Transparency Practices and Infrastructures of Value in Data Broker Platforms." *Annals of the American Association of Geographers* 113(1): 110–128.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 02:50:11, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431859.010