Tech REG CHRONICLE

BROKERING REFORM: REGULATION OF DATA MARKETS

OCTOBER 2023

CPI COMPETITION POLICY INTERNATIONAL

Competition Policy International, a What's Next Media and Analytics Company

LETTER FROM THE EDITOR

Dear Readers,

In an age where data is often likened to oil, its extraction, refinement, and sale have become central to the global economy. A particular type of entities has emerged as central – data brokers. These previously obscure firms are responsible for aggregating, analyzing, and selling vast amounts of personal and behavioral data from countless sources, and their influence growing silently but significantly behind the scenes.

The centrality of data to modern commerce, society, and politics makes the role of data brokers both essential and controversial. As the gatekeepers of invaluable information that can shape everything from individual consumer preferences to national elections, the unchecked power and reach of these entities have raised significant concerns regarding privacy, competition, market access, and the potential for abuse.

This edition of the Chronicle opens with a CPI TechREG Talks… interview with Mr. **Samuel Levine**, Director of the U.S. FTC's Bureau of Consumer Protection. In a wide-ranging interview, Mr. Levine discusses the risks posed to consumers by data brokers, the balance between the FTC's role as a consumer protection and antitrust authority in regulating data brokers, and the FTC's enforcement priorities in this domain.

Jessica L. Rich provides an overview of issues surrounding data brokers in the U.S. Policymakers have long debated whether new laws are needed to restrict the practices of data brokers, but until recently, regulation in the U.S. has been limited. During the past couple of years, however, there's been flurry of regulatory activity affecting data brokers at the federal and state levels. Of particular note, last month, California passed a new law (the Delete Act) that will allow consumers, in one step, to delete the data that all data brokers in the state have collected about them and to prevent future sales of their data.

As **Jeanne Mouton & Christian Rusche** underline, data brokers occupy an increasingly important and profitable role in the economy. Their paper adds to the discussion on whether this increasing role also requires additional regulation. After defining "data brokers," the paper discusses extent of data being sold and likely problems deriving from this business model. It then reviews recent EU regulation of the data economy, focusing on mandatory data sharing by data brokers.

Andreas Schauer & Daniel Schnurr address how data brokers are envisioned to improve the free flow of data and thus facilitate data access for a broad range of organizations. New data broker business models for personal data promise to directly compensate individuals for their co-creation of data. However, there have also been significant concerns about the well-functioning of today's data economy, especially with respect to the practices of current data brokers, the protection of individuals' privacy, and the general transparency of the data economy. The piece discusses key strands of the academic literature on data brokers and highlights challenges for data markets and data brokers. It highlights recent findings on the economic impact of data brokers in digital markets and scrutinizes the concept of personal data brokers. Finally, it discusses recent policy initiatives in the European Union, most notably the Data Governance Act and the Data Act.

Next, **Lothar Determann & Teisha Johnson** look at tradeoffs between competition and privacy in the regulation of data brokers. They examine the importance of data protection for individual privacy and access to data for competition , discuss the role of data brokers as to data privacy and sharing, and then review existing, new, and proposed regulations of data brokers. The authors note that consumers may benefit from added privacy protections if the new laws and regulatory actions enhance data accuracy, the quality of disclosures, transparency, and fair information processing practices. Nonetheless, consumers may suffer from increased fraud, reduced competition, fewer charge-free information services, price increases, and stifled innovation if additional regulations result in reduced competition, data sharing, and information availability. Smart, balanced regulations can create an environment where data brokers have a positive impact on the competitive marketplace.

In an era marked by increasing digitalization, the flow of personal data has become a focal point for both competition and privacy concerns. **Adriana Hernandez Perez** explains that while illicit personal data collection remains a widespread issue, a parallel concern arises from the extensive consent to share personal data, often attributed to lack of awareness regarding the potential risks of personal data sharing and to high transaction costs. At the heart of this discussion lies the pivotal role of data brokers, acting as intermediaries responsible for the collection, processing, and selling data. In the face of an ever-evolving landscape, the policies that remain consistent and robust in the face of advancements in behavioral economics literature are those focused on strengthening market information flows and consumer education.

Finally, **Chandni Gupta** argues that keeping the digital economy's modern-day alchemists, the data brokers, accountable needs a reset in the regulatory landscape which was not developed with such business models in mind. Manipulation, discrimination and exclusion, lack of control and data breaches are just some of the harms that consumers are exposed to when their data is mined and sold in a way that profits businesses despite often leaving consumers worse-off. Australian laws to date have not been adequate to mitigate these harms. The evolving Australian regulatory landscape where both, laws against unfair practices and stronger privacy protections in the offing may lead to a change in how these alchemists operate. There is also a broader consideration of how safety and care need to be embedded into the law so businesses are proactively mitigating harm in the way they collect, share and use data.

In sum, this Chronicle delves into the key issues surrounding antitrust regulation and data brokers. The various contributions explore the rise of data brokers, assess current regulations, and highlight potential gaps. The challenges are clear: ensuring fair competition and transparency while fostering innovation in the digital age. We hope this Chronicle prompts further research and discussion in this important area.

As always, many thanks to our great panel of authors.

Sincerely,

CPI Team

TABLE OF CONTENTS

CPI COMPETITION POLICY® INTERNATIONAL

SUMMARIES

CPI TECHREG TALKS...
...with Samuel A.A. Levine

In this edition of CPI TechREG Talks… we have the pleasure of discussing issues of consumer law and antitrust protection as they relate to consumer data with Mr. Samuel A.A. Levine, Director of the U.S. FTC's Bureau of Consumer Protection. Thank you, Mr. Levine for taking this time to respond to CPI's questions on this fascinating and timely subject.

DATA BROKERS IN THE HOT SEAT: A CONTINUING STORY
By Jessica L. Rich

For years, policymakers have debated whether new laws are needed to restrict the practices of data brokers – companies that collect consumers' data from various sources, process and package it, and then sell it to individuals and businesses for marketing and advertising, fraud detection, risk mitigation, and locating people, among other purposes. Supporters of stronger laws argue that data brokers operate behind the scenes, collecting and selling sensitive consumer data to a vast array of purchasers, who use it to make important decisions about consumers. Opponents argue that data brokers provide valuable services that help businesses and the government serve the public. Until recently, regulation of data brokers in the U.S. has been limited. During the past couple of years, however, there's been flurry of regulatory activity affecting data brokers at the federal and state levels. Of particular note, last month, California passed a new law (the Delete Act) that will allow consumers, in one step, to delete the data that all data brokers in the state have collected about them and to prevent future sales of their data. This article examines the recent regulatory activity surrounding data brokers and predicts continued focus on this industry as we move to 2024.

DATA BROKER REGULATION - COMPETITION V. PRIVACY CONSIDERATIONS: TRADE-OFFS
By Lothar Determann & Teisha Johnson

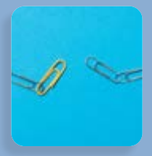
In the ongoing debate concerning data broker regulation, tradeoffs between competition and privacy are not always holistically appreciated. This article examines the importance of data protection for individual privacy and access to data for competition , discusses the role of data brokers as to data privacy and sharing, and then reviews existing, new, and proposed regulations of data brokers. Consumers may benefit from added privacy protections if the new laws and regulatory actions enhance data accuracy, the quality of disclosures, transparency, and fair information processing practices. But, consumers may suffer from increased fraud, reduced competition, fewer charge-free information services, price increases, and stifled innovation if additional regulations result in reduced competition, data sharing, and information availability. Smart, balanced regulations can create an environment where data brokers have a positive impact on the competitive marketplace.

IS PERSONAL DATA STILL UP FOR GRABS?
By Adriana Hernandez Perez

In an era marked by increasing digitalization, the flow of personal data has become a focal point for both competition and privacy concerns. While illicit personal data collection remains a widespread issue, a parallel concern arises from the extensive consent to share personal data, often attributed to lack of awareness regarding the potential risks of personal data sharing and to high transaction costs. This article explores the intricate landscape of data economics and data privacy in the digital era, shedding light on both the advantages and risks associated with the widespread use of information. At the heart of this discussion lies the pivotal role of data brokers, acting as intermediaries responsible for the collection, processing, and selling data. In the face of an ever-evolving landscape, the policies that remain consistent and robust in the face of advancements in behavioral economics literature are those focused on strengthening market information flows and consumer education.

TO SHARE OR NOT TO SHARE: REGULATING DATA BROKERS
By Jeanne Mouton & Christian Rusche

Data has become an increasingly important input in the economy. Hence, data and access to data play an increasingly key role in the global economy and for innovation and are crucial for the competitiveness of companies and the EU economy. Data brokers benefit from this development because they collect data from a wide variety of sources and offer access to this data, as well as products and services based on it. However, there is a trade-off between realizing the benefits of data by sharing as much data as possible and protecting consumers' personal data and the intellectual property ("IP")-related data of companies. In this article, two extreme solutions have been discussed for regulating data brokers. On the one hand, there is mandatory data sharing, which is supposed to reduce the incentives for data brokers and consumers to share data. On the other hand, banning data brokers' business model decreases data sharing and represents an extreme intervention. Both options are discussed as well as the recent regulations at the EU level that affect the data economy.



DATA BROKERS: INTERMEDIARIES FOR MORE EFFICIENT DATA MARKETS?
By Andreas Schauer & Daniel Schnurr

Data brokers play a pivotal role in addressing key policy challenges of data fragmentation and data concentration in the digital economy. In particular, data brokers are envisioned to improve the free flow of data and thus facilitate data access for a broad range of organizations. Furthermore, new data broker business models for personal data promise to directly compensate individuals for their co-creation of data. However, there have also been significant concerns about the well-functioning of today's data economy, especially with respect to the practices of current data brokers, the protection of individuals' privacy, and the general transparency of the data economy. In this article, we review and summarize key strands of the academic literature on data brokers and highlight challenges for data markets and data brokers that arise from the special characteristics of data as an economic good. We then highlight recent findings on the economic impact of data brokers in digital markets and scrutinize the concept of personal data brokers. Finally, we discuss recent policy initiatives in the European Union, most notably the Data Governance Act and the Data Act, with respect to their implications for data brokers and the goal to facilitate the emergence of well-functioning data markets.

KEEPING UP WITH THE ALCHEMISTS – REGULATING DATA BROKERS IN AUSTRALIA
By Chandni Gupta

Keeping the digital economy's modern-day alchemists, the data brokers, accountable needs a reset in the regulatory landscape which was not developed with such business models in mind. Manipulation, discrimination and exclusion, lack of control and data breaches are just some of the harms that consumers are exposed to when their data is mined and sold in a way that profits businesses despite often leaving consumers worse-off. Australian laws to date have not been adequate to mitigate these harms. The evolving Australian regulatory landscape where both, laws against unfair practices and stronger privacy protections in the offing may lead to a change in how these alchemists operate. There is also a broader consideration of how safety and care need to be embedded into the law so businesses are proactively mitigating harm in the way they collect, share and use data.

TechREG TALKS...

...WITH

SAMUEL A.A. LEVINE

Director of the U.S. FTC's Bureau of Consumer Protection.

In this edition of CPI TechREG Talks … we have the pleasure of discussing issues of consumer law and antitrust protection as they relate to consumer data with Mr. Samuel A.A. Levine, Director of the U.S. FTC's Bureau of Consumer Protection. Thank you, Mr. Levine for taking this time to respond to CPI's questions on this fascinating and timely subject.

Q1

In a recent speech, you spoke of a trend of data brokers looking to "maximize" how much information they can extract from consumers. Can you briefly elucidate these concerns? What, in your view, is different about today's economy and technology that allows for such trends (as opposed to the recent past)?

The *status quo* of pervasive commercial surveillance endangers our privacy, our financial welfare, and our liberty. With increasing precision, companies are collecting and sharing a staggering amount of information about American consumers. Without much cost or effort, anyone in the United States or abroad can obtain or infer detailed information about where Americans spend their days, sleep at night, what health conditions they have, who they associate with, as well as what their religious faith and political interests are. The trend toward maximizing the collection and monetization of personal information by data brokers and others has been gathering force over many years, so it's not a recent development at this point. Certainly, the proliferating use and variety of apps and online products and services has increased the amount of personal data that is being captured and sold.

Q2

What, in your view, are the key threats that such practices pose to consumers and citizens? Such concerns are typically framed around privacy concerns. Do you see broader issues at play (for example other Constitutional rights)?

The stakes are not limited to privacy, although those concerns are very important. Data broker practices may also adversely affect consumers' financial welfare because profiles containing personal information, and inferences generated based on such data, are increasingly used to determine if consumers qualify for a loan, insurance, jobs, or an apartment lease. Inaccurate or false data can impact decisions on job or housing applications. Further, governmental use of sensitive information about Americans, which is commercially available today, also has the potential to endanger our constitutional rights including freedom of religion, speech, assembly, and association, and freedom from unreasonable search and seizure. I am deeply concerned that the pervasiveness of tracking today may change some Americans' decision-making about whether to protest, worship, or seek healthcare. This should concern all of us.

Q3

The interplay between the FTC's antitrust and consumer protection roles are clearly at issue in this debate. How do you see concerns relating to data brokers within this matrix? Which rules do you foresee as taking center stage in this debate as it plays out?

We want to see companies compete in part on how well they protect people's privacy. Unfortunately, certain practices in this industry appear to create the opposite incentive – to maximize collection of data that can be shared and monetized. Companies' collection and use of personal data is also largely opaque to consumers which makes it difficult to create market pressures to reward privacy-enhancing business practices. These are some of the reasons that the FTC sought comment on whether to propose data protection rules, and why we've secured numerous orders requiring companies to delete, or limit the personal information that they collect, share, and retain about consumers.

Companies may engage with data brokers inadvertently. What advice would you give to corporations and citizens as regards compliance with the relevant rules?

As a starting point, companies must take action to evaluate what consumer data they collect and how they collect it. That means a comprehensive assessment of what type of consumer data they collect and if it is accurate. A critical part of this analysis is determining if the consumer data collected is sensitive and implementing policies and procedures to protect such sensitive consumer data, or technical measures to avoid collecting it in the first place. Companies need to ask more questions about vendors that are providing personal data. This includes, among other things, inspecting what consumers were promised at the time their data was collected about how it would be used, if it would be sold, to whom, and for what purpose. These inquiries also should include determining if consumers were tricked or manipulated through design techniques and dark patterns to give consent.

Companies must also do more to vet the third parties that they share consumer data with, ask more questions about how data will be used, and impose restrictions on downstream uses.

Q4

What will be your enforcement priorities in this regard over the short term? Do you foresee significant litigation on the horizon (either from the FTC or other public enforcers or from private parties)?

I can't comment on pending investigations or enforcement actions, but we've been clear in recent orders and statements about where we see concerns, especially around companies' handling of sensitive data. And if you look across the government, the FTC is not the only entity concerned about data broker practices. We are also seeing Congress, the Supreme Court, the Intelligence Community, and the CFPB expressing similar concerns about so much sensitive information about Americans being commercially available.

DATA BROKERS IN THE HOT SEAT: A CONTINUING STORY

BY JESSICA L. RICH

Of Counsel and Senior Policy Advisor for Consumer Protection, Kelley Drye & Warren LLP. Former Director, Bureau of Consumer Protection, Federal Trade Commission.

01 INTRODUCTION

For years, policymakers have debated whether new laws are needed to "rein in" the practices of data brokers – companies that collect consumers' personal data from various sources, process and package it, and then sell it to individuals and businesses for marketing and advertising, fraud detection, risk mitigation, and locating people, among other purposes.

Proponents of stronger laws cite data privacy and accuracy concerns, noting that most data brokers operate behind the scenes, unknown to consumers, and sell personal data (some of it highly sensitive) to a vast array of end users, who may use it to make important decisions about consumers. Data brokers counter that they provide valuable services that help businesses serve their customers, and help the economy operate efficiently and effectively.

To date, regulation of data brokers has been limited at both the federal and state level. Recently, however, there's been flurry of regulatory activity related to this industry, driven in part by the increased focus on data privacy concerns more generally. Whether in Congress or state legislatures, at federal agencies or the White House, many policymakers are pushing in the direction of increased regulation. This article provides an overview of the issues and recent activity surrounding data brokers, and forecasts stormy weather ahead for these companies.

02
WHAT ARE DATA BROKERS?

There's no universal definition of data brokers, especially since people with different perspectives tend to describe data brokers quite differently. For example, one data broker describes its business as follows:

> We unlock[] the power of data to create opportunities for consumers, businesses and society. At life's big moments – from buying a home or car, to sending a child to college, to growing a business exponentially by connecting it with new customers – we empower consumers and our clients to manage their data with confidence so they can maximize every opportunity. We help individuals take financial control and access financial services, businesses make smarter decision and thrive, lenders lend more responsibly, and organizations prevent identity fraud and crime.[2]

In contrast, a consumer advocacy group describes data brokers this way:

> Thousands of data brokers in the United States buy, aggregate, disclose, and sell billions of data elements on Americans with virtually no oversight. As the data broker industry proliferates, companies have enormous financial incentives to collect consumers' personal data, while data brokers have little financial incentive to protect consumer data. For these companies, consumers are the product, not the customer. Companies also maintain information about consumers that is often inaccurate, wrongfully denying them credit, housing, or even a job.[3]

In a 2014 report to Congress, the Federal Trade Commission ("FTC") (the primary consumer protection agency at the federal level, with jurisdiction over many data brokers) described data brokers somewhat more objectively as "companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual's identity, or detecting fraud."[4]

Meanwhile, California's new data broker law (SB 362, discussed in more detail below) defines a data broker as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."[5] This definition (echoed in other federal and state laws and bills) underscores one of the key issues driving concerns about data brokers – that they operate behind the scenes, collecting and selling consumers' sensitive data without most consumers' knowledge or control.

However data brokers are described or defined, they essentially collect, combine, process, and sell consumer data. They obtain this information from a range of sources, including government databases (e.g. real property and court records), publicly available sources (e.g. social media, blogs, and the internet), and commercial entities (e.g. retailers and magazine publishers). Often, they use online tools to collect the information, such as cookies, pixels, fingerprinting, application programming interfaces, or software development kits. They then combine the data, make inferences from it, and classify consumers by demographics, household income, familial status, political affiliation, hobbies, and other characteristics and preferences. A range of purchasers (individuals, businesses, and government) typically access data broker services online, and use it to find and authenticate people, detect and prevent fraud, and send consumers relevant advertising and offers, among other purposes.[6]

2 Large data broker's website. (I'm not naming the company to avoid singling out any one data broker. Other companies' narratives are similar.)

3 Electronic Privacy Information Center (EPIC) website, https://epic.org/issues/consumer-privacy/data-brokers/.

4 FTC Report, Data Brokers: A Call for Transparency and Accountability ("FTC Data Broker Report"), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (May 2014). Although this report is almost a decade old, it is still widely cited due to its in-depth examination of the practices of nine diverse data brokers.

5 SB 362 §1(c), https://legiscan.com/CA/text/SB362/2023.

03
BACKGROUND ON THE DATA BROKER DEBATE

The debate about whether and how to regulate data brokers started in the 1960s, when concerns arose about a particular type of data broker (consumer reporting agencies or "CRAs") that collect and sell consumer information for use in making decisions about consumers' eligibility for certain benefits (notably, credit, employment, and insurance). The concerns centered primarily around three issues: (1) the confidentiality of the information collected, which included consumers' credit histories, financial status, and even data about arrests and "general reputation," (2) the accuracy and currency of the information, since false or outdated information can lead to the denial of important consumer opportunities, and (3) the fact that this system of critical decisionmaking had been "built up with virtually no public regulation or supervision."[7]

In 1970, Congress passed the Fair Credit Reporting Act ("FCRA"), the nation's first commercial privacy law, to address these concerns. The FCRA imposes data privacy and accuracy requirements on CRAs that sell, and on people or entities that furnish and use, consumer data ("consumer reports") for consumer eligibility determinations (i.e. about credit, employment, insurance, and other specified benefits). Among other things, the law requires CRAs to implement "reasonable procedures" to maintain data accuracy, to allow access to consumers reports only by those with a "permissible purpose," and to discard outdated information. It also gives consumers the right to review and dispute the accuracy of the information collected about them.[8] The FCRA is considered the "mother" of commercial privacy laws in the US (described admiringly by one of my former FTC colleagues as the "magna carta" of privacy).[9]

The FCRA didn't end the discussion about data brokers, however. Since its enactment, there has been explosive growth in the data broker industry,[10] with many data brokers performing services that fall outside (or purport to fall outside) the FCRA.[11] As a result, critics of the industry have pressed for broader regulation – arguing that data brokers collect highly sensitive consumer data (about consumers' health, precise location, purchase histories, family members, etc.), make inferences and assign consumers to marketing categories ("financially challenged," "leans left," "bible lifestyle"), and sell this data with few limitations. Critics also point to use of this data by the government, contrary to civil liberties, and even stalkers, who can buy their victims' addresses online. These concerns have intensified as the ubiquity of mobile devices and technological advances have enabled data brokers to collect more detailed consumer data, and make more granular inferences and predictions, for sale to the public.[12]

In response, data brokers cite the many beneficial services they provide – such as stopping fraud against companies and the government, verifying identities for the administration of unemployment and nutrition programs, identifying potential donors for charitable and political campaigns, and allowing small businesses to reach a large customer base.[13] They also argue that existing laws already govern their use of data, and are sufficient to address any harms that occur. Notably, the FCRA (as discussed) regulates the use of

6 See e.g. FTC Data Broker Report, supra at n. 4; Congressional Research Service Report R47298 ("CRS Report"), https://crsreports.congress.gov/product/pdf/R/R47298l (Oct. 2022).

7 See e.g. National Consumer Law Center Digital Library website, https://library.nclc.org/book/fair-credit-reporting/141-overview.

8 FCRA, https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

9 Since enactment, the FCRA has been amended several times and has been actively enforced by the FTC, private plaintiffs, and, more recently, the Consumer Financial Protection Bureau (CFPB).

10 In 2021, digital marketing company Web FX estimated that there were over 4000 data brokers worldwide in an industry valued at more than $200 billion per year. See Web FX blogpost, https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/ (2021).

11 Some data brokers post disclosures stating that they are not CRAs and that purchasers cannot use their data for CRA purposes. Critics say that the data is used for such purposes anyway. See CFPB Press Release, CFPB Kicks Off Rulemaking to Remove Medical Bills from Credit Reports ("CFPB Rulemaking Proposal"), https://www.consumerfinance.gov/about-us/newsroom/cfpb-kicks-off-rulemaking-to-remove-medical-bills-from-credit-reports/ (Sept. 21, 2021).

12 See e.g. FTC Data Broker Report, *supra* at n. 4; CRS Report, *supra* at n. 6.

13 See, e.g. Consumer Data Industry Association Website, https://notosb362.org/.

data for eligibility determinations; the Gramm-Leach-Bliley Act ("GLBA") protects sensitive financial information;[14] numerous state privacy laws[15] now provide a range of privacy protections in those states; and the FTC Act gives the FTC broad and flexible authority to target data brokers that engage in "unfair or deceptive" practices.[16]

04
THE CURRENT FOCUS ON DATA BROKERS

Recently, the focus on data brokers has escalated, fueled by the increased, bipartisan focus on privacy in general[17] and, the sizeable growth of the data broker industry. For some policymakers, the Supreme Court's overturning of *Roe v. Wade* has added another important dimension to the debate – i.e. the worry that law enforcers in anti-abortion states will be able to purchase data about women's health and location in order to enforce anti-abortion laws. On August 15, the White House convened a roundtable of government officials, academics, advocates, and other experts to discuss "harmful data broker practices" which provided further impetus for regulation.[18] Here are some highlights illustrating the flurry of recent activity surrounding data brokers:

A. State Data Broker Registry Laws

Over the last few years, four states have enacted data broker registry laws (California, Vermont, Texas, and Oregon),[19] with Texas and Oregon doing so just this year. All of these laws require registration with the state, submission of information, and payment of a registration fee, subject to penalties. Beyond that, the laws vary, for example, in how they define "data broker," what information must be submitted to the state, and whether the information must be disclosed to the public. While the requirements in these laws are not enormously onerous, the passage of two news ones just this year (approved by wide margins) is notable. Even more significant, California just amended its data broker registry law (via SB 362) to add a range of strict new requirements.

B. California's SB 362

In brief, SB 362[20] would add to the registration requirements already in place by establishing an "accessible deletion mechanism" where consumers can direct data brokers to delete their information. This request would in turn trigger an ongoing obligation for data brokers to delete any new information received about the consumer every 45 days, to refrain from selling any further information about the consumer unless the consumers opts in, and to direct any service providers or contractors also to delete the information.

Additionally, the law would allow an "authorized agent" to request deletion for the consumer, require independent compliance audits every three years, and mandate regular reports to the public and to California's privacy regulator (the California Consumer Protection Agency). Due to the broad definition of "data broker," the bill would cover a wide array of entities, including members of the advertising industry that sell consumer data and have no consumer relationship.

The effects of this law could be quite sizeable. On the one hand, it gives consumers significant new deletion and opt-out rights that they can exercise easily, in one step. On the other hand, it raises the potential that large numbers of consumers might opt out *en masse*, whether on their own or through "authorized agents" – a prospect that could substantially impact the data broker and advertising industries, as well as the businesses and other clients that rely on them.[21] In addition, because California typically leads the states on privacy issues, it is possible that other states will follow suit, amplifying these effects considerably.

Not surprisingly, opposition to the bill among industry members was strong, with a large business coalition setting up a website for the purpose of opposing the bill (but with little success).[22] One silver lining for data brokers is that most of the law's new substantive requirements do not take effect until 2026 or even 2028.

> ***In brief, SB 362 would add to the registration requirements already in place by establishing an "accessible deletion mechanism" where consumers can direct data brokers to delete their information***

C. Congress

Congress, too, has been scrutinizing data brokers. For example, the leading comprehensive federal privacy bill (the bipartisan American Data Privacy and Protection Act or ADPPA) contains strict provisions that (like SB 362) require data brokers to register and comply with a one-stop-shop mechanism allowing consumers to delete data and prevent further collection by all data brokers.[23] Other recent federal bills (e.g. the bipartisan DELETE Act[24]) would impose similar requirements.

In April of this year, the Republican-led House Energy and Commerce Committee, as part of its deliberations on the ADPPA, held a hearing specifically on data brokers, making clear that committee members support strong regulation.[25] The Committee followed up in May with inquiry letters to multiple data brokers, which it announced in a press release stating (not so subtly) "E&C Leaders Continue Bipartisan Investigation into Data Brokers' Potential Exploitation of Americans' Privacy."[26] While the ADPPA is still pending in the House, the Committee's focus on data brokers is notable.

Some members of Congress are particularly concerned about government purchases from data brokers, believing that such purchases may bypass or undermine Fourth Amendment protections against unreasonable search and seizure.[27] Accordingly, over the past two years, several bills have been introduced in Congress[28] (all entitled "The Fourth Amendment is Not for Sale Act") that would require a court order, warrant, or subpoena (depending on the circumstances) for government purchases of consumers' location and web browsing and search history from data brokers. Similarly, earlier this year, some members of the House added an amendment to the National Defense Authority Act bill to restrict such purchases by the Department of Defense.[29]

14 GLBA, https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act.

15 As of this writing, 12 states have enacted comprehensive data privacy laws that apply to data brokers along with other businesses. See US State Privacy Legislation Tracker, International Association of Privacy Professionals ("IAPP State Law Tracker"), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last updated Sept. 15, 2023).

16 FTC Act, https://www.law.cornell.edu/uscode/text/15/chapter-2/subchapter-I.

17 In the late 1990s, the FTC was virtually the only agency in the country addressing privacy issues, often facing opposition or skepticism from Congress. Today, multiple policymakers and enforcers at the federal and state level focus on privacy, with rising bipartisan support, greater public awareness of the issue, and privacy in the headlines every day.

18 See White House Press Release, https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/16/read-out-of-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/?utm_source=link (Aug. 16, 2023).

19 See https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.48.&part=4.&chapter=&article (CA); https://sos.vermont.gov/corporations/other-services/data-brokers/ (VT); https://capitol.texas.gov/tlodocs/88R/billtext/pdf/SB02105F.pdf (TX); https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/HB2052/Enrolled (OR).

20 SB 362, https://legiscan.com/CA/text/SB362/2023.

21 Note that the comprehensive laws that have now been passed in 12 states require many businesses, including data brokers, to provide consumers with deletion rights and the ability to opt out of sales and/or sharing with third parties. However, SB 362's more demanding requirements – including its creation of a centralized deletion and opt-out mechanism, the continuing obligation to delete, and the empowerment of "authorized agents" – are likely to have a more impact on the industry.

22 See *supra* n. 13.

23 See H.R. 8152, https://www.congress.gov/bill/117th-congress/house-bill/8152/text. The bill uses the term "third party collecting entities" in lieu of data brokers.

24 See S. 2121, https://www.congress.gov/bill/118th-congress/senate-bill/2121/text?s=1&r=9&q=%7B%22search%22%3A%5B%22Ossoff%22%5D%7D.

25 House Energy and Commerce Committee Press Release, https://energycommerce.house.gov/events/oversight-and-investigations-subcommittee-hearing-who-is-buying-and-selling-your-data-shining-a-light-on-data-brokers (April 19, 2023).

26 House Energy and Commerce Committee Press Release, https://energycommerce.house.gov/posts/e-and-c-leaders-continue-bipartisan-investigation-into-data-brokers-potential-exploitation-of-americans-privacy (May 10, 2023).

27 Federal laws limit the government's ability to obtain consumer data from phone companies and other providers without a warrant, court order, or subpoena. Further, the Supreme Court has held that the government's acquisition of a person's cell phone records from a wireless carrier (which can reveal a person's precise location over time) is a 4th amendment protected search, requiring a warrant supported by probable cause. *Carpenter v. US*, 585 U.S. – (2018). However, according to press reports, the government routinely gets around these restrictions by purchasing consumer data from data brokers, rather than seeking it directly from the providers. See e.g. Byron Tau, *How Cellphone Data Collected for Advertising Landed at U.S. Government Agencies*, Wall Street Journal, https://www.wsj.com/articles/mobilewalla-says-data-it-gathered-from-consumers-cellphones-ended-up-with-government-11637242202 (Nov. 18, 2021)

28 See S. 1265, https://www.congress.gov/bill/117th-congress/senate-bill/1265/text; HR 4639, https://judiciary.house.gov/committee-activity/markups/hr-1631-hr-4250-and-hr-4639.

29 NDAA Amendment 256, https://www.congress.gov/amendment/118th-congress/house-amendment/256/text?s=a&r=2.

All of these efforts are pending, with passage uncertain, but they show mounting bipartisan efforts to place restrictions on the sale of consumer data by data brokers.[30]

D. Federal Trade Commission

Since Congress enacted the FCRA in 1970, the FTC has actively enforced it. In the late 1990s, the FTC also started to focus on the data practices of non-CRA data brokers, beginning with a report it released on "Individual Reference Services," a term then used for non-CRA data brokers.[31] Since then, the FTC has brought law enforcement actions against these companies (using its authority to police "unfair or deceptive" practices),[32] released a comprehensive report detailing their data practices (discussed above),[33] and proposed data broker legislation to Congress at least twice.[34]

More recently, the FTC has stepped up its scrutiny of data brokers, focusing in particular on the sale of health, location, and other sensitive data, and taking the position that sale of this data without consumer permission is an "unfair" practice under the FTC Act. In a blogpost last year, a senior FTC official warned that the FTC will use the "full scope of its authorities" to stop the "illegal use and sharing" of consumers' location, health, and other sensitive data, including by data brokers.[35] Soon after, the FTC filed a lawsuit against data broker *Kochava*, alleging that its sale of location data obtained from mobile devices harms consumers and is legally "unfair" because the data can reveal sensitive locations consumers visit, such as reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities.[36]

The FTC also has launched a rulemaking process, with the goals of limiting "commercial surveillance" and requiring companies to implement stronger security controls in their businesses.[37] While the FTC's proposal is at a preliminary stage, it is replete with references to data brokers and data sales, suggesting that this could be a focus of any rule the FTC proposes. In addition, on September 21, a top FTC official delivered a hard-hitting speech to the leading data broker trade group, detailing the harms caused by unfettered data sales and promising more enforcement.[38]

Like Congressional efforts, the FTC's actions here are pending but show a growing effort to restrict the practices of data brokers.

> ***In brief, SB 362 would add to the registration requirements already in place by establishing an "accessible deletion mechanism" where consumers can direct data brokers to delete their information***

30 Even the intelligence community (traditionally a major customer of data brokers) has raised concerns about government access to commercial data sources, especially data brokers. In a recently declassified report for the Director of National Intelligence, a senior advisory group discussed the increased availability of consumers' sensitive data, the privacy and civil liberty implications, and the need for more rigorous processes to safeguard and limit government use of this data. See ODNI Senior Advisory Group Report, https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf. (Jan. 27, 2022).

31 FTC Report, Individual Reference Services: A Report to Congress, https://www.ftc.gov/reports/individual-reference-services-report-congress (Dec. 1997).

32 See, e.g. FTC Press Release, Sequoia One LLC, https://www.ftc.gov/news-events/news/press-releases/2015/08/ftc-charges-data-brokers-helping-scammer-take-more-7-million-consumers-accounts (Aug. 12, 2015); FTC Press Release, Choicepoint, Inc., https://www.ftc.gov/news-events/news/press-releases/2009/10/consumer-data-broker-choicepoint-failed-protect-consumers-personal-data-left-key-electronic (Oct. 19, 2009).

33 FTC Data Broker Report, *supra* at n. 4.

34 *Id*. See also FTC Report, Protecting Consumer Privacy in an Era of Rapid Change, https://www.ftc.gov/news-events/news/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy (Mar. 26, 2012).

35 FTC Blogpost, https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal (July 2022).

36 FTC Press Release, Kochava, Inc., https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other (Aug. 29, 2022). The court dismissed the FTC's initial complaint due to the hypothetical nature of the injury alleged, but the FTC filed a new one, which is pending and under seal.

37 FTC Web Page, Commercial Surveillance and Data Security Rulemaking, https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.

38 Sam Levine, Speech at Consumer Data Association Law and Industry Conference, https://www.ftc.gov/system/files/ftc_gov/pdf/cdia-sam-levine-9-21-2023.pdf. (Sept. 21, 2023).

E. Consumer Financial Protection Bureau

Finally, in what could be the most consequential data broker regulation of all, CFPB Director Rohit Chopra announced (in mid-August, on the same day as the White House roundtable) that the CFPB would soon launch a rulemaking to "modernize" the FCRA so that it reflects how today's data brokers "build even more complex profiles about our searches, our clicks, our payments, and our locations" and "impermissibly disclose sensitive contact information" of people who don't want to be contacted, such as domestic violence survivors.[39] Then, on September 21, the agency released an outline describing its proposal, which, if ultimately implemented, could fundamentally alter the way data brokers are regulated in this country.[40]

Among the proposals that the CFPB is considering and seeking comment on are amendments to the FCRA that would bring within its scope:

(1) A data broker's sale of certain types of data (e.g. payment history, income, criminal records) because such data is "typically" used to make the eligibility determinations covered by the FCRA (i.e. decisions about consumers' eligibility for credit, employment, and other specified benefits). In other words, *any* data broker that sells this type of data would need to comply with the FCRA's strictures, including by limiting use of this data to the FCRA's "permissible purposes" and giving consumers the opportunity to dispute the accuracy of the data.

(2) Credit header information (identifying information typically included with a consumer report, such as name, address, SSN, and phone number), a major source of information for data brokers that has long been considered to fall outside the FCRA. In other words, this data, too, would be subject to all of the FCRA's data accuracy and privacy procedures.

(3) Targeted marketing that a CRA performs on behalf of clients, if consumer report data is used. Per the CFPB, CRAs may incorrectly believe that this activity isn't covered by the FCRA if the CRAs don't share the data with their clients.

(4) Household level data, or even data that is aggregated at a broader geographic level. This would be a major change as well.

Such amendments (and there are many others in the CFPB's lengthy proposal) would extend the FCRA's reach to a much broader class of data brokers than are currently covered, and dramatically limit how data brokers of all types collect and sell consumer information. The CFPB is at an early stage in the process, however.

05
WHERE DOES THIS LEAVE US?

If you're a consumer, you now have an increasing number of rights when it comes to data brokers, including those afforded under state data registry laws and California's SB 362. You also may soon gain additional rights through actions by the FTC, the CFPB, Congress, and additional states.

If you're a data broker, you may be mired in uncertainty, as you grapple with new laws coming into effect, and the looming possibility of additional actions from various policymakers and enforcers.

How and to what extent consumers will exercise their new rights is uncertain, since many consumers have become numb to the many privacy notices and choices coming at them.[41] We also don't know the effect that these new laws and proposals could have on the broader function of the economy – i.e. by disrupting data broker operations and the many clients that rely on them. One thing is certain, however: longstanding concerns about data brokers have escalated in a big way, and that trend seems likely to continue for the foreseeable future.

39 CFPB Press Release, Remarks of CFPB Director Rohit Chopra at White House Roundtable, https://www.consumerfinance.gov/about-us/newsroom/remarks-of-cfpb-director-rohit-chopra-at-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/. (Aug. 15, 2023).

40 CFPB Rulemaking Proposal, *supra* at n. 10.

41 Research has shown that frequent, repeated notices to consumers leads to "notice fatigue" and may cause consumers to ignore notices entirely. See, e.g. Lillian Ablon et. al, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, Rand Corp., https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf (2016).

TO SHARE OR NOT TO SHARE: **REGULATING DATA BROKERS**

BY JEANNE MOUTON

& CHRISTIAN RUSCHE

PhD Student, GREDEG, Université Côte d'Azur (France) and German Economic Institute (IW), respectively.

01 INTRODUCTION

Data and access to data play an increasingly important role in the global economy and for innovation. Companies that enable access to data and information derived from data benefit from this development: among those data brokers. This paper aims to feed the discussion on whether the increasing importance of data brokers also implies additional regulation, taking the form of mandatory data sharing. First, the paper defines what a data broker is. The extent of data being sold and likely problems deriving from this business model are discussed. The third section reviews the recent regulation at the level of the European Union ("EU") that affect the data economy. Section four concentrates on mandatory data sharing for data brokers since this directly affects their business model and can limit the challenges data brokers may cause. A conclusion is drawn in the last section.

02
DATA BROKERS

According to the US Federal Trade Commission (FTC, 2012, 68) data brokers "are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud."[2] Data brokers only collect and resell or share information. Most often they do not use these data themselves (OECD, 2013, 11).[3] This is how data brokers can be differentiated from digital platforms, which also collect data from different sources but mainly use these data for improving their core service: the matching between the different user groups (Büchel & Rusche, 2021).[4] A platform can even cover the whole data value chain, as it is the case in the online advertising market (CMA, 2020).[5] Nevertheless, a digital platform can also act as a data broker if it resells or shares information with customers of the platform.

Since data brokers collect data from different sources, including public records, and resell these data to their customers, consumers do not directly interact with them. Consumers may not even be aware of what kind of data about them is available, collected, and at which price their data can be purchased. The OECD (2013; 2019) gives a vivid example of this nexus.[6] Based on experiments in the United States, China, and India, it shows that consumers count their social security numbers (national identity numbers) as an example for their most valuable data and assign this information a value of 150 to 240 US-Dollars per entry (OECD, 2013, 31).[7] At the same time, the social security number is available at a data broker for around 8 US-Dollars per entry (ibid, 25).

03
VALUE OF THE DATA MARKET AND LIKELY PROBLEMS

Before diving into the problems that might come along with the activity of data brokers, some key estimates for the value of the data market might help reflect on the magnitude of the likely identified problems.

A recent study for the European Commission (2023, 108) estimates the data market monetization, i.e. the value assigned to the data that was traded in the EU.[8] In fact, in 2020 data for around 11.6 billion euros was traded, in 2021 this amount was 14.8 billion euros, while it is estimated to be 18.9 billion euros last year. It is relevant to stress here that the monetization also encompasses sales by other companies, not only data brokers. Furthermore, data brokers may also offer services based on their data and, therefore, generate additional sales. Nevertheless, the estimates give a first indication of the size of the turnover generated with the sale of data in the EU. According to the study, these sales also come from organizations that "recently discovered there is a market for this" (*ibid*, 2023, 113).

The data market as whole is far larger according to the study for the European Commission (2023) because it also includes some sales of hardware, software, services related to data and positive effects induced by the activity of data companies, for example. For 2022, the data market in the EU is estimated to have a value of almost 73 billion euros (*ibid*, 157). The study also gives estimates for other countries (ibid): in the United States, the data market is estimated to have a value of around 289.4 billion Euro in 2022. In China the value is nearly 40 billion, while it is 46 billion Euro in Japan. Compared to 2021, the value in the EU has increased by 12.6 percent in 2022. The growth in the U.S. (+19.4 percent), China (+24.1 percent) and Japan (+16.3 percent), however, was larger.

To sum up, data monetization and the data market as a whole experience dynamic growth. Data brokers benefit from this process, although digital platforms might profit even more because of the opportunities data offers for their core business model and for entering new markets. In what follows, we identify several key concerns that call for regulating data brokers.

The example of social security numbers shows that the increasing importance of data comes with challenges. The significant difference between the value consumers put on their (personal) data and the price that these data can be bought at from a data broker shows that most of the consumers are neither aware of the category of data available nor their market price. Remaining with this example, the large gap between the valuations can be explained by the fact that the data directly relates to the life of consumers and hence is more valuable to them, while it is only a single information to a company that is using it for offering or improving a service, for example validating an identity. The fact that data are available from data brokers at a low price, not matching the value declared by consumers, raises the question of whether there is sufficient transparency and, ultimately, whether consent to data sharing was given by the consumers.

Furthermore, data are non-rival in consumption, they can be copied and shared at virtually no cost (Rusche & Scheufen, 2018).[9] Once data is publicly available, it is hard to make it private again: once personal data is shared, for example in exchange for a service, the shared data may also be used in the future for other purposes of which the consumer is unaware. And even if the purposes are mentioned in the data privacy statement and the consumers are asked for their consent for data sharing, the consumers' awareness of their data being shared cannot be taken for granted. In a representative study of the Institut für Demoskopie Allensbach (2019, 5) for the German magazine Focus, 77 percent of the participants stated that it is useless to read the terms because you have to give consent any way to be allowed to use the respective service.[10] Furthermore, 73 percent of the participants stated that it is too tedious for them to read the clauses. The finding of the study is aligned with what was identified to be a "crisis of consent", one aspect of which being the overabundance of information (Schermer, Custers & van der Hof, 2014).[11]

> ***The example of social security numbers shows that the increasing importance of data comes with challenges***

Another problem was addressed by Dixon & Gellman (2013). The authors emphasize that public institutions use data brokers to circumvent privacy regulations.[12] Their analysis focuses on the U.S., however, this problem could occur anywhere else in the world. Instead of building databases in line with privacy regulations and high data protection standards to offer a service, public bodies outsource this service to a data broker or another private company, where the standards might be lower.

Furthermore, data brokers are not limited to a single country. For example, Acxiom, one of the biggest data brokers worldwide, is supposed to have information about 2.5 billion people (Lobe, 2021).[13] This results in the following problem: data brokers can, due to their activity in different jurisdictions, circumvent stricter regulations in certain countries, or circumvent them if they rely on suppliers of data that circumvent (stricter) restrictions. Also, specific software might be used to this end. In a recent paper it is stated that "Data brokers are indeed incentivized to develop software-driven strategies to circumvent any privacy law" (Reviglio, 2022).[14]

Finally, data brokers might influence competition in affected markets (Delbono et al., 2021).[15] This is done, for example, if data is not shared with all competitors in a market, or unjustifiably different conditions are applied to the relevant players.

2 FTC – Federal Trade Commission, 2012, Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for businesses and policymakers, FTC Report March 2012.

3 OECD, 2013, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, Nr. 220, https://doi.org/10.1787/5k486qtxldmq-en [14.4.2023].

4 Büchel, Jan & Rusche, Christian, 2021, On Gatekeepers and Structural Competition Problems, in: Intereconomics, Vol. 56, No. 4, pp. 205-210.

5 CMA - The Competition and Markets Authority, 2020, Online platforms and digital advertising, Market study final report 1 July 2020, London.

6 See *supra* note 3, and OECD, 2019, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, https://doi.org/10.1787/276aaca8-en [17.4.2023].

7 See *supra*, note 3.

8 European Commission, 2023, European DATA Market Study 2021 2023, D2.4 Second Report on Facts and Figures, Luxembourg.

9 Rusche, Christian & Scheufen, Marc, 2018, On (Intellectual) Property and other Legal Frameworks in the Digital Economy, An Economic Analysis of the Law, IW-Report, No. 48, Cologne.

10 Translation from German by the author. See Instituts für Demoskopie Allensbach, 2019, w/o title, Umfrage im Auftrag des Focus, https://d1epvft2eg9h7o.cloudfront.net/filer_public/d5/02/d5026d49-6fb4-4bc8-a188-0b68c3a23159/focus_allensbach.pdf [18.4.2023].

11 Schermer, Bart W., Bart Custers & Simone Van der Hof, 2014, The crisis of consent: How stronger legal protection may lead to weaker consent in data protection, in Ethics and Information Technology 16.

12 Dixon, Pam & Gellman, Robert, 2013, Data Brokers and the Federal Government: A New Front in the Battle for Privacy Opens, Third report in a series on Data Brokers, World Privacy Forum Report.

13 Lobe, Adrian, 2021, Ein milliardenschwerer, undurchsichtiger Markt, https://www.deutschlandfunkkultur.de/entfesselter-datenkapitalismus-ein-milliardenschwerer-100.html [18.4.2023].

14 Reviglio, Urbano, 2022, The untamed and discreet role of Data Brokers in surveillance capitalism: a transnational and interdisciplinary overview, in: Internet Policy Review, Vol. 11, No. 3, https://doi.org/10.14763/2022.3.1670 [18.4.2023].

15 Delbono, Flavio; Reggiani, Carlo & Sandrini, Luca, 2021, Strategic data sales to competing firms, Joint Research Centre (JRC) of the European Commission, JRC Digital Economy Working Paper 2021-05, Seville.

04

RECENT REGULATIONS IN THE EU

On the one hand, data become an increasingly important input in the economy and using it is crucial for the competitiveness of the (European) economy. Hence, more data must be made available to as many companies as possible (Büchel & Rusche, 2019).[16] On the other hand, consumers' personal data and the IP (Intellectual Property)-related data of companies must be protected in order to maintain the trust of the consumers and the investment of the companies. Accordingly, there is a trade-off between data protection and data sharing.

Lundqvist (2023) identifies three forms of incentive systems to shape regulation, with the aim to create or collect, information and knowledge that are discussed in academia: first, a system where the creator is being rewarded or granted funds, as a prize, second, a liability system and third a property system. As we are reviewing the recent regulation efforts of the EU of which data brokers are subject, we will see that the regulatory solutions do not consistently rely on only one form of incentive.[17] Rather, Lundqvist analyses the Article 6 of the Digital Markets Act as a liability solution, compared to the PSI Directive where purchase data agreements are contracted between public sector bodies and data brokers at a marginal cost or market value.

The **General Data Protection Regulation** (**GDPR**; Regulation (EU) 2016/679) published 2016, defines personal data and its protection. To this end, the GDPR introduces the guideline that data processing of personal data must be lawful, fair, and done in a transparent manner. Hence, consumers must be informed and must give consent to the use of their personal data. Data brokers are directly affected by the GDPR because of the consent management and the limitations on exchanging personal data. As shown in Section 2, however, there are strong hints that the limitations introduced by the GDPR can be circumvented by data brokers.

The **Data Governance Act** (Regulation (EU) 2022/868) which was published in the Official Journal of the European Union in 2022 aims at fostering data exchange and the uptake of digital services by introducing standards for data intermediation services. Furthermore, certain kinds of data held by the public sector should be made available. Making more public data available is also the aim of the **Open Data Directive** (Revised PSI Directive, Directive (EU) 2019/1024) published in the Official Journal in 2019.

Because gatekeepers already have massive amounts of data from various sources, they can combine new data with these data and can generate more value than other companies with less data (Büchel & Rusche, 2021). The **Digital Markets Act** (Regulation (EU) 2022/1925) published in 2022 is a regulation aiming at limiting the challenges on competition by gatekeepers. The DMA targets core platform services of gatekeepers and introduces obligations to regulate the relationship between them and business users. While the DMA does not aim to protect consumers from potential abusive practices from data brokers, the Regulation includes provisions on data access and portability between gatekeepers and their business users.

The latest effort in regulating the data market is the **Data Act** proposed by the European Commission in 2022. In June 2023, the EU Commission, the Council of the European Union and the Parliament reached an agreement on the final text. This act aims at making more data available by introducing data sharing rules. The regulation concentrates on manufacturers of products and related services and the users of these products and services. Furthermore, rules for making data available to public sector bodies and academic institutions are also introduced.

Finally, we expect the Artificial Intelligence Proposal from the EU Commission (2021) to regulate data brokers to some extent. As stated in its suggested preamble, the proposal is consistent with Union policies as "the promotion of AI-driven innovation is closely linked to the Data Governance Act, the Open Data Directive and other initiatives under the EU strategy for data, which will establish trusted mechanisms and services for the re-use, sharing and pooling of data that are essential for the development of data-driven AI models of high quality." Despite the best recent regulation efforts at the EU level, the business model of data brokers is not subject to any specific regulation. Accordingly, Reviglio (2022) concludes that data brokers are "legally under-regulated." The (likely) problems identified and the different regulatory approaches in the EU open a wide field of possible research. This article discusses the consequences of mandatory data sharing.

> ***On the one hand, data become an increasingly important input in the economy and using it is crucial for the competitiveness of the (European) economy***

16 Büchel, Jan & Rusche, Christian, 2021, On Gatekeepers and Structural Competition Problems, in: Intereconomics, Vol. 56, No. 4, pp. 205-210.

17 Lundqvist, Björn, 2023, Regulating Access and Transfer of Data, Cambridge University Press.

05

IS MANDATORY DATA SHARING NEEDED?

Hirshleifer (1971) already analyzed the incentives for investments in revealing information.[18] Hirshleifer distinguishes between foreknowledge, that is information that will be revealed sooner or later by nature herself (e.g. football results of next weekend), and hidden properties of nature, where an investment is necessary to reveal this information (e.g., the connection between greenhouse gases and global warming). Furthermore, Hirshleifer analyzes investment in information if only pure exchange is possible and if effects in production can be caused by new information. He shows that private information, i.e., where only the inventor uses this information, has no social value. Furthermore, in a world of pure exchange there will be overinvestment in information because new information also leads to profits based on reselling information, and speculation with private information.

These negative effects can be offset by positive effects based on improvements in production which result from the use of new information, if not only pure exchange is considered. Accordingly, collecting information about consumers may be of no social value if this information is only available to a limited number of players because this can then be classified as private information. Furthermore, if this information about consumers does not result in changes in production, the collection of data has no social value, especially if the information is sooner or later revealed by consumers themselves, for example, by purchases in an online shop without having seen advertisements for this shop. As a consequence of the above model, policy-makers have the choice between preventing the collection of data because of overinvestment, or between mandatory data sharing at cheap prices, making all private information of data brokers public.

Delbono et al. (2021) come to a similar conclusion in their analysis of strategic data sales.[19] They find that sharing data of data brokers that can be used for personalized pricing by the receiving firms with all interested firms yields the same welfare as no sharing of data (*ibid*, 16). However, they find that consumers prefer mandatory data sharing because of the fierce competition that this causes. Firms prefer not making data available at all. Data brokers, however, prefer selling data only to some firms, to yield higher prices for access to their data. Firms are willing to pay higher prices because of the exclusive right to monetize this information.

Regarding the incentives of data brokers for investing into collecting data, a mandatory data sharing might be preferred compared to prohibiting the whole business model. Because if collecting or sharing data is not allowed, there is no economic value in doing so. Furthermore, limiting the value that a data broker can create using his data by a mandatory data sharing at a low price also reduces the incentives to invest in collecting data in the first place. This is because the data broker can only generate fewer profits with the data. Mandatory data sharing, additionally, would prevent distortions to competition based on strategic data sales and opens the opportunity of using data to all competitors.

The result of Delbono et al. (2021) that consumers prefer mandatory data sharing does not necessarily hold when privacy concerns of the consumers are considered. In fact, making personal data of consumers available to all competing firms in a market might not be the first choice of consumers, even if this results in lower prices for the goods the consumers want. However, data that allow for personalized pricing are generally personal data.

06

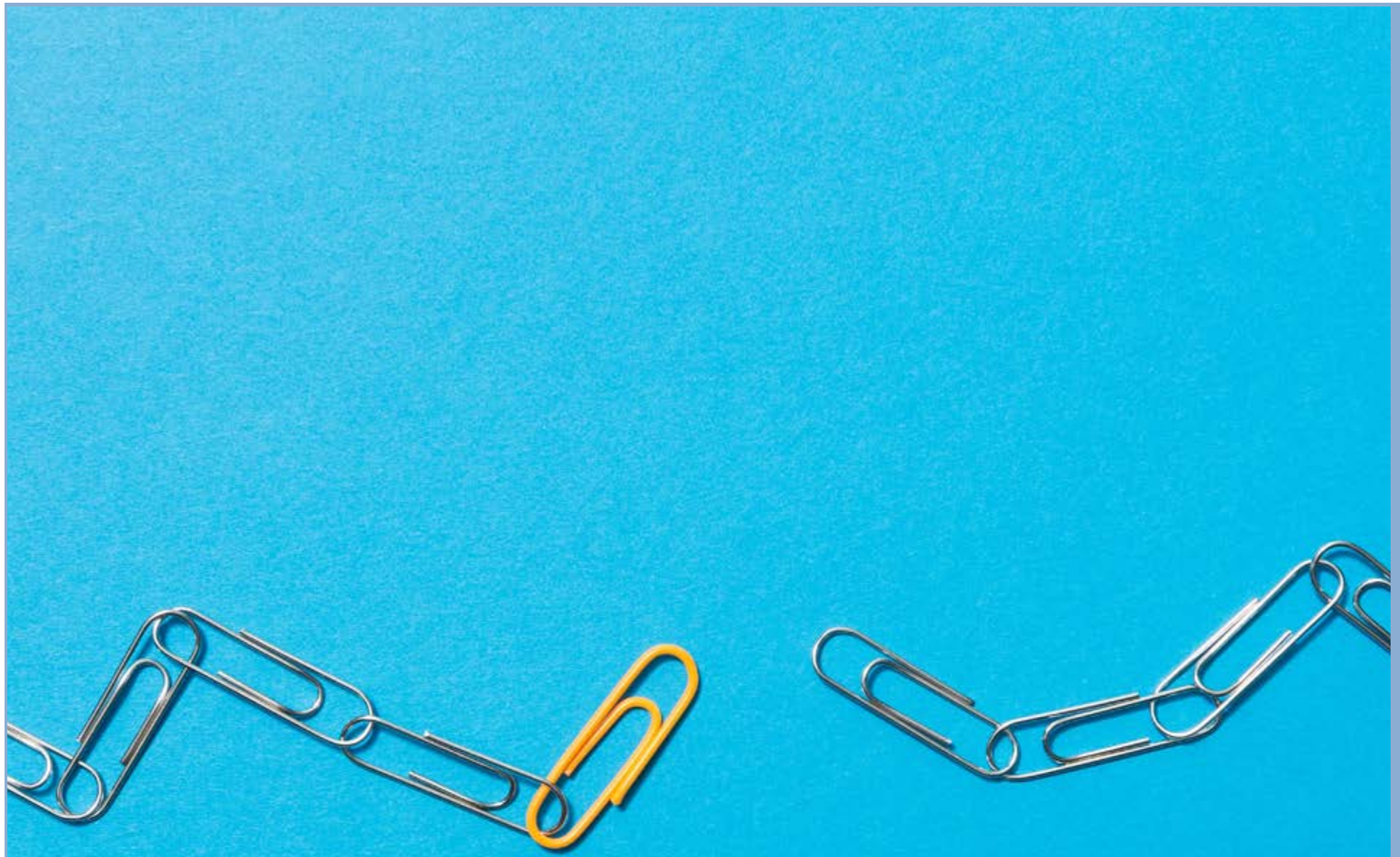
CONCLUSION

To conclude, this paper reviewed the challenges raised by data brokers, the recent regulations efforts at the EU level, and discussed the findings from the literature on whether there is a need for mandatory data sharing.

Balancing the legal challenges and risks with the recent regulations, one might fear an under-regulation of data brokers, since, if they happened to be in scope of several regulations, none is specifically dedicated to their business model. Two extreme solutions have been discussed to regulate data brokers. The first being mandatory data sharing. However, it must be weighed against the second solution: prohibiting the business model. These options represent the above-mentioned trade-off between data protection and data sharing. Mandatory data sharing reduces the incentives of data brokers for collecting data, and likely of consumers for supplying data. However, at least some data is available while a prohibition destroys the whole market. Both options have consequences for the competitiveness of the European economy. Mandatory sharing of data is only one recent research topic when it comes to the business activity of data brokers, among others, the question of an ethical use of digital technologies and data remains open. ■

18 Hirshleifer, Jack, 1971, The Private and Social Value of Information and the Reward to Inventive Activity, in: The American Economic Review, Vol. 61, No. 4, pp. 561-574.

19 Delbono, Flavio / Reggiani, Carlo / Sandrini, Luca, 2021, Strategic data sales to competing firms, Joint Research Centre (JRC) of the European Commission, JRC Digital Economy Working Paper 2021-05, Seville.



DATA BROKERS: INTERMEDIARIES FOR MORE EFFICIENT DATA MARKETS?

BY ANDREAS SCHAUER

& DANIEL SCHNURR

Respectively, Chair of Machine Learning and Uncertainty Quantification, University of Regensburg, andreas.schauer@ur.de and Chair of Machine Learning and Uncertainty Quantification, University of Regensburg, daniel.schnurr@ur.de.

01 INTRODUCTION

By now, data has become an important economic resource for firms and organizations to create manifold business value across diverse use cases and application domains.[2] In consequence, data has turned into an economic good itself that can be shared and traded between organizations and individuals. According to the DATA Market Study 2021-2023, the European data market is currently growing at an annual rate of 12.6 per-

2 Victoria Fast, Daniel Schnurr & Michael Wohlfarth, *Regulation of data-driven market power in the digital economy: Business value creation and competitive advantages from big data*, Journal of Information Technology 38(2), 202-229 (2023).

cent and has reached €72.9 billion in the European Union in 2022.[3] About one quarter of this market value can be attributed to the monetization of data. However, data exhibits several peculiar characteristics as an economic good, which may impede the emergence and well-functioning of data markets and therefore present overarching policy challenges with regard to *data fragmentation* and *data concentration.*[4]

Data brokers play a pivotal role in addressing both these challenges by acting as intermediaries that facilitate data sharing between organizations and also individuals. By collecting, aggregating, enriching, and exchanging both personal and non-personal data, data brokers are envisioned to improve the access to data for a broader range of organizations.[5] In consequence, even firms that do not (yet) have direct access to data sources could benefit from data-driven business models, data-driven quality improvements, and data-driven innovations.[6] In this vein, data brokers could alleviate concerns about data concentration. This applies in particular to user data that is generated as a by-product during consumers' usage of a digital service and therefore entails data-driven network effects. At the same time, data brokers can mitigate data fragmentation by establishing specialized institutions, trading mechanisms, and economic incentives for data sharing. This can generate social benefits and provide new opportunities for innovation through the sharing, aggregation, and combination of otherwise isolated and fragmented complementary data sets. Finally, personal data brokers are envisioned to offer immediate benefits to individuals and data subjects so that they can reap some of the business value associated with the sharing and processing of their data.

However, there are also widespread concerns about the business practices of current data brokers and the general transparency of the market for data.[7] This applies especially to data brokers that collect, process, and share personal data, often without the knowledge and explicit consent of the data subjects. Individuals often face difficulties in effectively exercising their rights to privacy and informational self-determination due to the inherent information asymmetries that they face vis-à-vis data brokers. This can yield significant privacy risks and may undermine individuals' trust in the data economy in general. Even if individual data sets are anonymized or pseudonymized, combining granular data can inadvertently reveal sensitive information or personal identities.[8] In consequence, this presents novel challenges in ensuring privacy for the sharing of granular behavioral data. In the context of non-personal data, similar concerns about data security and confidentiality can arise if data sets reveal commercially sensitive data, such as trade secrets.

In this article, we review and summarize key strands of the academic literature on data brokers and highlight the challenges for data markets and data intermediaries that arise from the special characteristics of data as an economic good. We then highlight recent findings on the economic impact of data brokers in digital markets and scrutinize the idea of personal data brokers and their promise to empower individuals and compensate them for sharing their personal data. Finally, we discuss recent policy initiatives in the European Union, most notably the Data Governance Act and the Data Act, with respect to their implications for data brokers and the policy goal to facilitate the emergence of efficient data markets.

02 THE ROLE AND IMPACT OF DATA BROKERS IN DIGITAL MARKETS

In general, data brokers can be distinguished based on the type of data they focus on. *Business-to-business ("B2B") data brokers* primarily facilitate the exchange of information between firms and organizations, for example by operating industrial data platforms.[9] In contrast, *personal data brokers* focus on data related to individual consumers, often including personal information. While consumers may have the opportunity to voluntarily share their own personal data with these intermediaries, personal data brokers commonly rely on two main sources: acquiring data from private enterprises and government agencies as well as actively collecting government-generated public data, such as property records and census data.[10] Therefore, these data brokers frequently collect, combine, analyze, and monetize individuals' data without the explicit knowledge of the data subjects. Although such data brokerage can nonetheless yield benefits for consumers (for example, by preventing fraudulent activities, enhancing product offerings, or enabling more informative personalized advertisements), it is also associated with inherent risks, particularly concerning consumer privacy.[11]

> ***"In general, data brokers can be distinguished based on the type of data they focus on***

A. The Special Characteristics of Data as an Economic Good and Associated Challenges for Data Markets

As data serves as a valuable input for diverse applications and digital services, data has become an economic good in itself that can be priced and traded between organizations. However, data exhibits several special characteristics that can present barriers to the emergence of efficient data markets.[12]

1. *Non-rivalry of data:*[13] Data can be used by multiple parties simultaneously for different purposes without ever being depleted or diminishing its original quality and functionality. From a welfare perspective, non-rivalry implies that data should be shared and used widely among firms and organizations to maximize social benefits.[14] However, non-rivalry may also discourage firms from sharing and selling data, when they fear that sharing the data with other firms could strengthen potential competitors and increase the risk of creative destruction. Moreover, non-rivalry may limit the exclusive use of data and thus limit firms' ability to profitably sell their data (see Section II.B).
2. *Data quality:* Data is a heterogeneous product and subject to quality differentiation,[15] which can be measured along multiple dimensions, such as accuracy, completeness, timeliness, or consistency.[16] Moreover, the information quality, which denotes the "fitness for use" of a particular data set and determines the ultimate business value of the data in a specific use case, is highly context-dependent and subjective. Therefore, the same set of data can be of very different value to different firms and organizations, which complicates the commodification of data and the emergence of data markets.
3. *Data as an experience good and the Arrow information paradox:* The pricing and trading of data is further complicated by data being an experience good, meaning its true quality and value can only be determined by an organization after it has acquired or used the data. This leads to the famous Arrow information paradox[17], according to which a buyer must gain detailed knowledge about the information in a data set to assess its value. Howev-

3 European Commission, European DATA Market Study 2021-2023 D2.5 Second Report on Policy Conclusions, CNECT/LUX/2020/OP/0027–VIGIE 2020-0655 (2023).

4 Daniel Schnurr, *Global Data Economics: Principles, Strategies and Policies*, in GLOBAL DATA STRATEGIES (Moritz Hennemann ed., 2023).

5 Federal Trade Commission, *Data Brokers – A call for transparency and accountability* (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

6 Michael Katz, *Multisided platforms, big data, and a little antitrust policy,* Review of Industrial Organization 54(4), 695-716 (2019).

7 See, e.g. FTC, *supra* note 5.

8 Yves-Alexandre De Montjoye, Laura Radaelli, Vivek Kumar Singh & Alex "Sandy" Pentland, *Unique in the shopping mall: On the reidentifiability of credit card metadata*, Science, 347(6221), 536-539 (2015).

9 Bertin Martens, Alexandre de Streel, Inge Graef, Thomas Tombal & Néstor Duch-Brown, *Business-to-Business Data Sharing: An Economic and Legal Analysis,* EU Science Hub (2020); For an overview of business data sharing, see also Antragama Ewa Abbas, Wirawan Agahari, Montijn van de Ven, Anneke Zuiderwijk & Mark de Reuver, *Business Data Sharing through Data Marketplaces: A Systematic Literature Review*, Journal of Theoretical and Applied Electronic Commerce Research 16(7), 3321-39 (2021).

10 Matthew Crain, The limits of transparency: Data brokers and commodification, *New Media and Society* 20(1), 88-104 (2018).

11 FTC, *supra* note 5.

12 Bertin Martens, *An economic perspective on data and platform market power* (JRC Digital Economy Working Paper 2020-09); Schnurr, *supra* note 4.

13 Jones Charles I. & Christopher Tonetti, *Nonrivalry and the Economics of Data*, American Economic Review 110(9), 2819-58 (2020); Shota Ichihashi, *Competing data intermediaries,* The RAND Journal of Economics 52(3), 515-537 (2021).

14 *Id*.

15 Martens, *supra* note 12.

16 Wenfei Fan & Floris Geerts, *Foundations of Data Quality Management*. Synthesis Lectures on Data Management 4(5), 1-217 (2012).

17 Kenneth Joseph Arrow, *Economic welfare and the allocation of resources for invention*, in *THE RATE AND DIRECTION OF INVENTIVE ACTIVITY: ECONOMIC AND SOCIAL FACTORS* (J. Kenneth ed. 1962).

er, after having established this knowledge, there is no more incentive for the buyer to acquire the data. In consequence, this can lead to sustained information asymmetries in data markets, which can present further barriers to trade and efficient market outcomes.

4. *Data-driven network effects:* When data is created as a by-product of usage, this can give rise to data-driven network effects. For example, the more data a firm can use to improve the quality of its service, the more users will be attracted by the service, which in turn generates more data.[18] In consequence, data-driven network effects can propel positive feedback loops and promote market concentration, as data-rich firms take over an increasing share of a market, which can further hamper incentives to share data.
5. *Economies of scale and scope:* Economies of scale and scope in data collection and data use may further promote data concentration.[19] In addition, there are often scale and scope advantages from complementary inputs for data processing such as the necessary technical infrastructure, algorithms, and skilled employees. These market characteristics can create additional barriers to the free flow of data.

To overcome these challenges, B2B data brokers may develop and establish economic institutions to facilitate the sharing and trading of non-personal data. Recent analytical and empirical studies explore such market mechanisms and investigate the effects of control and transparency on firms' incentives to share data and the well-functioning of data markets. Rasouli et al. propose market mechanisms and optimal pricing schemes for sharing data against money as well as sharing data against data.[20] These mechanisms leverage firms' ability to artificially alter the quality of the shared data to achieve socially optimal outcomes. In an experimental study on B2B data-sharing platforms, Krämer et al. demonstrate that giving firms on such platforms control over which other firms can access their data promotes data sharing.[21] The same holds for increasing transparency about other firms' decisions to share data and the resulting data transactions on the platform. This is because increased control and transparency allow firms to punish and deter other firms from free-riding, hence creating an incentive for participating in data sharing.

Insight 1: *Data exhibits special characteristics as an economic good that can present barriers to the emergence of efficient data markets. To overcome these challenges, B2B data brokers may establish targeted economic institutions and design data marketplaces to facilitate data sharing.*

> ***To overcome these challenges, B2B data brokers may develop and establish economic institutions to facilitate the sharing and trading of non-personal data. Recent analytical and empirical studies explore such mar***

B. Economic Impact of Data Brokers as Intermediaries

Several recent studies investigate the role of data brokers as information intermediaries in digital markets. To this end, various game-theoretic analyses examine the optimal strategies and the economic impact of monopolistic data brokers that sell consumer information to retailers in downstream markets, where the data is used for better demand forecasts,[22] price discrimination,[23] or targeted advertising.[24] Koski presents empirical evidence that the termination of a data broker's business led to price increases in the Finnish food retail sector, suggesting that information exchange through data brokers can have a pro-competitive effect on downstream markets.[25] In contrast, Zhang et al. show analytically that data brokers can promote data concentration, when larger firms exploit smaller firms' willingness to sell more data through a data broker.[26] Nonetheless, consumers may benefit from data brokerage in this case as firms have access to more data to improve the quality of their service.

Montes et al. demonstrate that it is optimal for monopolistic data brokers to rely on exclusive contracts when selling a single data set of consumer information. In contrast, Belleflamme et al. find that a data broker can increase its profit by serving more than one downstream firm, but only if it supplies data of different qualities to different retailers.[27] Similarly, Bounie et al. show that a data broker can profitably split its data set and sell mutually exclusive partitions to different downstream firms.[28] In both cases, the distinct input data sets allow retailers to differentiate themselves, which softens competition with personalized prices in the downstream market and thus increases retailers' willingness to pay for the data.

For competing data brokers, Ichihashi highlights that the non-rivalry of data reduces intermediaries' incentives to offer consumers a high reward for their data, as consumers may sell the same data to other intermediaries, thus lowering the commercial value of the data.[29] Thus, non-rivalry softens competition and lowers the reward for data creators. On a related note, Ichihashi as well as Gu et al. demonstrate that competing data brokers have an incentive to collect and sell exclusive data sets to evade the negative impact of intense competition or may even prefer to merge their individual data sets and sell a joint data set.[30] Therefore, the peculiar characteristics of data as an economic good have important implications for data brokers' incentives to differentiate their data sources and the competition intensity in data markets.

Insight 2: *Data brokers can promote competition in downstream markets that make use of the data. However, it is often optimal for data brokers to offer data exclusively or to differentiate its quality when selling to downstream firms. There is also the risk that data brokerage may reinforce existing data concentration. The non-rivalry of data softens competition between data brokers and may lead to lower rewards for data creators.*

> ***Montes et al. demonstrate that it is optimal for monopolistic data brokers to rely on exclusive contracts when selling a single data set of consumer information***

C. Privacy Risks and Consumer Empowerment

A further stream of empirical literature investigates the practices of personal data brokers in today's data economy and highlights the potential threats to data subjects that can emerge from these practices.[31] In particular, data brokers' lack of transparency in collecting and managing individuals' information often undermines consumers' data control, posing significant privacy risks.[32] As highlighted by the FTC, the indefinite retention periods practiced by data brokers present additional privacy and security risks.[33] Neumann et al. find that user profiles offered for sale by data brokers are frequently of low data quality, limiting their economic value and raising further privacy

18 Martens, *supra* note 12.

19 Néstor Duch-Brown, Bertin Martens & Frank Müller-Lange, The economics of ownership, access and trade in digital data (JRC Digital Economy Working Paper, 2017).

20 Mohammad Rasouli & Michael I. Jordan, *Data sharing markets* (Working Paper, 2021).

21 Jan Krämer, Nadine Stüdlein & Oliver Zierke, *Data as a public good: experimental insights on the optimal design of B2B data sharing platforms* (Working Paper, 2021).

22 Kostas Bimpikis, Davide Crapis & Alireza Tahbaz-Salehi, *Information sale and competition,* Management Science 65(6), 2646-2664 (2019).

23 Rodrigo Montes, Wilfried Sand-Zantman & Tommaso Valletti, *The value of personal information in online markets with endogenous privacy,* Management Science 65(3), 1342-1362 (2019); Paul Belleflamme, Wing Man Wynne Lam & Wouter Vergote, *Price discrimination and dispersion under asymmetric profiling of consumers* (Working Paper, 2017).

24 Dirk Bergemann & Alessandro Bonatti, *Selling cookies,* American Economic Journal: Microeconomics 7(3), 259-294 (2015).

25 Heli Koski, *How Do Competition Policy and Data Brokers Shape Product Market Competition?* (ETLA Working Paper No. 61. ETLA, 2018).

26 Xin Zhang, Wei Thoo Yue, Yugang Yu & Xiong Zhang, *How to monetize data: An economic analysis of data monetization strategies under competition*, Decision Support Systems 173, 114012 (2023); Javier Parra-Arnau, *Optimized, direct sale of privacy in personal data marketplaces,* Information Sciences 424, 354-384 (2018).

27 Belleflamme et al., *supra* note 23.

28 David Bounie, Antoine Dubus & Patrick Waelbroeck, *Selling strategic information in digital competitive markets,* The RAND Journal of Economics 52(2), 283-313 (2021).

29 Shota Ichihashi, *supra* note 13.

30 Yiquan Gu, Leonardo Madio & Carlo Reggiani, *Data brokers co-opetition,* Oxford Economic Papers 74(3), 820-839 (2022).

31 Sarah Spiekermann, Alessandro Acquisti, Rainer Böhme & Kai-Lung Hui, *The challenges of personal data markets and privacy,* Electronic Markets 25, 161-167 (2015).

32 Alexander Tsesis, *The right to erasure: Privacy, data brokers, and the indefinite retention of data,* Wake Forest L. Rev. 49, 433 (2014).

33 FTC, *supra* note 5.

concerns.[34] In particular, the study evaluates data brokers' ability to infer demographic information and interests, revealing frequent inaccuracies, especially in gender prediction. In a survey on 75 data brokers, Aımeur et al. show that personal data brokers offering personal information for free on their websites can reveal sensitive personal information and pose significant risks to data subjects, as data from different sources can easily be linked across different data brokers by malicious actors using data matching techniques.[35]

Building on these findings, recent studies analyze approaches to make brokerage of personal data more privacy-preserving and to involve data subjects more directly in the sharing of their data. From a technical perspective, privacy-preserving technologies, such as the encryption and signing of data to ensure identity preservation, data integrity, and data confidentiality,[36] have been proposed to mitigate the risks of data sharing and to increase data subjects' trust in data markets.[37] Moreover, blockchain-based infrastructures have been suggested to facilitate user-controlled data sharing, although their effect on privacy is controversial.[38]

From a policy perspective, the literature documents recent efforts by policymakers to give consumers more power and control over the sharing and monetization of their personal data.[39] In its European Strategy for Data,[40] the European Commission emphasizes that Personal Information Management Services ("PIMS")[41] could serve as a key building block for a user-centric data economy. In particular, PIMS allow data subjects to store, manage, and share data under their own control and could thus serve as a technical infrastructure to support business models that allow consumers to sell their data in return for a monetary reward.[42] To this end, it is important that data subjects can retrieve and aggregate their personal data from digital services that they regularly use. In the European Union, this is supported and facilitated by the right to data portability under the General Data Protection Regulation ("GDPR"). Technically, data transactions through personal data brokers could further be supported by smart contracts[43] and blockchain-based infrastructures.[44]

> ***Building on these findings, recent studies analyze approaches to make brokerage of personal data more privacy-preserving and to involve data subjects more directly in the sharing of their data***

34 Nico Neumann & Catherine E. Tucker, *Frontiers: How effective is third-party consumer profiling? Evidence from field studies*, Marketing Science 38(6), 918-926 (2019).

35 Esma Aımeur, Gilles Brassard & Muxue Guo, *How Data Brokers Endanger Privacy,* Transactions on Data Privacy 15, 41-85 (2022).

36 Chaoyue Niu, Zhenzhe Zheng, Fan Wu, Xiaofeng Gao & Guihai Chen, *Achieving data truthfulness and privacy preservation in data markets,* IEEE Transactions on Knowledge and Data Engineering 31(1), 105-119, (2018).

37 For an overview of privacy-enhancing technologies for data brokers: Gonzalo Munilla Garrido, Johannes Sedlmeir, Ömer Uludağ, Ilias Soto Alaoui, Andre Luckow, Florian Matthes, *Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: A systematic literature review*, Journal of Network and Computer Applications 207, 103465 (2022).

38 Daniel Amo, David Fonseca, Marc Alier, Francisco José García-Peñalvo & María José Casañ, *Personal data broker instead of blockchain for students' data privacy assurance*, WorldCIST'19 2019. Advances in Intelligent Systems and Computing 932, 371-380 (2019).

39 Chih-Liang Yeh, *Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers,* Telecommunications Policy 42(4), 282-292 (2018).

40 European Commission, *A European strategy for data*, COM(2020) 66 final (2020).

41 Serge Abiteboul, Benjamin André & Daniel Kaplan, *Managing Your Digital Life*, Communications of the ACM 58, 32–35 (2015).

42 Matias Travizano, Martin Minnoni, Gustavo Ajzenman, Carlos Sarraute & Nicolas Della Penna, *Wibson: A decentralized marketplace empowering individuals to safely monetize their personal data,* (White Paper, 2018); Xin Zhang, Wei Thoo Yue, Yugang Yu & Xiong Zhang, *supra* note 26.

43 Sachit Mahajan, *Data Marketplaces: A Solution for Personal Data Control and Ownership?,* Sustainability 14(24), 16884 (2022).

44 Guy Zyskind & Oz Nathan, *Decentralizing privacy: Using blockchain to protect personal data*, 2015 IEEE Security and Privacy Workshops (2015).

In practice, there have been numerous examples of startup firms like *Datacy*[45] and *Datum*[46] promising to establish such personal data brokers to the benefit of consumers. However, so far, the success of these businesses has been very limited, with several personal data brokers having stopped their operations without paying significant rewards to consumers.[47] Haberer et al. show that this may be explained by the strategic interactions and the economic effects that arise in the context of personal data brokers.[48] In particular, providers of digital services, where the data is originally created as a by-product of consumers' usage, may invest less into the quality of their services when a personal data broker competes for the same data-driven revenues. This is especially the case when monetary rewards do not only remunerate consumers for their existing data, but also offer incentives for consumers to create additional data through more usage. Only if the provider of the digital service can appropriate some of the consumers' rewards from the personal data broker through a higher price for its service, the provider will be willing to raise the quality of its service again. In consequence, consumers only benefit from personal data brokers if these brokers are very efficient in generating revenues from data and can therefore increase the industry's overall data revenues. Evidently, current personal data brokers seem not to meet this efficiency threshold and thus can only sustain a marginal existence where they pay only negligible rewards to consumers. This further questions whether personal data brokers can fulfill the expectations of European policymakers to serve as a core building block of a user-centric data economy.

> ***In practice, there have been numerous examples of startup firms like Datacy and Datum promising to establish such personal data brokers to the benefit of consumers***

Insight 3: *Lack of transparency, indefinite data retention, risks of malicious access and data leakage, as well as the disclosure of sensitive information from data combination pose significant privacy risks for data subjects in the context of personal data brokers. In combination with PIMS, personal data brokers can empower consumers and may allow data subjects to directly sell their personal data. However, consumers can also be worse off with personal data brokers if these brokers are not sufficiently efficient in generating data revenues.*

03
RECENT EUROPEAN DATA REGULATIONS AND THEIR IMPACT ON DATA BROKERS

The GDPR has established a general regulatory framework for the brokerage and sharing of personal data in the European Union. To this end, the GDPR has strengthened the rights and control of data subjects, which may limit the business opportunities and practices of data brokers. However, with the right to data portability, the GDPR has also established new rules that can foster the availability and free flow of data. Based on a game-theoretic analysis, Ke and Sudhir conclude that the privacy rights stipulated by the GDPR are likely to reduce the total volume of consumer data available in the market, whereas the overall effect on consumer welfare depends crucially on the competition intensity in a market.[49] In practice, empirical studies show that the right to data portability has so far had a very limited impact in unlocking personal data for effective data sharing, which is commonly attributed to technical challenges and the limited scope of data access.[50]

45 Datacy, *Your data tells a story* (2023), https://datacy.com/consumer.

46 Datum, *Blockchain Data Storage and Monetization* (2023), https://datum.org/.

47 See, e.g., Datacoup, *Datacoup is shutting down operations and will be decommissioning all of our servers* (2019), https://en.wikipedia.org/wiki/Datacoup.

48 Bastian Haberer, Jan Kraemer & Daniel Schnurr, *Do Consumers Benefit from Selling their Data? The Economic Effects of Personal Data Brokers in Digital Markets,* TPRC 46 (2022).

49 Tony Ke & K. Sudhir, *Privacy Rights and data security: GDPR and personal data markets*, Management Science 69(8), 4389-4412 (2023).

50 Emmanuel Syrmoudis, Stefan Mager, Sophie Kuebler-Wachendorff, Paul Pizzinini, Jens Grossklags and Johann Kranz, *Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20*, Proceedings on Privacy Enhancing Technologies 351-372 (2021); Jan Krämer, *Personal data portability in the platform economy: economic implications and policy recommendations,* Journal of Competition Law & Economics 17(2), 263-308 (2021).

In this context, the recently adopted Data Act provides an extended right to data portability to both consumers and business users and extends the scope of data access to non-personal data created during the usage of connected products and related digital services.[51] Under the Data Act, users may not only access data themselves but can also request that data holders transfer the data directly to an authorized third party. This is done with the goal of unlocking new data sources and promoting the free flow of data to mitigate data fragmentation. However, the Data Act also stipulates several restrictions on third parties' data access, such as the need for contractual agreements, compensation based on FRAND (i.e. fair, reasonable and non-discriminatory) terms, or restrictions on the use of the accessed data. These restrictions are intended to safeguard the legitimate interests of data holders but run the risk of undermining the ultimate effectiveness of the Data Act in achieving its goal to increase data availability.[52] In particular, these restrictions make it unlikely that data brokers can make effective use of the data that could in principle become available through the new data access rights in the Data Act.[53] This is exacerbated by further limits on commercial practices, such as the prohibition of exclusive contracting between a user and a third party. Thus, there is the risk that the Data Act will fall short in achieving its intended goals as its rules do not sufficiently account for the role that data brokers and data markets could play in promoting data sharing and the widespread use of data.

In this context, the recently adopted Data Act provides an extended right to data portability to both consumers and business users and extends the scope of data access to non-personal data created during the usage of connected products and related digital services

51 European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)*, COM(2022) 68 final (2022).

52 Jan Krämer, *Improving the Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act,* in DATA ACT: TOWARDS A BALANCED EU DATA REGULATION (Centre on Regulation in Europe CERRE, 2023).

53 id.

As a further key pillar of the European Strategy for Data, the Data Governance Act aims to increase trust in data sharing and overall data availability.[54] The rules, which are applicable since September 2023,[55] directly address data brokers as key actors of the data economy and impose several requirements for data intermediary services. Most notably, the Data Governance Act requires data intermediation services to notify a competent public authority about its operation, stipulates structural unbundling of intermediation services and prohibits the re-use of data for any purpose other than data intermediation, requires prices for data access to be based on FRAND terms, and imposes additional transparency requirements.[56] These requirements for data intermediaries can be expected to have some positive effects on the general transparency of data markets and could help regulators to obtain better information about the identities and practices of data brokers in the market. Furthermore, the legislation establishes a legal basis for regulatory intervention to remedy non-compliance and potential market failures, which could lead to better protection of data subjects. However, the Data Governance Act does not address any of the barriers to data brokerage that stem from the special characteristics of data as an economic good, as identified in this article. Instead, by imposing additional requirements and obligations on data intermediation, the regulation is further diminishing the economic incentives to engage in data brokerage and increases the costs for establishing such businesses. For example, imposing FRAND as a general principle for data access pricing is in stark contradiction to the optimal strategies for data brokers as identified by the economic literature. Overall, the Data Governance Act is therefore more likely to discourage rather than to promote an active data broker industry that could facilitate the free flow of data and increase data availability in the European Union.

As a further key pillar of the European Strategy for Data, the Data Governance Act aims to increase trust in data sharing and overall data availability

54 European Commission, *REGULATION (EU) 2022/868 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act),* L 152/1 (2022).

55 The rules on data intermediation services will become applicable only by September 2025.

56 Heiko Richter, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, GRUR International, 72(5), 458-470 (2023); Moritz Hennemann & Lukas von Ditfurth, *Datenintermediäre und Data Governance Act - Vertrauen durch Regulierung?,* NJW, 1905-1910 (2022).

DATA BROKER REGULATION - COMPETITION v. PRIVACY CONSIDERATIONS: **TRADE-OFFS**

BY LOTHAR DETERMANN

& TEISHA JOHNSON

The authors are partners at Baker McKenzie's Palo Alto and Washington D.C.'s offices. Opinions expressed in this article are solely their own and not their firm's, clients' or others.

01 INTRODUCTION

Data brokers face stiff criticism, lawsuits, actions from regulators, proposed new legislation and regulation, and political headwinds, in the United States as elsewhere.[2] Privacy advocates and journalists claim data brokers are not sufficiently regulated,[3] even though data brokers have been subject to privacy law restrictions in some of the oldest U.S. privacy laws. In the ongoing debate, tradeoffs between competition and privacy are not always holistically appreciated.

2 See, for example, www.cnn.com/2023/08/15/tech/privacy-rules-data-brokers/index.html.

3 See, for example, www.popsci.com/technology/data-brokers-explained/.

02
DATA

In an increasingly interconnected world, data is a valuable asset. No one owns data,[4] yet every business needs information to make intelligent decisions about market focus, product development, pricing, advertising, and all other aspects of running a successful company. Every online action — from liking a social media post to buying a new shirt — generates data. Companies that operate successful online presences collect lots of information that they can use to compete in their core business areas, monetize to target advertisements on their platforms, or sell to other companies or government agencies.[5] Many new market entrants and smaller businesses in particular state that they need to purchase data to compete.

03
BROKERS

Generally, brokers act as intermediaries between buyers and sellers of any item of value, including real estate, commodities, securities, and all kinds of products and services. Brokers focus on meeting demand and help optimize market dynamics, pricing, and quality. They play an important role for commerce and competition in all areas. So do data brokers. "Data brokers may provide information that can be beneficial to services that are offered in the modern economy, including credit reporting, background checks, government services, risk mitigation and fraud detection, banking, insurance, and ancestry research, as well as helping to make determinations about whether to provide these services."[6]

04
PRIVACY CONSIDERATIONS

Data brokers sell various categories of data and not all relates to individual persons. But, much of the information humans care about relates to humans and thus qualifies as "personal information" or "personal data." Under California privacy law, "data broker" means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.[7] Without a direct relationship, data brokers cannot easily inform consumers about their data collection and processing practices. From the consumer's perspective, the brokers operate "behind the scenes," collecting information from numerous sources, including e-commerce websites, social medial platforms, public records, online transactions, surveys, and more. These data collection efforts enable data brokers to amass a wide array of data and information, from basic personal details (*e.g.* names, addresses, phone numbers, email addresses) to intricate personal behavior insights (*e.g.* financial status, family connections, health conditions, details on shopping and online browsing activities, travel habits, and geolocation data) that can create a detailed profile of an individual. The collected data can also be aggregated and compiled into comprehensive datasets to be licensed or sold to various businesses and institutions including, advertisers, marketers, researchers, and financial institutions. The businesses that ultimately buy and use personal information about consumers often do not have relationships with the consumer either and with some of them -- e.g. collection agencies, law enforcement authorities, and telemarketers -- consumers would rather not have relationships at all. Most consumers would prefer that their data is not sold to organizations that do not wish them well or might harass them with cold calls and unwanted text messages. Most consumers also do not see any tangible upside from their data being traded by brokers. Many fear that poor data quality or hostile data usage practices could ultimately harm them. Some feel they should receive a "cut" from the profits generated with their data.[8]

05
COMPETITION CONSIDERATIONS

Without data, companies cannot effectively develop products, stock the right amount of goods in the right place, target advertisements effectively to potentially interested persons, or make informed decisions about important issues such as loans and payment terms. As the significance of data continues to increase, firms without sufficient access to data, such as new market entrants and smaller players, may not be able to effectively compete with larger, already established firms. Data brokers can play an important role in our data-driven economy by providing entities with valuable consumer insights through data selling and sharing.

However, data collection and sale can also create competition concerns if data brokers amass large amounts of unique data resulting in a data broker gaining significant market power. If access to that data set is withheld (either entirely or selectively) or if the cost of obtaining the data is so large that only a limited number of well-established data purchasers can financially purchase the data, this could create barriers to entry both for smaller firms desiring to purchase the data and for smaller data brokers attempting to enter the market as a data broker. Owning large amounts of data—particularly unique data—heightens the competition concern as there is an increased risk of the data owner taking actions to solidify its market position by behaving in anticompetitive ways that could slow innovation, cause prices to rise, reduce quality and choice, and cause other negative effects such as affecting credit decisions and how customers are treated.

Data brokers can also enhance the competitive environment and facilitate positive outcomes for consumers by embracing and facilitating the flow of data. Consumers can directly benefit from data trading where companies offer services or financial incentives to consumers in exchange for collecting information from consumers. Also, consumers can indirectly benefit, namely from effective competition, informed product development, relevant advertisements, and loan risk mitigation throughout the economy. If overly rigid data broker regulation inhibits data selling and sharing, smaller and newer companies may not have access to sufficient data to enter new product markets and compete. Without competition, companies could then solidify their market positions and raise prices, slow down innovation, deteriorate products, withhold credit, and treat consumers poorly.

06
DATA BROKER LAWS AND REGULATIONS

Fair Credit Reporting Act. Data brokers have been subject to sector-specific data privacy laws for more than 50 years in the United States. Congress enacted one of the oldest data privacy laws in the world, the federal Fair Credit Reporting Act ("FCRA"), in 1970 to regulate credit reporting agencies and provide privacy rights for personal data in consumer reports.[9] FCRA was substantially updated by the Fair and Accurate Credit Transactions Act ("FACTA") in 2003.[10] Companies have to comply with FCRA if and to the extent they act as "consumer reporting agencies," "users" or "furnishers." Most companies act at a minimum as "users" of credit reports, namely when they obtain background checks on employees or candidates. A "consumer reporting agency" is any person or entity that compiles or evaluates information on consumers for the purpose of furnishing consumer reports to third parties for a fee.[11] Equifax, Experian, and TransUnion are among the most prominent consumer reporting agencies. Other businesses that collect similar data on consumers may also be subject to the FCRA rules, depending on the purposes for which the data they sell is used.[12] "Users" are employers,

4 Lothar Determann, No One Owns Data, 70 Hastings Law Journal 1 (2019), available at SSRN: https://ssrn.com/abstract=3123957.

5 See, www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data.

6 See, recital (d) of Assembly Bill 1202 that introduced registration requirements for data brokers in California, see https://legiscan.com/CA/text/AB1202/2019.

7 Cal. Civ. Code §1798.99.80(d).

8 https://www.cnbc.com/2019/02/12/california-gov-newsom-calls-for-new-data-dividend-for-consumers.html.

9 15 U.S.C. §§ 1681–1681x. On the history of credit bureaus and regulation, see Rowena Olegario, Credit-Reporting Agencies: Their Historical Roots, Current Status, and Role in Market Development, http://documents.worldbank.org/curated/en/209261468762614853/Credit-reporting-agencies-their-historical-roots-current-status-and-role-in-market-development.

10 See 16 C.F.R. Part 682.

11 15 U.S.C. § 1681a(f).

12 LinkedIn was sued in a class action over alleged FCRA violations, but the suit was dismissed, see Sweet v. LinkedIn Corp., N.D. Cal., No. 5:14-cv-04531-PSG, 2015 WL 1744254 (N.D. Cal. April 4, 2014). Spokeo settled with the FTC on alleged FCRA violations, Stipulation for Entry of Consent Decree and Order for Civil Penalties, Injunction and Other Relief, United States of America v. Spokeo, Inc., No. CV12-05001 (C.D. Cal. June 7, 2012), available at www.ftc.gov/sites/default/files/documents/cases/2012/06/120612spokeoorder.pdf.

lenders, insurers, and other companies that use consumer reports for various purposes.[13] "Furnishers" are companies that report information about transactions with consumers to consumer reporting agencies, such as banks or merchants that report that a debtor is late making payments. A company that furnishes only reports regarding its own transactions does not become a "consumer reporting agency," because such reports are excluded from the definition of "consumer report."[14] Friends, acquaintances and neighbors who answer requests for information from consumer reporting agencies do not qualify as furnishers either.[15]

State Privacy Laws. In 1975, California enacted the California Consumer Credit Reporting Agencies Act ("CCRAA"), with a similar focus as the federal FCRA.[16] The CCRAA regulates consumer credit reporting agencies doing business in California. More recently, states including California, Texas, Vermont, and Oregon enacted laws regulating data brokers more broadly. Vermont was the first state to require data brokers to register with the state government. California soon followed, and just this year Texas and Oregon joined California and Vermont in enacting laws regulating data brokers. The specific requirements and obligations imposed on data brokers vary by state. However, there are common themes in the regulations, including: (1) similarities in the definition of "data broker" and "personal data;" (2) the requirement that data brokers register in the state; and (3) penalties associated for data brokers who fail to register and/or provide the required information to the state. State rules also require that data brokers maintain certain security measures with respect to the data.

A. Overview of State Data Regulation Rules

Vermont, in 2018, became the first state to enact a law implementing registration requirements and regulations with respect to data brokers.[17] Vermont's law established registration, disclosure and data security requirements for data brokers trading in Vermont residents' personal information. Data brokers must register annually and adopt information security programs with appropriate safeguards to protect personal information.[18] The Vermont law defines data brokers to mean a business that "knowingly collects and sells or licenses to third parties brokered personal information of a consumer with whom the business does not have a direct relationship,"[19] and defines brokered personal information as "computerized data elements, if categorized or organized for dissemination to third parties" that include certain items about a Vermont consumer, including name, address, date or place of birth, mother's maiden name, biometric data, social security number (or any government-issued identification number) and any other information that alone or in combination with other licensed/sold information would reasonably allow the consumer's identification with reasonable certainty.[20] The law imposes civil penalties of up to $50/day (not exceeding $10,000 per year) for data brokers that fail to register.[21] As Vermont was the first state to enact data broker laws, it set a precedent which other states have followed.

> ***Vermont, in 2018, became the first state to enact a law implementing registration requirements and regulations with respect to data brokers***

California enacted a data broker law that looked similar (but not identical) to Vermont's data broker law. The California law requires data brokers to register every year on or before January 31 with the California Attorney General, and pay an annual registration fee.[22] In registering with the Attorney General, data brokers are required to provide its name, primary physical, email, and internet website addresses. California's data broker law borrowed many of the broad definitions from the previously adopted California Consumer Privacy Act ("CCPA") enacted in 2018, including "business," "consumer," "personal information" and "sale."[23] Companies that exchange employee or business contact information with affiliates or other business partners for consideration (monetary or other) may qualify as a business that sells personal information under CCPA; if a business does not have a direct relationship with the consumer to whom the data relates, the business may have to register as a data broker.

In September 2023, California amended its data broker law, and passed Senate Bill 362 adding additional obligations on data brokers by introducing a single "accessible deletion mechanism."[24] California consumers will be able to use the mechanism via a website maintained by the California government to request that every data broker that maintains any personal information about the consumer delete such personal information held by the data brokers or associated service providers or contractors.[25] The data brokers will be required to process deletion requests that are made through the CPPA mechanism within 31 days of receiving them, and in 2026, continuously delete the personal information of the requesting consumer and not sell or share new personal information of the consumer. Data brokers will also be required to direct all service providers or contractors associated with the data broker to delete all personal information in their possession related to the requesting consumer. The new law will require data brokers to provide additional information when registering as data brokers, including specifying whether they collect the personal information of minors, consumers' precise geolocation, and consumers' reproductive health care data.

Currently, the new California law is the first and only law giving consumers the ability to request that their data be deleted in a single request. Also, California applies the most rigid restrictions on "selling" and "sharing" of personal information in the United States and probably worldwide, applicable to businesses that have a direct relationship with consumers and who supply data to brokers and other businesses.[26] These restrictions could significantly reduce the amount of California consumer information that data brokers can trade, unless data brokers and businesses can make the case to consumers that consumers benefit from more efficient competition enabled by data trading. California privacy law also requires companies to inform consumers about the value of their personal information to the business in "notices of financial incentives" whose disclosures and terminology is dictated by prescriptive statutory requirements and regulations.[27] It remains to be seen whether these restrictions and transparency requirements will enable and enhance fair competition in data markets or stifle the data broker industry so much that smaller businesses can no longer compete with large data owners, which do not have to sell or share data.

> ***Currently, the new California law is the first and only law giving consumers the ability to request that their data be deleted in a single request***

In June, Texas signed into law a new data broker law (SB 2105) (effective as of September 1, 2023) creating registration, security, and disclosure requirements for data brokers that meet certain annual revenue or processing thresholds regarding personal data (any information that links or is reasonably able to be linked to an individual, including pseudonymous data used in combination with other identifying information).[28] Texas considers a data broker to be any business entity whose principal source of revenue is derived from collecting, processing or transfer-

13 See 15 U.S.C. § 1681m (requirements on users of consumer reports); 15 U.S.C. § 1681s-2 (responsibilities of furnishers of information to consumer reporting agencies).

14 15 U.S.C. § 1681a(d)(2)(A)(i).

15 16 C.F.R. § 660.2(c).

16 Cal. Civ. Code §§ 1785.1-1785.36. The law became effective in California in 1975 and has been subject to several amendments. See, for example, www.leginfo.ca.gov/pub/09-10/bill/sen/sb_0901-0950/sb_909_cfa_20100621_110753_asm_comm.html.

17 9 V.S.A. §§ 2430, 2433, 2446 and 2447

18 See, Guidance on Vermont's Act 171 of 2018 Data Broker Regulation, 2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf (vermont.gov).

19 9 V.S.A. § 2430(4)(A).

20 9 V.S.A. § 2430(1)(A).

21 9 V.S.A. § 2446 (b).

22 Cal. Civ. Code §1798.99.82.

23 See, Determann, California Privacy Law, Practical Guide and Commentary, Chapter 2C (5th Ed. 2023).

24 Cal. SB 362 (2023)

25 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/united-states-senate-bill-362-to-amend-california-data-broker-law.

26 Lothar Determann, California Privacy Law Vectors for Data Disclosures, in: *Data Disclosure: Global Developments and Perspectives*, edited by Moritz Hennemann, Kai von Lewinski, Daniela Wawra and Thomas Widjaja, Berlin, Boston: De Gruyter, 2023, pp. 121-146, https://ssrn.com/abstract=4146903.

27 https://www.connectontech.com/united-states-california-attorney-general-sets-sights-on-consumer-loyalty-programs-for-ccpa-enforcement/.

28 See Texas S.B. No. 2105 (2023).

ring personal data that the entity did not collect directly from the individual linked to the data.[29] Data brokers operating in Texas are required to (1) pay a fee and register with the state, (2) post language on its website or app identifying itself as a data broker, and (3) implement and maintain a comprehensive written information security program.[30] The law also outlines what must be included in the security program, including identifying risks, employee training policies, monitoring plan performance, and implementing technical safeguards around data. Violations of the law are subject to penalties of at least $100 per day, not to exceed $10,000 in one year.[31]

Oregon is the most recent state to pass a data broker registration law (HB 2052). The law was enacted in late July 2023, and similar to Vermont, California, and Texas, requires data brokers to pay a fee and register with the Oregon Department of Consumer and Business Services.[32] Oregon defines data brokers as a business entity or part of a business entity that collects and sells or licenses "brokered personal data" to another person, and broadly defines "brokered personal data" as any computerized data elements about an Oregon resident if those elements are categorized or organized for the sale of licensing to another person.[33] This includes basic information about an individual, such as name, addresses, birthdate or place, biometric information, social security number (or any government-issued identification number) and any other information that alone or in combination with other licensed/sold information that can be reasonably associated with an Oregon resident.[34] Data brokers that violate the broker registration law may face penalties up to $500 for each violation, each day (with a yearly cap of $10,000). HB2052 is set to go into effect Jan. 1, 2024.[35]

Though each state has slightly different rules, each state defines "data broker" and "personal data" broadly, requires data brokers to register, and have similar penalties for violations. While the similarities in state regulations could conceivably provide a roadmap to federal regulation, it is also possible that U.S. federal regulation of data brokers will go beyond what the states have implemented and further burden the industry with additional complexities if federal law does not preempt state laws.

B. Role of the U.S. Federal Agencies

Congress and federal agencies are becoming increasingly bullish on data broker regulation. While this is not new –there have been proposed Congressional bills and statements by federal agencies regarding data brokers over the years--the Consumer Financial Protection Bureau ("CFPB") recently announced that it plans to propose rules under the Fair Credit Reporting Act ("FCRA") requiring data brokers to comply with the FCRA.[36] The FCRA establishes data privacy requirements when consumer reporting agencies use consumer data for items such as credit and employment. The stated purpose of the to-be-proposed rules is to protect American consumers from data brokers by subjecting data brokers to greater oversight and regulation, ensuring that sensitive consumer data is protected, and preventing misuse and abuse by data brokers.

> ***Though each state has slightly different rules, each state defines "data broker" and "personal data" broadly, requires data brokers to register, and have similar penalties for violations***

In order to require data brokers comply with the FCRA, according to CFPB Director Rohit Chopra, the CFPB is considering categorizing a data broker that sells certain types of consumer data, such as a consumer's payment history, income, and criminal records as a "consumer reporting agency," thus triggering requirements to ensure that the data sold is accurate, prohibits misuse, and contains a mechanism to handle inaccurate information.[37] The rationale behind treating data brokers selling those types of consumer data as a consumer reporting agency centers around how that data is used. According to the CFPB, this type of data is typically used for credit and employment determinations, and thus should comply with the FCRA.

The CFPB and Director Chopra noted that the CFPB's rulemaking will complement other federal agencies, specifically recognizing the role of the Federal Trade Commission (FTC) as leading many efforts on privacy and data security.

The FTC has been actively involved in evaluating the conduct of data brokers for over a decade.[38] As the federal commission tasked with overseeing consumer protection, the FTC's primary concerns regarding data brokers have centered around data security, transparency, and misuse of personal information. In 2012, the FTC issued Orders requiring nine data brokerage companies to provide the agency with information about how they collect and use consumer data, specifically with respect to privacy practices.[39] That same year, they also called on the data broker industry to improve business practices by increasing transparency.[40] The FTC has continued to devote resources to gathering information about data brokers, monitoring data broker practices, and has filed suit against companies for alleged violations of the FTC Act[41] and the FCRA. The FTC views the collection, use and sale of consumer data as having the potential to cause harm to consumers due to the sensitive nature of the information collected, possible lack of protection of such data, and the potential for misuse.

The FTC Act, which prohibits deceptive and unfair practices, gives the FTC the authority to initiate enforcement actions or perceived violations of the FTC Act. The FTC has used this authority to take action against various data brokers for violations of the FTC Act consumer protection laws. The cases have resulted in significant settlements requiring data brokers to pay fines, institute tighter security measures, provide clearer disclosures to consumers, or cease operations entirely. In 2014, the FTC filed suit and agreed to settle with two data brokers on violations of the FCRA and FTC Act.[42] The allegations revolved around the use of consumer data without notifying consumers that their information was being reported, and without ensuring accuracy.[43] The FTC also published an extensive report calling for transparency and accountability for data brokers.[44] In this report, the Commission recommended that Congress consider enacting legislation to regulate data broker practices, and allow consumers to have more rights and access to their data. The key findings in the report emphasized the limited control consumers have over their personal data. The collection of data, often without consumer knowledge, can flow through multiple layers of data brokers, allowing data to be exchanged between brokers, and leading to multiple levels of data brokers storing, accessing, and making inferences about consumers based on this data.[45] All harms that the FTC would like to protect against.

> ***The FTC Act, which prohibits deceptive and unfair practices, gives the FTC the authority to initiate enforcement actions or perceived violations of the FTC Act***

While Congress has not enacted legislation based on the FTC's recommendation, the FTC continues its pursuit against alleged consumer harms caused by data brokers. In 2016, the FTC issued an Order settling charges against a data broker operation who was alleged to have fraudu-

29 See Texas S.B. No. 2105, Sec. 509.001 (2023).

30 See Texas S.B. No. 2105 (2023)

31 See Texas S.B. No. 2105, Sec. 509.008 (2023).

32 See Oregon H.B. 2052 (2023).

33 Oregon H.B. 2052, Section 1 (2023).

34 See Oregon H.B. 2052, Section 1 (2023).

35 Oregon H.B. 2052, Section 1, 7 (2023).

36 See Protecting the Public from Data Brokers in the Surveillance Industry, August 2023

37 See Remarks of CFPB Director Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices, August 2023.

38 See Data Brokers: A Call for Transparency and Accountability, 2014; and FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information | Federal Trade Commission.

39 See Order to File Special Report.

40 See FTC Report, Protecting Consumer Privacy in an Era of Rapid Change, March 2012.

41 15 U.S.C. §§ 45(a) et. al.

42 See Consent, U.S. v. Instant Checkmate, Inc.; and see, U.S. v. Infotrack Information Services, Inc.

43 See Complaint, U.S. v. Infotrack Information Services, Inc. (2014).

44 See Data Brokers, A Call for Transparency and Accountability, FTC, May 2014.

45 See Data Brokers, A Call for Transparency and Accountability, FTC, May 2014.

lently collected and sold consumer data without their consent, in violation of the FTC Act, resulting in a $7 million harm.[46]

In the past year, the agency has reconfirmed its commitment to protecting sensitive consumer data, including geolocation and health data, promising that protecting consumer data is a top priority.[47] The FTC also warned that they are committed to using the "full scope" of their authority to enforce the law against illegal use and sharing of highly sensitive data.[48] To emphasize the point, the FTC filed a complaint alleging that a location data broker engaged in unfair or deceptive acts in violation of the FTC Act when it acquired consumer's geolocations data and utilized this data to track consumer's movements and locations.[49] The complaint alleged the data broker sold precise geolocation data associated with unique identifiers revealing consumers visits to sensitive locations, and that the data broker employed "no technical controls to prohibit its customers from identifying consumers or tracking them to sensitive locations." [50] The lawsuit claimed the sale of the highly sensitive data put consumers at significant risk and would likely cause substantial injury. The FTC sought to stop the sale of the sensitive geolocation data by permanently barring the data broker from selling consumer data in the future and requiring the company to delete the data it has collected. The case was dismissed, ordering that while the FTC's legal theory of consumer injury was plausible, the FTC had not made sufficient factual allegations to proceed. To do so, it must not only claim that the practices could lead to consumer injury, but that they are likely to do so.[51] In response, the FTC filed an amended complaint that currently is under seal.

The setback has not deterred the FTC from staying at the forefront of the data broker regulation efforts. The agency has shown that it will not hesitate to go after companies for alleged misuse of consumer data, including the collection, retention, and exchange or sale of this sensitive data. To accentuate the point, in late September, 2023, speaking at the 2023 Consumer Data Industry Association Law & Industry Conference, the Director of the FTC's Bureau of Consumer Protection voiced his concern with data brokers looking to "maximize" data at the cost of the consumer, posing serious risks. [52]

It is clear that there will continue to be scrutiny and enforcement around data brokers. Though the federal landscape lacks a comprehensive regulatory framework, the FTC has become the federal agency leading the charge against alleged violations by data brokers, and individual states have taken the initiative to introduce and pass legislation regulating data brokers.. As the economy evolves and data becomes an even more invaluable commodity, we can expect to see new state and federal laws regulating data brokers.

It is clear that there will continue to be scrutiny and enforcement around data brokers

46 See Stipulated Order, FTC v. Sequoia One, LLC (Nov. 2016)

47 https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

48 https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

49 *FTC v. Kochava Inc.*, Case No. 2:22-cv-00377 (Complaint).

50 *FTC v. Kochava Inc.*, Case No. 2:22-cv-00377 (Complaint).

51 See, *FTC v. Kochava Inc.*, Case No. 2:22-cv-00377 (Memorandum Decision and Order), May 24, 2023

52 https://www.ftc.gov/system/files/ftc_gov/pdf/cdia-sam-levine-9-21-2023.pdf.

07
CONCLUSIONS AND OUTLOOK

Data brokers face additional and varying restrictions in state and federal privacy and consumer protection laws that will increase their compliance costs. Consumers may benefit from added privacy protections if the new laws and regulatory actions enhance data accuracy, the quality of disclosures, transparency, and fair information processing practices. But, consumers may suffer from reduced competition, fewer charge-free information services, price increases, and stifled innovation if additional regulations result in reduced competition, data sharing, and information availability. Established businesses with large amounts of data do not have to sell or share their information and could rely less on data purchases. Similarly, data brokers that amass large amounts of unique data can pick winners and losers if they decide to whom they will and will not sell their data. Legislators will need to be thoughtful about data broker regulations—if regulation creates barriers to easy entry, it can put smaller players at a competitive disadvantage, resulting in data being consolidated into the hands of few. Smart, balanced regulations can create an environment where data brokers have a positive impact on the competitive marketplace. As regulators continue to evaluate the impact of data brokering on both privacy and competition, this discourse will continue to evolve.

Data brokers face additional and varying restrictions in state and federal privacy and consumer protection laws that will increase their compliance costs

IS PERSONAL DATA **STILL UP FOR GRABS?**

BY
ADRIANA HERNANDEZ PEREZ

Adriana Hernandez Perez holds a Ph.D. in Economics from the Toulouse School of Economics, France, a Master's degree in Economics from Fundação Getulio Vargas, Brazil, and a Bachelor's degree in Economics from the Federal University of Rio de Janeiro. She worked as a researcher at FGV, was head of R&D at Banco Itaú-Unibanco, and served as a consultant for the World Bank. Currently, she is part of the technical team at Consultoria Tendências since 2021. She has extensive experience in higher education and is currently a professor in the Master's program in Economics and Finance at Fundação Getulio Vargas. Adriana is a Non-Governmental Advisor (NGA) at the International Competition Network (ICN) and coordinates research on Brazilian competition case law as a member of the Brazilian Institute of Studies on Competition, Consumer Affairs, and International Trade (IBRAC). Linkedin https://www.linkedin.com/in/adriana-hernandez-perez-b351b017/.

01 SETTING STAGE

Economic theory praises the widespread use of information, given its non-rival features. However, the collection, compilation and processing of information, a core feature of digital economies, where data brokers play an important, can also present some risks, from privacy concerns to paying higher prices, extortion, and fraud.

This article reviews the economics of data and data privacy. Central to our discussion is the

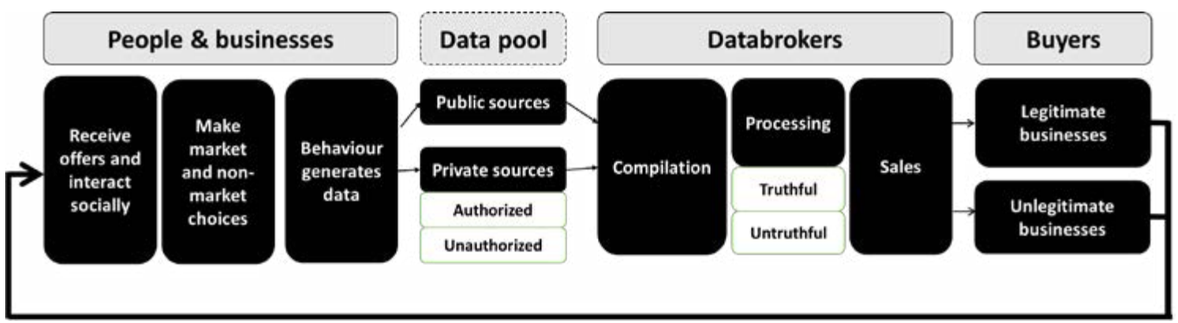
pivotal role played by data brokers in the circulation of information, and the pressing need to mitigate the associated risks. Before delving into the topic, some crucial elements of the environment must be characterized.

Data brokers collect, process, and sell information that was not necessarily transferred to them in a conscious or proper transaction-like manner by the owner of that information, being people or businesses (also referred to as data subjects). Also, data brokers can sell truthful or misleading information about its subjects.

Information can be collected from a variety of sources, public or private, and can span from public records, with demographics like age, gender, and address, but also detailed information on online transactions and searches, social media activities and interactions, location tracking, health data, among others. In the digital word, users normally allow data to be collected, compiled, and sold in exchange for free online services. This is the case of internet search engines, email and messaging services, social networks, and apps, among others.

Data buyers are very heterogenous, ranging from legit businesses such as targeted advertising, credit scoring, risk management, and market research, to non-legit business, such as fraud and extortion. While the latter is very concerning and is undoubtedly damaging to people and businesses, the former is not absent of concern either. Also, because data buyers are so widespread, seemingly unrelated markets are becoming increasingly connected.

The figure below shows how information generated by people and business flow through data brokers who compile, process, and sell information to interested buyers, which in turn act upon it, adjusting their strategies when interacting with people or businesses, who will make new decisions, creating new behavioral data to be tracked and furthermore transacted, in a cyclical data producing engine. Finally, data brokers and buyers may be integrated or the (digital) environment where data is generated may belong to a private business, as is the case of GAFAM companies.



The above description raises concerns on the potential setbacks related to the performance of the data broker market but also in connecting and seemingly unrelated markets. I emphasize on three of them. However, before we delve with these potential setbacks, it is important to qualify the importance of information on new products' development, innovation, and economic growth.

02
DATA: THE MORE, THE MERRIER?

Information is characterized as a non-rival good in economic theory, which means that, once 'out there', its consumption by one person does not prevent other from consuming it.[2] Information, then, differs from a regular (rival) product, such as apples and oranges, where the consumption of a fruit eliminates it for other person's consumption. Information, then, is closer to the classical example of light provision in a given street, where the use of one passerby does not prevent other passerby's use of the light.

Given that information may be an important input for new products and services innovations, it is desirable to have as much as possible of it. However, as a non-rival good, the economic theory forecasts that, if information is costly, then markets would underperform because the sellers of information would not be able to prevent consumers from using information once the first transaction occurs. Given it is easily copied and could be distributed (almost) freely, sellers would not have incentive to sell it and buyers would miss out on valuable information.

2 For an up to date discussion on this feature of data, see Charles I. Jones & Christopher Tonetti, *Nonrivalry and the Economics of Data* AMERICAN ECONOMIC REVIEW, 110 (9), 2819-58 (2020). Available in this link.

In our example of street lighting, one of the solutions to curb its under provision is for the State to coordinate and organize the service in exchange of taxpayers funding. There are also cases where open access is incentivized (or mandated) as the case of publicly funded research or anonymized health data. The aim is to foster broader access to data that can help societies better understand its needs and expand new research frontiers.

In the music and software business, open access policies aren't prevalent. Instead, there's a heavy reliance on instruments like licensing and royalties to safeguard intellectual property. This ensures that creators can earn from their endeavors. Similarly, in the innovation sector, governments have instituted patent systems. These not only allow inventors to profit from their creations but also ensure that society is provided with detailed descriptions of these innovations, making their features more accessible.

Other solution includes giving free access to basic information content, but charge for a more elaborate content. This is the case of newspapers or online reviews (CPI does it), that allow online readers to access the headlines and a short descriptive paragraph of the article but charge a fixed subscription fee for full articles access. Another solution is getting some sponsorship, public or private, that would subsidize the flow of information.

03
PERSONAL DATA IN THE DIGITAL AGE

It's vital to examine if the public and private solutions, widely accepted in various markets to promote information dissemination, are apt for managing the flow of personal data. This becomes especially pertinent when such information can sway economic results in favor of specific groups, potentially intensifying society's most pronounced inequalities.

One thing for sure is that personal data has been historically up for grabs. With the gigantic expansion of the digital economy, not only the capture of personal data became easier, but also an exponential amount of data is being created about people's behavior by the minute. So, while the flow of personal information may help developing many new products and services, there is a clear dilemma with respect to how this information is treated and used and if it flows in a secured and transparent fashion.

This leads to the first of three concerns regarding the main actors in the personal data market, the data brokers.

It's vital to examine if the public and private solutions, widely accepted in various markets to promote information dissemination, are apt for managing the flow of personal data

A. Concern 1: Is There Excessive Consent to Sharing Personal Data?

There is a concern whether data brokers are selling something that does not belong to them. European and Brazilian privacy regulations have given property rights to data subjects, that is, to individuals to whom the data pertains.[3] As a result, data brokers must have the individual's consent to use, treat and trade personal information. Despite that, not only personal data is compiled from a variety of sources without much owner control, but a big portion of it corresponds to personal data generated and collected in the digital environment (platforms, websites, cookies, apps, etc.) under the "I Agree to Privacy Policy" checkboxes.

Following these regulatory reforms on privacy, the web user now explicitly decides whether it allows data collection, use and sale to fully navigate in a particular website. However, people face transaction costs from reading long privacy contracts or ticking non standardized checkboxes.[4] Recall how people have learned to use internet websites or 'free' online services: they frequently and intensively navigate the internet, hopping from one site to another, not much aware of privacy risks and benefits. After the enactment of privacy regulation, it is hard to overcome the usage intensity to con-

3 The European privacy Law is known as General Data Protection Regulation and, in Brazil, the corresponding law is Lei Geral de Proteção de Dados, both enacted in 2018.

4 I disagree with the assertion that distributing property rights would be enough, as stated in Charles I. Jones & Christopher Tonetti, *supra* note 2.

sider privacy issues, especially when you do not know what is at stake. [5]

In this very inefficient contractual environment, it is expected that people, willing to have immediate access to online services, just click whatever comes to mind in order to be serviced, without having a full picture of the impact on the offers they get on prices, services, news feeds, advertising, consumer and political profiling and, let's not forget, fraudulent or abusive conducts.

This 'one-click-away' environment, combined with the lack of transparency regarding its use, may lead people to consent excessively their personal data. Given the pervasive use of nudged frameworks everywhere in the digital economy, clicking away privacy seems to be a good shortcut to content and 'freebies' from digital economy services. Additionally, when one person's behavior informs about other person's behavior, like friends and peers, the negative externality on privacy is even stronger.

As a corollary, in a fully nudged online environment, where companies are incentivized to harvest personal data for profit, people may end up acting more loosely with respect to their privacy. This is a well-defined market failure, as data is commercially valuable and there is excessive collection, treatment, and transactions of data.

Granting property rights to data subjects alone is insufficient in addressing an externality when transaction costs are high, as Coase has taught us.[6] It is imperative to ensure adequate transparency so that individuals have a clear understanding of what they are clicking into.[7]

It is useful to use the framework of analysis from an informational perspective, that is, *How informed are we about giving up our personal information?*

In this perspective, this market resembles one of a credence good. A *credence good* is a type of product or service where its quality is difficult to ascertain even after its purchase and use. A classic example of credence good are medical services, as the patient does not know and will never know if its treatment was the adequate one.

As it stands today, it is impossible for the 'data subject' to know, after clicking away its data, how the information is being used to its benefit, demise or something in between. For credence goods, when people do not have information to judge the cost-benefits of data consent even after consent is done, they usually rely heavily on reputation or trustworthy recommendations or just plain inertia. Nevertheless, they might be taken advantage of by unscrupulous providers. In health services, there are plenty of healers pretending to perform great deeds.[8] Recently, financial gurus, who make their livings on viewers, are on the rise, using platforms like YouTube channels to catch followers. Seemingly, a worrying proportion is being accused of financial schemes or, at least, giving ludicrous financial advice.

In summary, the inefficient way personal data consent takes place affect related and seemingly unrelated markets. This means that spillovers or externalities spread across different markets, amplifying the impact of this market failure.

> ***This 'one-click-away' environment, combined with the lack of transparency regarding its use, may lead people to consent excessively their personal data***

B. Concern 2: Data Brokers Can Sell Misleading Information

The second concern is related to the sale of misleading or biased information about consumers and businesses. If data brokers' clients cannot identify whether the information being sold is truthful, we have an additional market failure due to the asymmetry of information between parties. Would data brokers' objectives be aligned with their clients? If pricing on data is positively correlated to the performance of the buyer in using that information, then the asymmetry mentioned would not pose an efficiency problem. In this case, it will be in the data broker's best interest to sell the most accurate information, so the buyer maximizes its profit.

However, while the impact of misleading and biased information can be very detrimental to the most vulnerable segments of society, one should also be cautious when the information provider has access to unique strategic data and competes in the same (or related) market of their data buyers. Such players would be able to sell misleading information if there is no proper third-party auditing or market contestability. The motivation to take action would hinge on weighing the short-term gains from selling deceptive information to potential competitors against the potential long-term loss in revenue from not being viewed as a reliable data source.

C. Concern 3. Tipping Rents Under Price Discrimination

The third concern is due to the welfare reducing potential of such activities. Suppose that an airline has invested in a technology that enables her to discover more about its customer base, such that it can better forecast their propensity to pay for an air ticket. In the extreme case where the company knows perfectly the customers' propensity to pay and it can segment and sell to each consumer separately, the airline can extract all the gains from trade. Customers are left with the air ticket, but nothing else, since they just paid their maximum reserve price.[9]

In other words, the ability to access this crucial information about its customers enables to airline company to fully maximize its profit but prevents customers from getting anything closer to a bargain - much on the contrary - they pay exactly the maximum amount it would be willing to give up for the ticket.

Then, having access to data, if not very costly, makes the airline company better off. However, all those customers that were already buying the product before the adoption of this technology are worse off[10]. Perfect discrimination leads to a well-known puzzling result in economics: all transactions that are mutually beneficial take place in equilibrium, which is a highly efficient outcome, but the distribution of gains from trade are extremely unequal, as all gains tip to the seller.

Even when the company cannot segment customers by their propensity to pay, companies can make offers that lead customers to 'reveal' how much they value the service or product.[11] Although this strategy entails some 'revelation' costs for the company, it may still be better than charging an uniform price across consumers. If customers' valuations are very diverse, discrimination hurts customers *ex-ante* whenever the company can better guess who are the most valuable customers.[12] This is because it can customize offers to avoid giving significant discounts to customers who have a higher willingness to pay.

04

HOW TO PROTECT THE 'DATA SUBJECT'? MARKET MECHANISMS AND PUBLIC POLICIES

When a company values its reputation for customer privacy, it typically tends to prioritize, invest, and signal to its customer base. This competitive edge often results in enhanced privacy protection for users. Indeed, several prominent companies, especially in the messenger and email service sectors, actively promote their commitment to data security and take measures to prevent data leaks, for instance.

However, problems still arise when, while using a website or an app, consumers are only asked once about personal data access and usage. Furthermore, by accepting a website cookie, the user's browsing will be tracked for an unspecified duration, or at least until the cookies are deleted. Meanwhile, how often does a banner you consistently decline reappear until you accidentally click 'Yes'?

When poor practice is hidden from view and drives competitive advantage, a more ostensive privacy protection policy should be introduced. The policies that remain consistent and robust in the face of advancements in behavioral economics literature are those focused on

5 A recent study accounts that consumers would give greater value to their personal data in the case of an opt-in system than an opt-out system. See Alessandro Acquisti, Leslie K. John & George Loewenstein. *What is privacy worth?* THE JOURNAL OF LEGAL STUDIES 42.2, 249-274 (2013).

6 See discussion over the Coase Theorem in Stigler, G. J. THE THEORY OF PRICE (3rd ed. 1966). New York: Macmillan.

7 For an excellent review on economics of privacy, see Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, JOURNAL OF ECONOMIC LITERATURE, 54 (2), 442-92.(2016).

8 About this phenomenon, the reader is referred to the classic 1957 Italian movie 'Il medico e lo stregone', where the healer is played by an incredible Vittorio de Sica.

9 In economics, this is described as first-degree-price-discrimination or personalized pricing.

10 Overall, the effect of improved discrimination can be negative for consumers if the market is already covered by the companies.

11 This is referred to second-degree price discrimination.

12 See Chapter 2 of Jean Jacques Laffont & David Martimort, THE THEORY OF INCENTIVES: THE PRINCIPAL-AGENT MODEL, Princeton University Press (2002).

strengthening market information flows and consumer education.[13] The literature on consumer policy in the context of asymmetric information presents interesting solutions, some of which are already available in the market. There are plenty of tools and services that can significantly enhance online privacy – although no solution is entirely foolproof.[14]

The first one is to strengthen the dissemination of proper standardized framework of choices for the consumer, who must be promptly shown the menu of options with respect to data usage Typically, it includes the following four options: (i) personalization; (ii) marketing and ads; (iii) improving services; (iv) third-party sharing. If there is third-party sharing, like data brokers, it should be given transparency into who buys their data. Here, it would not be necessary to name specific companies, but general profiles like “Marketing Agencies” or “Health Research Firms”. This would give individuals a clearer picture.

The second one is to incentivize websites and privacy certifiers to inform the degree of risk and benefit of how giving consent in a *certain platform*, in light of the previous history of the platform on selling information to data brokers or experiencing data leaks. Therefore, just as investors are informed of potential financial risks, individuals should be informed of the potential risks associated with their data being sold or misused. This can also include steps describing the data broker takes to mitigate these risks.

The third one is to enforce the disclosure of data transaction by data collectors and data brokers on data acquisition and sales. This information is essential to help third parties map broadly people’s risks.

Fourth, and related to the previous point, is to incentivize services that would evaluate *how exposed is the individual*, given information over its online track record or footprint. An individual’s risk profile can be determined by analyzing the cookies, apps, and online services they use, along with information about past data breaches that impacted them.

While risk transparency is essential, presenting this information requires meticulous consideration, leveraging insights from behavioral economics, to ensure individuals grasp the consequences of their decisions. For instance, one should consider offering an informative *summary box* on the risks and benefits of its personal data exposure, where they could be alerted to potential risks of fraud, as well as the dangers of paying elevated prices for specific products or facing excessive online privacy exposure and its likely repercussions.

Fifth, incentivize opting-out services, where you can suspend data collection, and “delete” services, where you can ask to delete their existing (online) data.

> ***While risk transparency is essential, presenting this information requires meticulous consideration, leveraging insights from behavioral economics, to ensure individuals grasp the consequences of their decisionsa***

13 See Spiegler, BOUNDED RATIONALITY AND INDUSTRIAL ORGANIZATION, Oxford: Oxford University Press (2011).

14 For a comprehensive review on the interplay between customer policy and competition policy, the reader is referred to Mark Armstrong, *Interactions between competition and consumer policy*, COMPETITION POLICY INTERNATIONAL 4.1 (2008).

05
REGULATION MOVING FORWARD

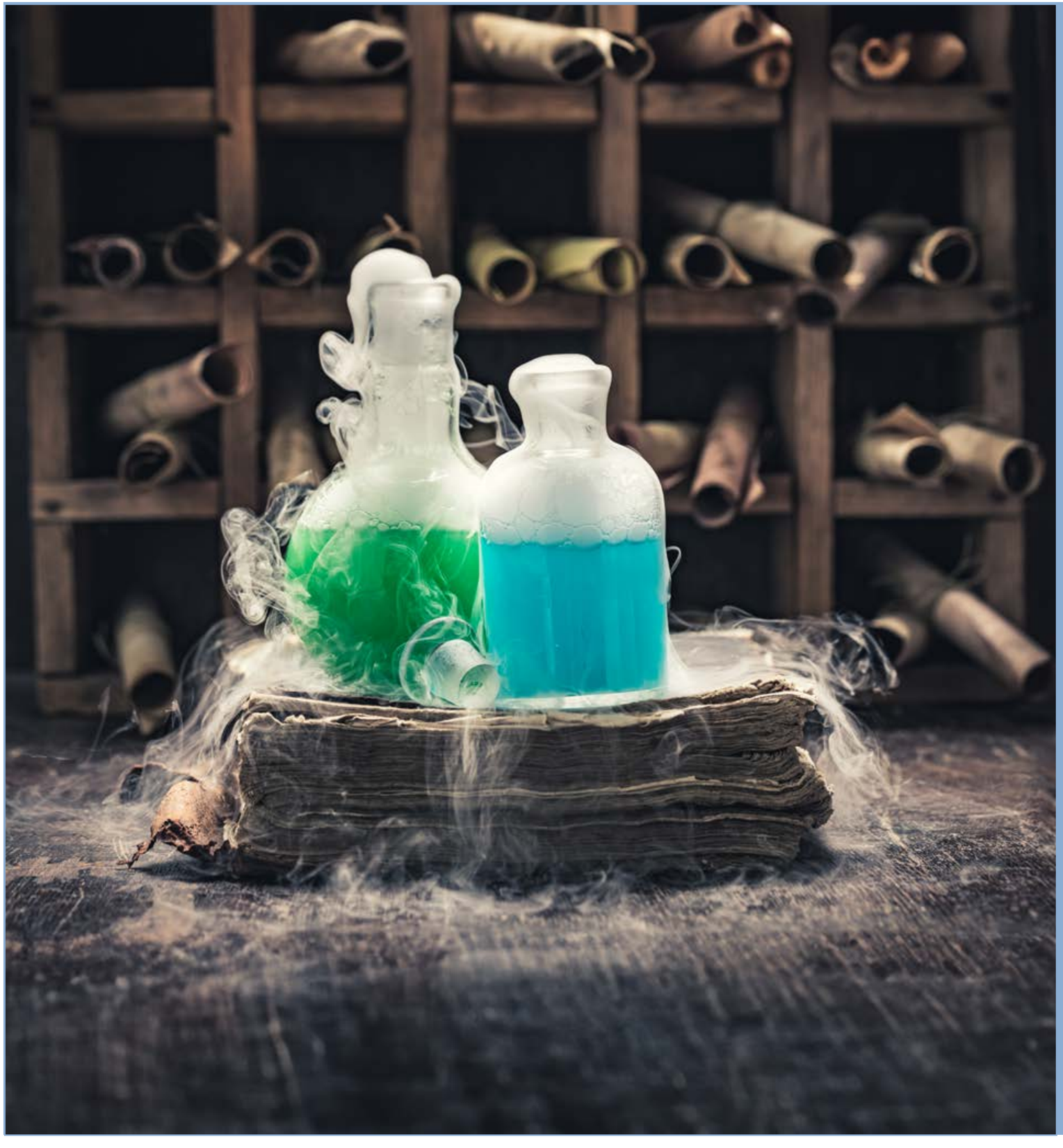
Finally, one must consider how these policies, once implemented, would affect the companies and the way they compete and collect data. Companies can react to summary boxes by adjusting their strategies to dimensions that remain invisible to the consumer.

The introduction of privacy regulations in major jurisdictions prompted businesses to adhere, but often on their own terms. Consent is often sought and provided in a less-than-transparent manner. Regulation must try its best to anticipate such movements and keep up to date to obscure business practices.

Data brokers must play an enhanced role on helping strengthening market transparency. This can be achieved by actively encouraging (or reinforcing) the reporting of data transactions and data breaches.

Finally, while the examples above discuss mainstream theory on market transactions, there’s limited understanding of the impact of personal information dissemination on interpersonal relationships, privacy rights, and political oversight, among others. Regardless of the context, data brokers are pivotal in implementing essential changes to enhance people’s protection. ■

> ***Finally, one must consider how these policies, once implemented, would affect the companies and the way they compete and collect data***



KEEPING UP WITH THE ALCHEMISTS – REGULATING DATA BROKERS IN AUSTRALIA

BY
CHANDNI GUPTA

Chandni Gupta is the Deputy CEO and Digital Policy Director of the Consumer Policy Research Centre (CPRC). CPRC is an independent, not-for-profit, consumer think-tank that champions new thinking to create systemic change for consumers through evidence-based research.

01 INTRODUCTION

Data brokers are the alchemists of our digital world – mining and refining our personal information and selling it to the highest bidder.

Insights from data broker services can support businesses to refine their advertising targeting strategies which can be anything from personalising what products consumers may be offered, what prices they pay, or whether they are excluded from specific products and services. In Australia, there is little to no transparency in how data brokers collect, share and use personal information.

This article throughout highlights research from the Consumer Policy Research Centre ("CPRC") on what consumers expect from businesses that are dabbling with their personal information, and the confidence they have in being protected from data misuse. It comes with no surprise that there is a significant gap in what consumers expect and what happens in reality. This article highlights necessary reforms, including laws against unfair business practices, modernizing privacy protections, and interim labelling requirements to enhance transparency across regulators and consumers. It also explores the concept of a best-interests duty or a duty of care and its potential to shift the onus of responsibility from consumers to businesses within the data brokering landscape.

02

TIERS OF DATA BROKER HARMS

There are four tiers of harms that consumers face when their data is collected, processed and analyzed by data brokers.

- **Manipulation**: Companies can use sophisticated techniques to manipulate online user interfaces, often employing deceptive and manipulative designs (also known as dark patterns) to exploit consumers' psychological vulnerabilities. This manipulation can lead to unfair outcomes, data misuse, loss of privacy, and distortions in the competitive landscape. CPRC's research into dark patterns revealed that manipulative online design is costing Australians money, and is leading to a loss of control over their personal information as well as impacting their well-being – 83 percent of Australians have experienced negative consequences as a result of dark patterns.[2] There is also no shortage of examples where data broking practices can exploit people's vulnerabilities for profit. As an example, in 2019 data broking company Quantium was found to be using de-identified transaction data from the National Australia Bank which was supporting advertising for the gambling business Sportsbet.[3]
- **Discrimination and exclusion:** Data curated by brokers can be used to discriminate against consumers, creating digital redlining. Commercial entities may profile consumers, effectively assigning a "value score" to them, which can lead to discriminatory practices in advertising and pricing. Lack of transparency in this process makes it challenging for consumers to understand or influence their profiles, potentially resulting in some groups paying more for the same services.[4] For example, in 2020 a CHOICE investigation into personalised pricing found that people over the age of 30 were offered prices more than double that of those aged under 30 on the dating app, Tinder. While it is not a direct example of use of data brokers, it highlights the issue of how targeted profiling can lead to discriminatory and exclusionary practices.[5]
- **Lack of control**: Consumers often feel uncomfortable with the extensive data collection and lack of control over their information. Personal data can be traded between companies in supply chains without consumer awareness,[6] and terms and conditions can be unclear or ineffective at enabling informed choices. [7]
- **Data breaches**: There is a lack of confidence in companies' ability to secure data, despite the expectation that they should. CPRC's consumer research confirmed that while the majority of Australians (84 percent) agree that businesses should be responsible for keeping their data safe, there is little to no confidence (less than 26 percent) in businesses actually doing so.[8] Data hoarding by brokers increases the risk of sensitive information exposure, potentially leading to identity theft and fraud. For instance, Equifax experienced a massive data breach in 2017, exposing personal information of over 147 million Americans.[9] In Australia, issues with Equifax involved data quality, misleading consumers and making inappropriate disclosures.[10]

03

DATA BROKING IN ESSENTIAL MARKETS

A competitive market should enable consumers with the freedom to choose, yet choice is often absent when data broking is combined with essential services such as renting. Renters do not have the luxury to choose the process or the platform that a rental provider or agent utilizes as part of the application process. They are compelled to divulge extensive personal information, including IDs, employment, and financial details, with no control over its handling, relying solely on general information privacy principles. Unlike typical consumers, renters are not the direct customers; property owners hold that status. While some states in Australia have estate agent regulations that offer some protection for renters, they do not adequately address the broader issues of data collection, sharing, and use by third-party platforms involved in data brokering.[11]

04

WHY AUSTRALIAN PROTECTIONS DON'T GO FAR ENOUGH

Privacy policies often claim data collected by data brokers is anonymized or aggregated. However, these practices are insufficient in protecting consumers. De-identified data, while not immediately harmful to an individual, can affect groups or communities when aggregated.[12] It can also be used against similar individuals not in the original dataset.[13] CPRC research has also shown that de-identified data like telephone metadata, transaction history, and social connections can be re-identified. [14]

In addition to how data may be treated, it is unlikely that consumers will engage with a legalese and laborious privacy policy, which often appears at the precipice of accessing a product or service. In fact, CPRC's 2020 consumer research found that 94 percent of Australian consumers reported not reading all of the privacy policies or terms and conditions that applied to them in the past 12 months. For those who had engaged with any privacy policy, 69 percent accepted the terms even when they were not comfortable with them. To further add to this power imbalance, even if a consumer engaged with a policy, most consumers are unlikely to recognize many of the data broker business names or realize that data brokers are part of that particular ecosystem. Within privacy policies, data brokers may not always be referred as per their name, but more obscure terms such as 'trusted partners', 'data partners' or 'data sources' may be used to refer to these third-parties, which may feed in or have a pipeline into consumer data.

2 CPRC, *Duped by design - Manipulative online design: Dark patterns in Australia*, (June, 2022), https://cprc.org.au/dupedbydesign/.

3 Brigid Richmond, *Research Report: A Day in the Life of Data, (May 29, 2019),* https://cprc.org.au/research-report-a-day-in-the-life-of-data/.

4 Cathy O'Neil, Weapons of Math Destruction 143 (2016).

5 CHOICE, *Tinder charges older people more,* (August 11, 2020), https://www.choice.com.au/about-us/media-releases/2020/august/tinders-secret-pricing-practices.

6 Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (May, 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

7 Brigid Richmond, *Research Report: A Day in the Life of Data, (May 29, 2019),* https://cprc.org.au/research-report-a-day-in-the-life-of-data/.

8 CPRC, *Not a fair trade,* (March, 2023), https://cprc.org.au/not-a-fair-trade/.

9 Alfred Ng, *How the Equifax hack happened, and what still needs to be done*, CNET, (September 17, 2018), https://www.cnet.com/news/privacy/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed.

10 Andy Kollmorgen, *Equifax data breach a 'one-off', agency claims*, CHOICE, (August 18, 2021), https://www.choice.com.au/consumers-and-data/protecting-your-data/data-privacy-and-safety/articles/equifax-security-breach.

11 Commissioner for Residential Tenancies, personal communication, July 26, 2023.

12 Katharine Kemp, *Concealed data practices and competition law: why privacy matters*, (November, 2020), European Competition Journal, Volume 16, 2020 – Issue 2-3, https://doi.org/10.1080/17441056.2020.1839228.

13 CPRC, *In whose interest: Why businesses need to keep consumers safe and treat their data with care*, (March, 2023), https://cprc.org.au/in-whose-interest/.

14 Brigid Richmond, *Research Report: A Day in the Life of Data, (May 29, 2019),* https://cprc.org.au/research-report-a-day-in-the-life-of-data/.

This ecosystem thrives due to the absence of adequate parameters. Australia's outdated privacy protections, piecemeal approach to privacy enforcement and no overarching laws against unfair practices, makes the digital ecosystem ripe to take advantage of consumers under the guise of providing choice in products and services.

Unlike other countries that have prohibitions on unfair practices, business practices that lead to unfair consumer outcomes are currently not illegal in Australia. This means that businesses predicating on opaque business practices that undermine consumer autonomy or exploiting consumer vulnerabilities and failing to provide accessible and meaningful support are all operating under legitimate business models.[15] Many of these business models exist within the data broking landscape.

Furthermore, in Australia the current approach to safeguarding consumer privacy still centers around notification and consent. This system places consumers in a situation where they make a single decision regarding data sharing, which could have lasting consequences throughout their lifetime. This one-time choice is not a fair arrangement. Relying heavily on notification and consent empowers businesses to gather substantial volumes of customer data and employ it for a wide range of purposes. Presently, there are no safeguards in place to prevent businesses from burying consent for the collection, sharing, and utilization of personal information, including its aggregation with other data points within lengthy and intricate terms and conditions.

05
WHAT DO AUSTRALIANS WANT?

It is clear there is a chasm between what consumers expect of businesses and what is actually happening when it comes to their data. CPRC's research found 74 percent of Australians are not comfortable with companies sharing or selling their personal information, and less than 10 percent are comfortable with the status quo of targeted advertising (i.e., based on monitoring online behavior or using personal characteristics without express permission).

Consumers want the confidence to know that if they are participating online, they can do so without having their personal information shared and used as a mere commodity. CPRC's research found that:

- 79 percent of Australians agree that a company should only collect information that it needs to provide the product or service
- 79 percent do not want companies to sell their data under any circumstances
- 88 percent expect governments to protect them against data misuse, and
- 85 percent expect governments to ensure consumers are not opted-in by default to data collection and sharing options.[16]
- It is clear that consumers need and want adequate guardrails to hold businesses including data brokers accountable to a much higher bar than what currently exists in an Australian setting.

06
WINDS OF CHANGE IN AUSTRALIAN REGULATION

After decades of attempting to enforce outdated protections, Australia is now at a significant juncture of reform. In August 2023, the Australian Government released its regulatory impact statement on introducing laws against unfair business practices, proposing a number of options on how this could be achieved for Australians.

One of the proposals to counteract unfair business practices is to establish an overarching prohibition along with a blacklist of business practices that are deemed unfair. This could lead to a change in shifting data business models that, as yet, are reliant on opacity and exploitative practices as their means for driving profit. In the context of data broking, it has the potential of businesses in the data broking ecosystem, to consider their data-based practices through a lens of fair outcomes for consumers and enable regulators to hold businesses accountable when they fail to do so.

15 CPRC, *Unfair Trading Practices in Digital Markets: Evidence and Regulatory Gaps*, (March, 2021), https://cprc.org.au/unfair-trading-practices-in-digital-market-evidence-and-regulatory-gaps-2/.

16 CPRC, *Not a fair trade,* (March, 2023), https://cprc.org.au/not-a-fair-trade.

However, for this to take meaningful effect, it will involve more than just having a prohibition enshrined in law. When CPRC conducted its research into an unfair trading prohibition, it concluded that, in addition to being drafted as principles-based law with an evolving blacklist, a law against unfair business practices should:

- allow regulators to investigate and proactively enforce the law before widespread harm takes place
- have provisions in place for the law to evolve over time to address new and emerging unfair practices
- hold businesses accountable through penalties and enforcement action that effectively deter unfair business practices
- offer meaningful redress to consumers impacted by unfair practices
- quickly stop practices found to be unfair overseas from making their way to Australia, and
- expand the scope of consumer harm to include the impact on mental health in addition to financial and reputational loss.[17]

In terms of privacy protections, in end September 2023, the Government released its response to the Privacy Act review noting acceptance of several reforms proposed by the Attorney-General's Department in March 2023.[18] It appears that Australia's privacy protections dating back to 1988 are finally making their way into the new millennium. Some of the planned protections that are likely to apply to data brokers include modernising the definition of personal information, introducing a new 'fair and reasonable' test for how businesses collect, use and share personal information, establishing a stronger definition of consent and creating stricter rules on targeting and trading of personal information, especially relating to children.

> ***While a prohibition on unfair business practices and stronger privacy laws certainly enhances protections, there is a broader question on how we ensure safety and care is embedded in how consumer data is handled by businesses in general***

07
WHAT MORE COULD BE DONE?

While a prohibition on unfair business practices and stronger privacy laws certainly enhances protections, there is a broader question on how we ensure safety and care is embedded in how consumer data is handled by businesses in general. The notion of a best-interests duty or a duty of care is not uncommon in many sectors and is now a concept that is slowly being introduced into the data space. New York Privacy Act (NYPA) includes a Data Fiduciary Obligation, and the European Union introduced a duty of care for large technology platforms via its Digital Services Act. In the United Kingdom, the proposed Online Safety Bill proposes a statutory duty of care for social media companies to keep their users safe and tackle illegal and harmful content on their platforms.

CPRC consumer research confirms that Australians support their data being used with their best interests and the interests of the community in mind. Australians agree:

- personal information should only be collected and used in a way that personally benefits them (70 percent)
- their personal information should not be collected and used in a way that harms them or others (83 percent), and
- personal information should only be collected or used if it is in a person's best interest and is unlikely to cause harm to them and others (70 percent).[19]

17 CPRC, *How Australia can stop unfair business practices*, (September, 2022), https://cprc.org.au/stopping-unfair-practices.

18 Attorney-General's Department, *Government's response to the Privacy Act Review Report*, (September, 2023), https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report.

19 CPRC, *Not a fair trade,* (March, 2023), https://cprc.org.au/not-a-fair-trade.

Such an obligation would naturally shift the onus of responsibility from consumers to businesses. A best-interests or duty of care obligation would:

- help move away from individual level of consent and shift the focus to system set-up and embedding safety by design
- protect people that may have the inability to consent such as children, people living with a disability or other consumers who are unable to participate in the consent model, regardless of how well it may be set-up
- align interests of organizations and consumers as taking on new data will mean taking on new responsibilities, which can encourage a culture of data minimisation (collect only what you need not what you think you might need), and
- address issues of trust and confidence in both government and industry.[20]

A practical option is to consider a best-interests obligation that is broad but is supported by clear guidance and rules, including no-go zones which could evolve over time, with the regulator having the power to regularly review and update guidance and no-go zones instead of them being enshrined in legislation.[21] A similar example of this is the United Kingdom's Financial Conduct Authority's Consumer Duty which has a broad principle to act to deliver good outcomes, while being supported by detailed guidance on what that looks like.[22]

08

TRANSPARENCY AS A STOP-GAP PRE-REFORM

You cannot challenge what you do not know. As a minimum temporary measure and before economy-wide reforms are formally enshrined, one option is to consider interim labelling requirements for products and services where data captured or used involves the use of data brokers. This transparency can lay the foundation for improved consumer protection in the future, allowing regulators, researchers, and the public to gain insight into the extent of data brokering, which is presently poorly understood. It can enable regulators to conduct widespread sweeps and target its information-gathering powers to uncover potential data practices that could lead to significant community harm or where the power imbalance between the consumer and market is woefully tipped.

> ***You cannot challenge what you do not know***

20 CPRC, *In whose interest: Why businesses need to keep consumers safe and treat their data with care*, (March, 2023), www.cprc.org.au/inwhoseinterest.

21 CPRC, *In whose interest: Why businesses need to keep consumers safe and treat their data with care*, (March, 2023), www.cprc.org.au/inwhoseinterest.

22 Financial Conduct Authority (UK), *Finalised Guidance - FG22/5 Final non-Handbook Guidance for firms on the Consumer Duty*, (July, 2022), https://www.fca.org.uk/publication/finalised-guidance/fg22-5.pdf.

09

CONCLUSION

There is a regulatory gap to fill to keep businesses accountable for the data they collect, share and use more broadly. There are clear examples where data broking practices can lead to significant digital harms, not only to the individuals but to wider communities, leading to manipulation, exclusion and discrimination, lack of consumer control over their own data and data breaches that leave consumers vulnerable to fraud and scams. Strengthening privacy laws and prohibiting unfair business practices are likely to get Australia regulatory landscape closer to the protections consumers expect and deserve, but there is a wider consideration of how safety and care can be embedded into data practices more generally that delivers consumers with a digital economy that is fair, safe and inclusive.

> ***There is a regulatory gap to fill to keep businesses accountable for the data they collect, share and use more broadly***

WHAT'S **NEXT**

For November 2023, we will feature a TechREG Chronicle focused on issues related to **Tech & Intellectual Property**.

ANNOUNCEMENTS

CPI TechREG CHRONICLES December 2023

For December 2023, we will feature a TechREG Chronicle focused on issues related to **Encryption**.

Contributions to the TechREG Chronicle are about 2,500 – 4,000 words long. They should be lightly cited and not be written as long law-review articles with many in-depth footnotes. As with all CPI publications, articles for the CPI TechREG Chronicle should be written clearly and with the reader always in mind.

Interested authors should send their contributions to Sam Sadden (ssadden@competitionpolicyinternational.com) with the subject line "TechREG Chronicle," a short bio and picture(s) of the author(s).

The CPI Editorial Team will evaluate all submissions and will publish the best papers. Authors can submit papers in any topic related to competition and regulation, however, priority will be given to articles addressing the abovementioned topics. Co-authors are always welcome.

ABOUT **US**

Since 2006, **Competition Policy International** ("CPI") has provided comprehensive resources and continuing education for the global antitrust and competition policy community. Created and managed by leaders in the competition policy community, CPI and CPI TV deliver timely commentary and analysis on antitrust and global competition policy matters through a variety of events, media, and applications.

As of October 2021, CPI forms part of **What's Next Media & Analytics Company** and has teamed up with **PYMNTS**, a global leader for data, news, and insights on innovation in payments and the platforms powering the connected economy.

This partnership will reinforce both CPI's and PYMNTS' coverage of technology regulation, as jurisdictions worldwide tackle the regulation of digital businesses across the connected economy, including questions pertaining to BigTech, FinTech, crypto, healthcare, social media, AI, privacy, and more.

Our partnership is timely. The antitrust world is evolving, and new, specific rules are being developed to regulate the so-called "digital economy." A new wave of regulation will increasingly displace traditional antitrust laws insofar as they apply to certain classes of businesses, including payments, online commerce, and the management of social media and search.

This insight is reflected in the launch of the **TechREG** Chronicle, which brings all these aspects together — combining the strengths and expertise of both CPI and PYMNTS.

Continue reading CPI as we expand the scope of analysis and discussions beyond antitrust-related issues to include Tech Reg news and information, and we are excited for you, our readers, to join us on this journey.

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL