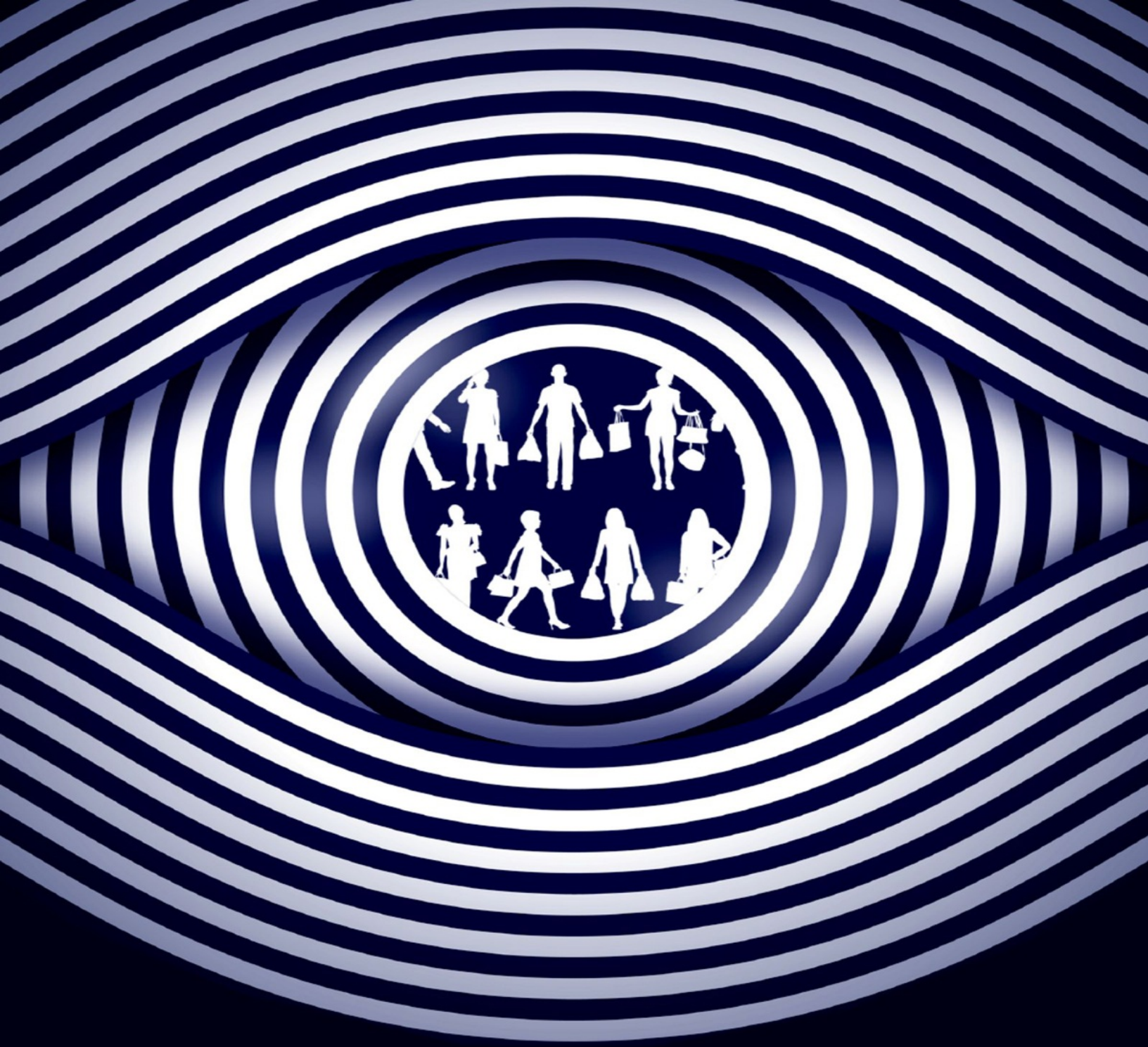

# Breaking Away

## How to Regain Control Over Our Data, Privacy, and Autonomy

Maurice E. Stucke

# Breaking Away

# Breaking Away

*How to Regain Control Over Our Data, Privacy, and Autonomy*

MAURICE E. STUCKE

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press is a department of the University of Oxford. It furthers the University's objective of excellence in research, scholarship, and education by publishing worldwide. Oxford is a registered trade mark of Oxford University Press in the UK and certain other countries.

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America.



Library of Congress Control Number: 2021033615

ISBN 978–0–19–761760–1 (hbk.)
ISBN 978–0–19–761761–8 (pbk.)
ISBN 978–0–19–761763–2 (epub.)

DOI: 10.1093/oso/9780197617601.001.0001

*To Amelia, Thomas, Clara & Walt*

# Table of Contents

# Preface

At the 2018 congressional hearing, Facebook's CEO was asked a simple yet revealing question:

> "Would you be comfortable sharing with us the name of the hotel you stayed in last night?"
>
> "Um," Mark Zuckerberg said before a long pause, "No."[1]

The point, of course, is that Facebook and a few other powerful platforms know a lot about us. Within a few minutes, Facebook's CEO could learn more about our personality, political attitudes, physical health, and any substance abuse, according to one study, than what our coworkers, friends, parents, or even spouses know.[2] But we know relatively little about what personal data Facebook collects, how it uses our data, and with whom it shares our data.

We are at the frontiers of the Panopticon, an architectural design conceived by the father of utilitarianism, Jeremy Bentham. Imagine a round tower lined with cells. In its center is the watchman. While the cells have transparent glass, the watchtower's glass is tinted so that a single guard can watch any factory workers or inmates without them knowing they are being monitored. Today, those guards are the data-opolies who track us across the web, collect data about us, profile us, and manipulate us—to hold our attention and induce us to buy things we otherwise wouldn't at the highest price we are willing to pay.

Is this simply paranoia? Consider a conversation Alastair Mactaggart had among friends at a social outing. The San Francisco real estate developer asked an engineer working for Google whether we should be worried about privacy. "Wasn't 'privacy' just a bunch of hype?," Mactaggart asked. The Google engineer's reply was chilling: "If people just understood how much we knew about them, they'd be really worried."

Enforcers, policymakers, scholars, and the public are increasingly concerned about Google, Apple, Facebook, and Amazon and their influence. That influence comes in part from personal data.[3] Google, Apple, Facebook, and Amazon are "data-opolies," in that they are powerful firms that control our data. The data comes from their vital ecosystems of interlocking online platforms and services, which attract users; sellers; advertisers; website publishers; and software, app,

and accessory developers.[4]

The public sentiment is that a few companies, in possessing so much data, possess too much power. Something is amiss. In a 2020 survey, most Americans were concerned

- about the amount of data online platforms store about them (85%); and
- that platforms were collecting and holding this data about consumers to build out more comprehensive consumer profiles (81%).[5]

But data is only part of the story. Data-opolies use the data to find better ways to addict us and predict and manipulate our behavior.

While much has been written about these four companies' power, less has been said about how to effectively rein them in. Cutting across political lines, many Americans (65%) think Big Tech's economic power is a problem facing the U.S. economy, and many (59%) support breaking up Big Tech.[6] Other jurisdictions, including Europe, call for regulating these gatekeepers.[7] Only a few argue that nothing should be done. In looking at the proposals to date, however, policymakers and scholars have not fully addressed three fundamental issues:

- *First*, will more competition necessarily promote our privacy and well-being?
- *Second*, who owns the personal data, and is that even the right question?
- *Third*, what are the policy implications if personal data is non-rivalrous?

As for the first question, the belief is that we just need more competition.[8] Although Google's and Facebook's business model differs from Amazon's, which differs from Apple's, these four companies have been accused of abusing their dominant position, using similar tactics, and all four derive substantial revenues from behavioral advertising either directly (or for Apple, indirectly).

So, the cure is more competition. But, as we'll see, more competition will not help when the competition itself is toxic. Here rivals compete to exploit us in discovering better ways to addict us, degrade our privacy, manipulate our behavior, and capture the surplus.

As for the second question, there has been a long debate about whether to frame privacy as a fundamental, inalienable right or in terms of market-based solutions (relying on property, contract, or licensing principles). Some argue for laws that provide us with an ownership interest in our personal data. Others

argue for ramping up California's privacy law, which the realtor Alastair Mactaggart spearheaded; or adopting regulations similar to Europe's General Data Protection Regulation.

This book seeks to reorient the debate from "Who Owns the Data" to "How Can We Better Control Our Data, Privacy, and Autonomy." As we'll see, easy labels do not provide ready answers. Providing individuals with an ownership interest in their data doesn't address the privacy and antitrust risks posed by the data-opolies; nor will it give individuals greater control over their data and autonomy. Even if we view privacy as a fundamental human right and rely on well-recognized data minimization principles, data-opolies will still game the system. To illustrate, we'll explore the significant shortcomings of the California Consumer Privacy Act of 2018 and Europe's GDPR in curbing the data-opolies' privacy and competition violations.

For the third question, policymakers currently propose a win-win situation—promote both privacy and competition. That is true when firms compete to protect privacy. But in crucial digital markets, privacy and competition conflict. Policymakers, as a result, can fall into several traps, such as when in doubt, opt for greater competition.

Thus, we are left with a market failure where the traditional policy responses—define ownership interests, lower transaction costs, and rely on competition—will not necessarily work. Instead, we need new tools to tackle the myriad risks posed by these data-opolies and the toxic competition engendered by behavioral advertising. We'll assess the strengths and weaknesses of a spectrum of policy options.

With so many issues competing for our attention, why should we care about data-opolies?

Power! As the data-opolies have refined their anticompetitive playbook and will eventually wield their prediction and manipulation tools to financial services, healthcare, insurance, and the metaverse, they'll have all the cards.

Next is blackmail. The game here isn't simply to provide us with relevant ads. Instead, as Facebook's patented "emotion detection" tools suggest, the aim is to detect and appeal to our fears and anger, to pinpoint our children and us when we feel "worthless," "insecure," "defeated," "anxious," "silly," "useless," "stupid," "overwhelmed," "stressed," and "a failure."[9] In changing our newsfeed with depressing or uplifting stories, Facebook, without our knowledge, has experimented in manipulating our moods and how we respond to others.[10] That

wasn't an isolated case. As the evidence reveals, we are the lab rats, as we enter a marketplace of behavioral discrimination: data-opolies already know our personality, whether we have internal/external locus of control, our willingness to pay, and our impulsivity. And we have little choice but to enter this ecosystem, which they have primarily designed and now control.

Third is the toll in addicting us and manipulating our behavior. It is simply too great to ignore. Congress, in an extensive market inquiry of the power of Google, Apple, Facebook, and Amazon, found "significant evidence that these firms wield their dominance in ways that erode entrepreneurship, degrade Americans' privacy online, and undermine the vibrancy of the free and diverse press."[11] The stakes, as FTC Commissioner Rohit Chopra noted in 2019, are huge:

> The case against Facebook is about more than just privacy—it is also about the power to control and manipulate. Global regulators and policymakers need to confront the dangers associated with mass surveillance and the resulting ability to control and influence us. The behavioral advertising business incentives of technology platforms spur practices that are dividing our society. The harm from this conduct is immeasurable, and regulators and policymakers must confront it.[12]

If we continue along the current course, the result is less privacy, less innovation, less autonomy, greater division and rancor, and a threatened democracy. In short, as an influential 2020 congressional report observed, "[o]ur economy and democracy are at stake."[13] We cannot afford remedies, which while well-intentioned, do not address the root of the problem. Nor can we ignore the looming privacy/competition clash, which some of the data-opolies are already exploiting.

The first two chapters set the stage by outlining how the data-opolies became so powerful and their anticompetitive playbook. Given the data-opolies' durable market power, Chapter 3 surveys the multiple proposals to rein them in. Improving privacy protection is a necessary, but not sufficient, step to address some of the risks these data-opolies pose and deter their data hoarding.

All the policy proposals assume that with more competition, our privacy and well-being will be restored. But that won't be the case in many online markets, as Chapter 4 explores.

The current remedies also do not address our next question: *Who owns the personal data?* The law in the United States and elsewhere currently is unclear on the users' ownership interest in their personal data. Chapter 5 explores

whether property law is the proper legal framework.

The United States, unlike Europe, does not have a baseline privacy framework. Instead, privacy protection in the United States is a patchwork of the FTC Act; common law torts; state laws; constitutional claims; and specific statutory protections, such as the Children's Online Privacy Protection Act of 1998.

A privacy baseline is much needed. Without such a framework, the federal and state agencies cannot curb the data-opolies' expropriation of our data. Without it, the race to addict us, manipulate us, and profit from behavioral advertising will continue.

After exploring multiple shortcomings of a market-based approach to privacy, we'll consider in Chapter 6 an alternative approach of viewing privacy and one's right in one's data as a fundamental, inalienable right. But that approach, as we'll see with Europe's and California's privacy laws, has its shortcomings.

The challenge then is to enact the privacy framework that attacks the source of the problem: the surveillance economy that a few powerful companies have designed for their benefit, at our expense. Suppose policymakers successfully implement these data minimization principles. The good news is that the privacy policies, in minimizing the collection and use of our data, would give us greater control over our privacy and loosen the data-opolies' powerful grip. But it brings us headlong into the book's third fundamental question: *What are the policy implications if data is non-rivalrous?*

Chapter 7 explores the upcoming clash between privacy and competition, which has been largely unexplored by policymakers and the literature to date. After flagging in Chapter 8 several traps that await policymakers in promoting both competition and privacy, we'll examine in Chapter 9 several solutions that can promote privacy, deter the toxic competition caused by behavioral advertising, and balance privacy and healthy competition when they conflict. After addressing in Chapter 10 the potential risks and criticisms in banning behavioral advertising and the surveillance apparatus, Chapter 11 concludes with signs of hope.

The aim is to promote an inclusive digital economy that advances our privacy, well-being, and democracy. When venturing online, engaging with our smart speakers, or checking our news feed, we should not have to play "multidimensional chess against massive artificial intelligence that have nearly perfect information about us" as a Facebook adviser and investor (and now critic) warned.[14] Our lives should not devolve to monetization opportunities.

So, if competition in the online world is supposed to be a click away, let's see how a few dominant firms re-engineered the keyboard.

---

1 Sarah Frier, Nico Grant, & Selina Wang, *Six Takeaways from Zuckerberg's Time in the Senate Spotlight*, Bloomberg (Apr. 11, 2018), https://www.bloomberg.com/news/articles/2018-04-11/six-takeaways-from-zuckerberg-s-time-in-the-senate-spotlight [https://perma.cc/63LG-HZNS].

2 Michal Kosinski, David Stillwell, & Thore Graepel, *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 Proc. Nat'l Acad. Sci. 5802 (2013), https://doi.org/10.1073/pnas.1218772110 [https://perma.cc/2LR4-4782].

3 Personal data, as used herein, means "any information relating to an identified or identifiable individual (data subject)." OECD, Directorate for Financial and Enterprise Affairs Competition Committee, *Consumer Data Rights and Competition —Background Note by the Secretariat*, at ¶ 16 (Apr. 29, 2020), https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf.

4 Democracy Under Threat: Risks And Solutions In the Era of Disinformation and Data Monopoly, Report of Canada's House of Commons, Standing Committee on Access to Information, Privacy and Ethics (Dec. 2018), https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/etee.pdf; Maurice E. Stucke, *Should We Be Concerned About Data-opolies?*, 2 Geo. L. Tech. Rev. 275 (2018); Maurice E. Stucke, *Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data*, Harv. Bus. Rev. (Mar. 2018), https://hbr.org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-data [https://perma.cc/88QR-DSXQ].

5 Press Release, Consumer Reports, Consumer Reports Survey Finds That Most Americans Support Government Regulation of Online Platforms (Sept. 24, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-that-most-americans-support-government-regulation-of-online-platforms/ [https://perma.cc/9D3J-G2LA].

6 Rani Molla, *Poll: Most Americans Want to Break Up Big Tech*, Vox (Jan. 26, 2021), https://www.vox.com/2021/1/26/22241053/antitrust-google-facebook-break-up-big-tech-monopoly.

7 *See, e.g.*, European Commission's proposed Digital Markets Act, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en; Consumer Reports Survey, *supra* note 5 (60% of those surveyed supported more government regulation of platforms to deal with their growing power that may be hurting competition and consumers).

8 Max Greenwood, *Majority Supports Antitrust Review of Tech Giants: Poll*, The Hill (Aug. 5, 2019), https://thehill.com/policy/technology/456221-majority-supports-antitrust-review-

of-tech-giants-poll [https://perma.cc/EF3Q-JT2D] (finding from 2019 Harvard CAPS/Harris Poll survey that more than two-thirds of U.S. voters believe that tech giants like Google and Facebook should be subject to federal antitrust review, 68% said that internet giants have largely built products and offered services to maximize their profits and accumulate market power, and 67% believe that the tech giants have taken steps to reduce competition in the market).

9 Sam Machkovech, *Report: Facebook Helped Advertisers Target Teens Who Feel "Worthless,"* Ars Technica (May 1, 2017), https://arstechnica.com/?post_type=post&p=1087191 [https://perma.cc/DE6V-M6Q5], Nick Whigham, *Leaked Document Reveals Facebook Conducted Research to Target Emotionally Vulnerable and Insecure Youth*, News.com.au (May 1, 2017), http://www.news.com.au/technology/online/social/leaked-document-reveals-facebook-conducted-research-to-target-emotionally-vulnerable-and-insecure-youth/news-story/d256f850be6b1c8a21aec6e32dae16fd [https://perma.cc/B4WS-NUB6]; Shoshana Zuboff, The Age of Surveillance Capitalism 287 (2019).

10 Adam D.I. Kramer et al., *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 Proc. Nat'l Acad. Sci. 8788 (2014), https://doi.org/10.1073/pnas.1320040111. In that study, Facebook experimented on 689,003 users to see whether their "emotional states can be transferred to others via emotional contagion, leading people to experience the same emotions without their awareness." By manipulating its News Feed algorithm, Facebook could lead people "to experience the same emotions without their awareness." For one large group of users, Facebook reduced positive emotional content in their News Feed, and they in turn "produced fewer positive posts and more negative posts; when negative expressions were reduced, the opposite pattern occurred." As one can imagine, the study drew sharp criticism. *See, e.g.*, Evan Selinger & Woodrow Hartzog, *Facebook's Emotional Contagion Study and the Ethical Problem of Co-opted Identity in Mediated Environments Where Users Lack Control*, 12 Res. Ethics 35 (2016), (arguing that the emotion contagion study exploited users' inability to determine how information is presented to others in the technologically mediated environment that Facebook constructs and demonstrates the limits of relying on control as a central virtue of information ethics).

11 Majority Staff of H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial and Administrative Law, Report and Recommendations: Investigation of Competition in Digital Markets (2020), https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf, 7 [hereinafter House Report].

12 Dissenting Statement of Commissioner Rohit Chopra, *In re* Facebook, Inc., Commission File No. 1823109, July 24, 2019, https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_st24-19.pdf.

13 House Report at 7.

14 Roger McNamee, Zucked: Waking Up to the Facebook Catastrophe 84 (2019).

# Acknowledgments

This book was published with the help of many.

First, I am grateful to the many scholars, competition and privacy officials, policymakers, lawyers, and business leaders who took the time to discuss these ideas and help develop them. I am also indebted to my Antitrust and Privacy seminar students for their insights and stimulating class discussions.

I was fortunate to present parts of this book in various venues and universities, and benefit from the panelists' and audience's feedback and curiosity, including the University of California Berkeley's Center for Long-Term Cybersecurity Research seminar on "Data Rights, Shared Value, and Re-defining 'Privacy' and 'Security' with AI/ML and Emerging Technologies"; the University of North Carolina Hussman School of Media and Journalism's seminar "Thwarting the Growth of News Deserts: Strengthening Local News and Democracy"; the University of North Carolina's First Amendment Law Review & UNC Center for Media Law & Policy's symposium, "The First Amendment and an Informed Society"; the World Bank's "Law, Justice and Development Week 2019"; the Australian Competition and Consumer Commission & University of South Australia's "17th Annual Competition Law and Economics Workshop"; Germany's Bundeskartellamt's "19th International Conference on Competition"; The Institute for New Economic Thinking's "Too Deep to Fail: Big Tech and Civil Society"; and the Georgetown Tech Law and Policy Colloquium.

For their help, support, and feedback at various stages of this project, special thanks are due to Ann Cleaveland, Ariel Ezrachi, Chris Hoofnagle, Barry Lynn, Pia Malaney, Dina Srinivasan, and Steven Weber.

Bringing this book to print was a team effort. I am very much indebted to Sibyl Marshall for her tireless and selfless effort in proofreading and editing the book's footnotes. I am appreciative to Alex Flach, Imogen Hill, and Charlotte Holloway at Oxford University Press for shepherding the book's production.

I would like to thank the Institute for New Economic Thinking, the University of California Berkeley's Center for Long-Term Cybersecurity Research, and the University of Tennessee College of Law for their generous research grants.

Finally, I thank my family for all of their support—both before, during, and

after completing this book, and coming up with the book’s title and the term data-opolies.

# 1
# The Rise of the Data-opolies

Most U.S. companies live short lives. Half of all publicly traded U.S. companies that began trading in any given year have disappeared in 10.5 years.[1] For companies that were created and died between 1950 and 2009, most died after their initial public offering, and fewer than 5% remained alive after 30 years.[2]

Companies that control platforms are not immune from failure. One study calculated that 209 platforms had failed and died over the past 20 years. Most of them (85%) were transaction platforms, which had shorter lives (on average 4.6 years) than the innovation platforms (5 years) or hybrid platforms (7.4 years).[3]

So, if many companies and platforms die within 10 years of their birth, why have Google, Apple, Facebook, and Amazon successfully dominated multiple markets for years and seem poised to continue their domination over the next decade? After canvasing the many markets that these data-opolies have dominated, we will explore four features of the digital economy that lead these markets to tip to monopolies or duopolies. The price we pay includes our privacy, attention, and autonomy.

## A. GAFA

What is remarkable about the data-opolies is how they have come to dominate numerous markets. Alphabet (which, for our purposes, we will call Google) has dominated over the past decade general search and general search advertising in the United States, Europe, and elsewhere.[4] Google has leveraged its search monopoly to dominate other markets, including web browsers (Chrome),[5] mobile operating systems (Android),[6] web-mapping (Google Maps and Waze[7]), and YouTube, the leading user-generated entertainment and video content platform.

By 2020, nine of Google's products—Android, Chrome, Gmail, Google Search, Google Drive, Google Maps, Google Photos, Google Play Store, and YouTube—had over a billion users each.[8] Google Pay, by 2018, was the most downloaded financial technology app worldwide, with millions of consumers spending and transferring "tens of billions of dollars."[9] Google Home and Assistant products, by 2019, were the market leaders in that category on a global

basis.[10]

When it comes to social networking, Facebook dominates. Facebook, Instagram, Messenger, and WhatsApp collectively have significantly more users than its closest competitors, Twitter (582 million users) or Snapchat (443 million users), combined.[11] As we shall also explore, Facebook and Google dominate online advertising. Facebook is "the third-most visited website outranked only by Google and YouTube."[12] Of the top 10 most popular free apps in Apple's app store in 2019, Facebook and Google each had three apps, and Amazon had one.[13]

Amazon controls the dominant e-commerce platform,[14] accounting by 2018 for nearly half of the then-$252.7 billion U.S. e-commerce market—which was more than double the share of the next nine companies (eBay, Apple, Walmart, Home Depot, Best Buy, Qurate Retail Group, Macy's, Costco, and Wayfair) combined.[15] At the onset of the COVID-19 pandemic, Amazon's sales increased 26% to over $75 billion in the first quarter of 2020.[16] That is over $25 billion in sales per month, $833 million in sales per day, or over half a million dollars in the minute you spent reading this paragraph.

Amazon is leveraging its power to other markets, like the parcel delivery business, where it has already surpassed the U.S. Post Office in terms of parcels delivered; it is projected to overtake Federal Express and UPS by 2022.[17] Also, Amazon Web Services ("AWS") is the largest provider of cloud computing services, accounting by 2020 for nearly half of all global spending on cloud infrastructure services, with "three times the market share of Microsoft, its closest competitor."[18] The U.S. cloud computing business is consolidating around three companies: Amazon, Google, and Microsoft.[19]

Apple, as of January 2021, had the largest market capitalization of any company in the world.[20] Since mid-2012, Apple has controlled over half of the mobile operating systems in the United States, with Google's Android controlling nearly the rest.[21]

How did these data-opolies become so powerful? Among the many well-accepted factors,[22] we will examine four: economies of scale, network effects, attention, and the four Vs of personal data (volume, variety, velocity in processing, and value).

## B. The Importance of Scale

Economies of scale arise where average costs per unit decrease with an increase

in production or output.[23] Economies of scale exist in the brick-and-mortar economy, such as newspapers, automobiles, and military airborne radios.[24] But, as an expert report for the EU noted, "the digital world pushes this phenomenon to the extreme."[25]

For example, a search engine—whether Google's or Bing's—has to crawl and index the web, a significant upfront cost for any entrant (in the billions of dollars) and high annual cost for the current search engines (estimated at hundreds of millions of dollars annually).[26] So, whether the search engine handles over 90% of the searches or only 1%, it must incur this significant cost, assuming that many websites will consent to be crawled by a search engine other than Google (and perhaps Bing).[27] This annual expense of hundreds of millions of dollars does not increase proportionately with the number of users.[28] But the larger search engine in achieving scale for both search queries and search advertising can better cover these high expenses than smaller search engines. Economies of scale can help the big get bigger, while the smaller firms weaken.[29]

One hears that just as Google displaced Yahoo and Facebook displaced Myspace, so too an entrant can replace these monopolies. But given the scale at which Google, Apple, Facebook, and Amazon currently operate, displacing them will be a lot harder than it was when these companies displaced earlier rivals.[30] As one expert report found:

> The level of dominance achieved by the early leaders in markets such as social networks and online search is not comparable to the scale and reach that has been achieved by Facebook and Google. For example, the number of monthly unique global visitors to Myspace peaked at around 100 million, and it was valued at $580 million when it was purchased by News Corporation in 2005. In comparison, Facebook reportedly has over two billion monthly active users, with over 40 million in the U.K. alone, and was valued at more than $470 billion in February 2019. It is possible that companies such as Myspace never achieved the critical mass necessary to secure the market.[31]

Consequently, as Facebook internally recognizes, once a data-opoly has reached this scale, it is harder for an entrant, even one with better features, to win over many users.[32]

## C. Network Effects

One of Facebook's early investors and advisers (and still a significant shareholder), Roger McNamee, summarized the history of Silicon Valley in two

laws:

- *Moore's Law* (which deals with the number of transistors on a microchip doubling every two years, thereby increasing computer speed and capability); and
- *Metcalfe's Law* (where a network's value is the square of the number of nodes in the network).[33]

McNamee's point is that bigger networks, say with 1,000 people (whose value under Metcalfe's Law is 1,000,000) are generally more valuable than smaller ones, say with 10 people (whose value under Metcalfe's Law is 100).[34]

Network effects occur when a product's or service's value increases as others use it.[35] Although network effects exist in the brick-and-mortar economy, the digital platform economy has multiple network effects, all of which contribute to a powerful feedback loop that attracts users, sellers, app developers, and advertisers to the leading platforms.[36]

Strong network effects are a significant barrier to entry in many digital platform markets.[37] In 2012, Facebook internally described its network effects as a "flywheel, which get 'stronger every day.' "[38] As another internal Facebook report notes: "a serious concern is network effects: when you use an app less, that makes it less appealing to other people, and at certain times and places those effects could be very large."[39] So, as the internal report notes, while "mobile phone users tend to use five different social maps in a month, they only use '1.5 messaging apps and 1 social app, out of 10 total apps per day.' "[40]

Figure 1.1 identifies five important network effects in the digital economy.

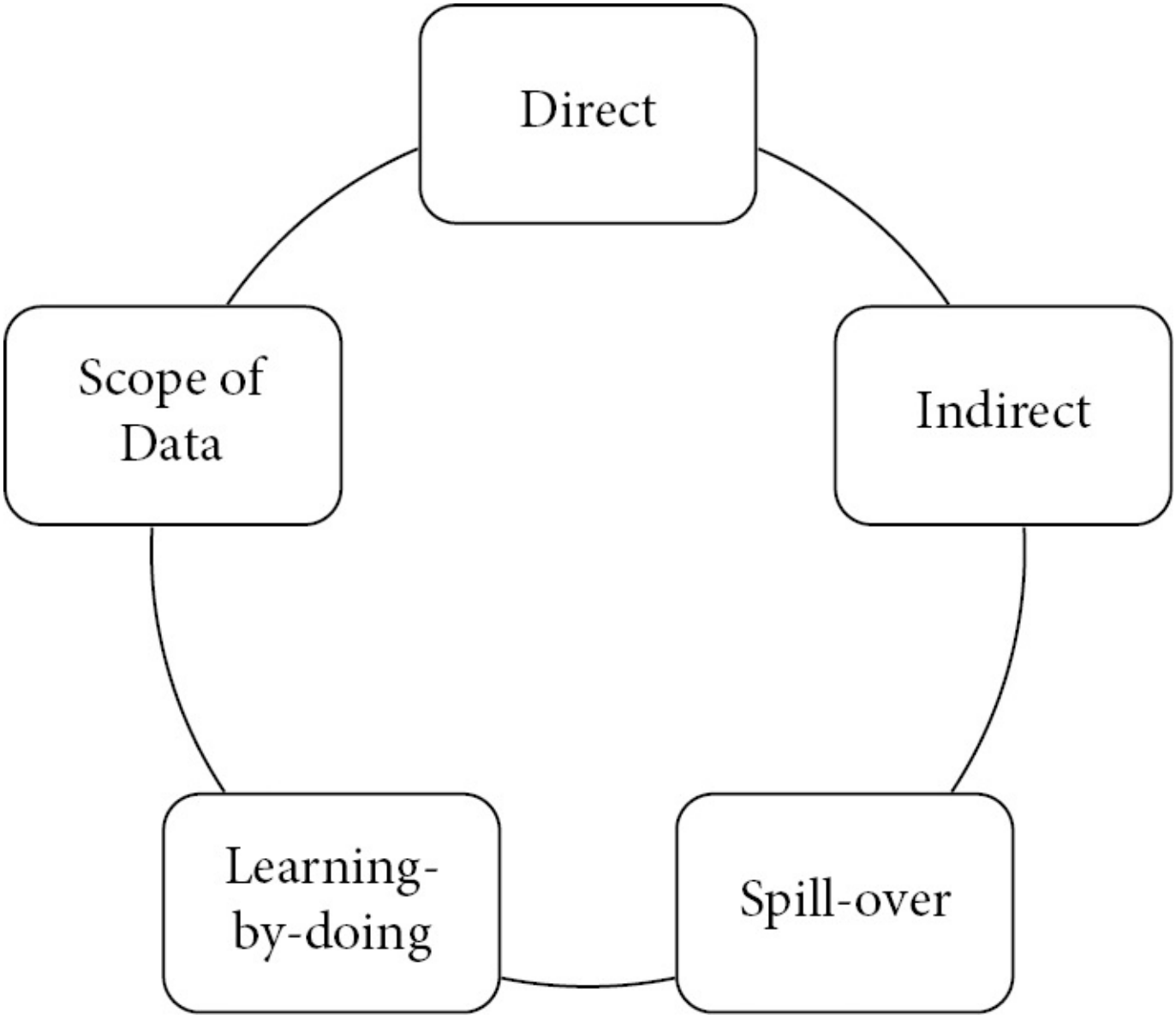


**Figure 1.1** Identifies at least five network effects in the digital platform economy

We see *direct network effects* in today's social networks, like Facebook, and texting apps, like Facebook Messenger and WhatsApp. As more people join the platform, the more people with whom one can share information, follow, and communicate, the more popular the leading platform becomes in attracting others.[41] So here again, even if an alternative social network emerges with better features and more robust privacy protections, it will likely fail against a dominant social network unless many people switch en masse.[42]

*Indirect network effects*, as the U.S. Supreme Court discussed, "exist where the value of the platform to one group depends on how many members of another group participate."[43] A classic example is Microsoft's operating system for personal computers.[44] As more people used Microsoft Windows, the more

attractive the operating system became to software providers to write programs compatible with Windows, which attracted more customers to Windows, and contributed to Microsoft dominating the PC operating system market for decades.[45] One sees similar indirect network effects for cloud computing,[46] browsers,[47] operating systems for mobile phones (Google's Android and Apple's iOS),[48] and digital personal assistants (like Google Home and Amazon Alexa).

If you want a digital personal assistant, you would like one that offers a greater choice of applications and skills and connects with more smart appliances in your home. App developers and smart appliance manufacturers prefer designing their products to be compatible with platforms with larger audiences. So, as one or two platforms attract more users, they, in turn, will attract more developers and manufacturers, which, in turn, will attract more users, propelling the feedback loop. Once many users switch to the leading platforms, it is harder for smaller platforms to attract and maintain users and developers.

*Spillover effects* emerge where more consumers on one side of the platform attract more content providers, sellers, or advertisers, on the other side of the platform, which can, in turn, attract more consumers.[49] With personal data, the spillover network effects are amplified. The more personal data the platform collects, the better the platform can refine its algorithms on what content—whether recommended videos, articles, products, or services—to attract (and addict) users and what behavioral ads to target them; as the algorithms improve in predicting and manipulating behavior, the platform becomes even more attractive to advertisers and sellers.[50]

Also, as more people use the platform's service (whether a search engine, map, or social network), businesses have a greater incentive to optimize their products for that service (such as ensuring that the information about them on Google Maps is accurate[51]). In effect, this amounts to "free" crowdsourcing improvements by businesses whose livelihood depends on being discovered by the people using that service.[52] A pizza shop in Rego Park, Queens, for example, has an incentive to ensure that the leading mapping app correctly identifies its store location. Otherwise, if Google Maps positions the pizza shop in Brooklyn Heights, the pizza shop cannot quickly deliver to the Brooklyn residents and will not get as much business from Queens customers.[53] Plus, if one's business is not on Google Maps or Google Search, it does not exist for many potential customers.[54]

The*learning-by-doing* network effect concerns how the increase in data can

help train and improve the algorithm (such as improving its ability to recognize speech or voice patterns), thereby attracting additional users.[55] This network effect includes measuring the impact of minor design changes on our behavior[56] and advertising.[57]

To see how this data-driven network effect can make the leading firm even stronger, consider search engines.[58] Does your utility from using a particular search engine increase when others also use it? It does.[59] As more people use the same search engine, the algorithm has more opportunities to learn, as "[t]he greater the number of queries a general search service receives, the quicker it is able to detect a change in user behaviour patterns and update and improve its relevance."[60] Its more relevant search results will attract others to the search engine, and the positive feedback continues.[61]

This network effect is less pronounced for objective queries (such as what is the capital of Hungary), to which DuckDuckGo or Bing can respond. Rather, this network effect favors the dominant search engine on less common (or tail) inquiries.[62] About 15 to 20% of queries that search engines typically see daily are common (what search engines call "head" queries), and about 25 to 30% of the queries are uncommon ("tail") queries.[63] As we judge a search engine's performance both on the common and uncommon queries, the more data a general search engine collects for rare tail queries, "the more users will perceive it as providing them the more relevant results for all types of queries."[64] With more users and more tail queries, the dominant search engine benefits from seeing what links its users click for these tail inquiries.[65] Plus, with other personal data on the users, including their location, the algorithm can further improve the search results. Thus, as the U.K. competition authority found, the smaller search engines' "lack of comparable scale in click-and-query data is likely to be a key factor that limits [their] ability . . . to compete with Google."[66]

*Scope of data* network effects concern how the range of personal data collected about us helps the platform personalize ads and services (and anticipate, predict, and manipulate our behavior). To better predict and influence our behavior, algorithms require a significant *variety* of personal data.[67] For example, the more you use a digital assistant like Amazon's Alexa, the more personal data it collects, the more opportunities Alexa can anticipate your different needs, including products you might want to buy.[68]

Ordinarily, these network effects should benefit us as, definitionally, our utility should increase when others join the platform. But network effects,

besides increasing entry barriers, can harm us, including, as FTC Commissioner Rohit Chopra noted, in fostering our addiction to the platform:

> As with other artificial intelligence, the recommendation engine is more effective at hooking viewers into watching more videos the more its user surveillance trains its recommendation engine to pick videos that keep the viewer engaged. The unlawful collection of data on children allowed Google's YouTube recommendation engine to glean deep insights on children's viewing habits. This further solidifies YouTube's dominance among children, which in turn, makes creators of child-directed content more reliant on YouTube for distribution.[69]

Try searching for "Greatest Conservatives" on YouTube; a few videos later, Google might be showing you Dr. Phil episodes like "Couple Gets Physical During Arguments." As a former Google engineer in charge of tweaking this algorithm discussed, the content to keep our children and us addicted can quickly devolve to conspiracy theories and other disturbing content.[70]

Data-opolies, as we will see, can create—or harness—these network effects for their advantage and to lock us in.[71]

## D. Importance of Attention and Personal Data

Advertising in the digital economy is driven primarily by competition for our attention and data, both of which data-opolies have a significant advantage over rivals.[72] Our personal data is used to train algorithms to find ways to attract and maintain our attention. Once they sustain our attention, the data-opolies have more opportunities to predict and manipulate our behavior and to target us with ads. These experiments (such as seeing what ads we click or videos we watch) yield even more data about us.[73] This data-rich accumulation is self-reinforcing: "Companies with superior access to data can use that data to better target users or improve product quality, drawing more users and, in turn, generating more data —an advantageous feedback loop."[74] This feedback loop reinforces the data-opoly's power – with more users, the data-opoly can access and collect more personal data than its rivals. The data-opoly uses the data, for among other things, "a more targeted user experience, which in turn attracts more users and leads those users to spend more time on the platform."[75]

By capturing more of our attention, data-opolies make it harder for rivals to access our data, target us with behavioral ads, or otherwise manipulate our behavior. It becomes harder for others to enter, as "a new entrant would need to

compete on many fronts to displace" the data-opoly, thereby further insulating it from competitive pressure.[76]

We know the data-opolies collect a lot of personal data, but let us see how much.

## 1. Google

In 2010, Google's then-CEO Eric Schmidt said, "We know where you are. We know where you've been. We can more or less know what you have been thinking about."[77] Boasting? Hardly. Google harvests data from

- its 50+ services for users, nine of which—Android, Chrome, Gmail, Google Search, Google Drive, Google Maps, Google Photos, Google Play Store, and YouTube—have over a billion users each;[78]
- third-parties (including the analytical technology Google places on millions of third-party websites and apps);
- our homes and smart appliances (through its digital assistant Google Home and Google Nest security cameras, doorbells, and smart thermostats);
- its cloud computing service Google Cloud; and
- Verily (which is developing tools to collect and organize our health data).[79]

But even if you went offline, Google can still access your data. As *The Wall Street Journal* found, Google has struck partnerships with some of the country's larger hospital systems and renowned healthcare providers. "In just a few years," Google "has achieved the ability to view or analyze tens of millions of patient health records in at least three-quarters of U.S. states."[80]

In acquiring Fitbit, a leading platform for wearables, Google will obtain even more sensitive health and personal data, which outside of Europe, it can use "to design new software, underpinned by advanced artificial intelligence and machine learning, that zeroes in on individual patients to suggest changes to their care."[81]

Google is also forging alliances with Ford, General Motors, Volvo, and Renault-Nissan-Mitsubishi for a competitive- and data advantage in driverless cars.[82]

Google also accesses data from millions of Mastercard users, which,

according to news reports, helps Google track retail sales and "link ads people have seen to purchases they've made in the real world."[83]

As the Colorado-led states alleged in their 2020 monopolization complaint, "Put simply, Google may have more data about more people than any other entity in the history of the world."[84]

## 2. Facebook

When other data-opolies are alleged to use Facebook to spy on their employees, you know the company collects a lot of data.[85] As Facebook's market power grew, so too did its surveillance and extraction of rich data. Our "personal connections, activities, identity, demographics, interests, and hobbies" are just some of the data Facebook collects.[86] Facebook accesses our data whenever we visit its various owned and operated sites—including its virtual reality gaming platform Oculus—and whenever we visit the mobile apps within the Facebook Audience Network.[87] That alone catches over three billion people each month.[88]

Even seemingly benign bits of information—such as what we "Like" on Facebook—can tell Facebook and advertisers a lot about us. Using one's Likes, computer scientists at one university, with their algorithm, could estimate a Facebook user's sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender.[89]

But even if we could avoid Facebook and its advertising network, Facebook still tracks us whenever we visit the millions of websites and apps with a Facebook "Like" button or that use "Facebook Analytics" services.[90] Data is transmitted to Facebook when we visit that third-party website or app, even before we see the "Like" button.[91] For example, one 2018 study found that at least 61% of the 34 apps it tested, which included language-learning tool Duolingo, travel, and restaurant website TripAdvisor, and flight search engine Skyscanner, automatically transferred data to Facebook the moment a user opened the app.[92] "This happens whether people have a Facebook account or not, or whether they are logged into Facebook or not," the report said.

The amount of data Facebook receives is staggering. Facebook received approximately one billion events per day from health apps alone on users, such as when someone opened the app, clicked, swiped, or viewed certain pages, and placed items into a checkout.[93] With all that data, Facebook compiles some 200 "traits" attached to its 2.8 billion users' profiles. These traits "include various

dimensions submitted by users or estimated by machine-learning models, such as race, political and religious leanings, socioeconomic class, and level of education."[94]

A 2019 study found many popular apps deliver even more sensitive health and financial information to Facebook, without affording users any way to stop this.[95] So, if you are among the 25 million active users of the Flo Period & Ovulation Tracker, then Facebook (and its advertisers) would likely know when you are menstruating or wanting to get pregnant.[96]

## 3. Amazon

We think of Amazon.com as the dominant online shopping platform, which it is. But as a former Amazon employee noted, "Amazon is first and foremost a data company, they just happen to use it to sell stuff."[97] As the Congressional Antitrust Report notes,

> Amazon's expansion into a diverse array of business lines—from brick-and-mortar supermarkets to home security—has reinforced its significant stockpile of consumer data. With more data about online and offline consumer behavior, Amazon's acquisitions set in motion a self-reinforcing cycle, creating an ever-widening gap between the platform and its competitors.[98]

To develop "a highly targeted marketing plan for each customer," Amazon closely tracks what we search, what we buy and choose not to buy, and how we spend our time on its shopping platform.[99] It collects data about the movies we watch and songs we listen to on Amazon Prime, and what we purchase at its Whole Foods grocery stores.[100] Amazon, which accounts for over half of all print book sales and over 80% of e-book sales in the United States,[101] tracks what books you buy. If you are reading this book on Kindle, Amazon is tracking what words you are highlighting.[102] Why? Amazon uses the data "for predicting the products you are likely to purchase, when you may buy them, and where you might need the products."[103]

As more people bring Amazon's smart speakers into their homes, the digital assistant—in controlling already over 85,000 smart home products (from televisions to doorbells to earbuds) and in executing over 100,000 "skills"—collects even more personal data.[104] As of late 2019, Amazon was processing "billions of interactions a week, generating huge quantities of data about your schedule, your preferences, and your whereabouts."[105] In turning its Alexa into

“an omnipresent companion that actively shapes and orchestrates your life,” Amazon will need to “know you better than ever before.”[106] Thus, Alexa is expanding onto our bodies with wireless earbuds, smart rings, and smart glasses.[107] Amazon’s vision “effectively assumes Alexa will follow you everywhere, know a fair bit about what you’re up to at any given moment, and be the primary interface for how you coordinate your life.”[108]

“No cable or satellite? No problem.”[109] That’s how Amazon touts its Amazon Fire TV devices, which allow you to watch live TV and sports, and access millions of songs. Since you must pay for subscriptions to access many popular TV stations, you might think your privacy is secure. But Amazon, Google, and Facebook are tracking what you are watching. One study detected Amazon trackers on 687 of the top 1,000 television channels on Amazon Fire TV, followed by multiple Google trackers (each covering hundreds of channels) and Facebook trackers on 196 television channels.[110]

You may be among the millions of purchasers of Amazon Ring internet-connected doorbells, which enable you to surveil who is coming to your house and share the videos with over 400 police departments.[111] But you did not think that Amazon secretly was surveilling you and allowing Google and Facebook to track you. But the Ring doorbell app, as the Electronic Frontier Foundation found, was sending sensitive personal information to the other two data-opolies.[112]

In 2020, Amazon announced an “autonomously flying” surveillance drone for our homes.[113] As its drone could not yet navigate stairs, Amazon recommended buying a surveillance drone for each floor.[114] So, when you are spending the night at a friend’s house, that sound approaching the bedroom may be none other than the $249 Ring Always Home Cam. And as Amazon promises, like “all Ring Video Doorbells and Cams, you will be able to live stream video at no cost.”[115]

But even if you fastidiously avoid Amazon’s supermarket, shopping platform, Alexa devices, and other products, and even if you could avoid the neighborhoods with Ring surveillance cameras, the data-opoly can still obtain information about you. Amazon might capture your data indirectly whenever millions of companies use Amazon’s AWS cloud services, including Airbnb, Baidu, Capital One, Comcast, Disney, Dow Jones, ESPN, Expedia, Financial Times, Guardian News & Media, Hitachi, ITV, Johnson & Johnson, Lyft, McDonalds, Netflix, Pinterest, Scribd, Slack, Sony, Spotify, Turner Broadcasting, Ticketmaster, Unilever, Vodafone Italy, WIX, Yelp, and Zillow.[116]

One congressional concern is that, despite Amazon's promises of secrecy, Amazon is "positioned to use customer and seller data from one line of business to inform decisions in other lines of business, analogous to its conduct in Amazon Retail."[117]

Even if Amazon's cloud service is not furtively tapping into its clients' data, another concern is that Amazon is helping other companies stalk you. As one report observed, "[c]ompanies may benefit from AWS by using them to analyze customer demographics, spending habits, and other pertinent information to more effectively cross-sell company products in ways similar to Amazon. In other words, these retailers can use Amazon to stalk you, as well."[118]

## 4. Apple

As the thinking goes, Apple collects less personal data on us, as it makes most of its money from its products and services rather than behavioral advertising.[119] Unlike Google and Facebook, Apple does not track its customers over time and across third-party websites to provide behavioral advertising.[120] Moreover, Apple's recent iOS 14 policy requires apps like Facebook's to get Apple users' permission to track them, prompting a public feud between the two data-opolies.[121]

Facebook claims that Apple's no-tracking policy change is "about profit, not privacy."[122] One reason is that Apple is not playing by its rules.[123] We will explore that emerging "profits, not privacy" concern later. For our purposes now, Apple's advertising business is growing fast. Apple, for example, charges app developers to advertise in its App Store, where Apple then takes a hefty share of any in-app subscription revenue.

Apple, according to its Privacy Statement, also collects and uses "personal information to help [it] create, develop, operate, deliver, and improve [its] products, services, content, and advertising."[124] If you use Apple products and services, then you are segmented into groups of 5,000 or more other people who Apple determines share similar characteristics and are served with "relevant ads." To segment you, Apple uses your data, including the topics and categories of stories that you read and publications you follow, all the music, movies, books, TV shows, and apps you download, your account information (including your address, age, and every device registered to your Apple ID account), in-app purchases, activities in other apps, your searches and purchases in the Apple Store, and your interactions with the ads targeted at you.[125]

Moreover, Apple relies on personal data and attention for a competitive advantage.[126] People spend a lot of time within Apple's ecosystem. In the United States, according to a 2017 survey, 79% used an Apple device daily, and 10% used it several times a week.[127] Apple uses "information about your purchases, downloads, and other activities in the Stores to tailor features and offer personalized recommendations for you."[128] Apple collects data on how consumers interact with its websites and apps, including all the movies and music one downloads off iTunes,[129] to determine what pages or features are popular and where its products and services could be improved. As Apple's revenues shift from hardware to services, which include advertising, its incentives to monetize our data and attention will increase.[130]

But even if Apple's profiling and surveillance are not as invasive as Facebook's and Google's, Apple, as we will soon see, significantly profits in enabling some of the biggest privacy offenders to harvest our data and manipulate our behavior.

## E. Winner-Take-All-or-Most Markets

Because of these economies of scale and data-driven feedback loops, digital platform markets can tip in one or two companies' favor, making it hard to dislodge them.[131] The mobile operating system market, for example, went from multiple competitors in 2010 (with Google and Apple collectively accounting for 39% of unit sales) to a duopoly eight years later.[132] With 3.1 million Android apps in the Google Play store and 2.1 million apps in Apple's App Store in 2020,[133] it would be difficult for a new mobile phone operating system to overcome these network effects, even if it offers better features.[134] As the influential 2019 U.K. Expert Report concluded, "it is clear there is little incentive for app developers to go to the trouble and expense of ensuring their apps work on any smaller rival operating systems, as the potential target market will be so small."[135]

Likewise, in 2008, two years after its launch, Facebook had already eclipsed Myspace in the number of active users.[136] As the States allege in their antitrust complaint, Facebook aimed to tip every other geographic market to its favor:

> In October 2008, responding to a request from Facebook Chief Operating Officer Sheryl Sandberg to top Facebook executives, the Vice President of Partnerships wrote that one of his goals was to "try to tip every single major market where [Facebook] hasn't yet tipped. . . ." He listed nine countries or regions of the world that fell into that category. The United States was conspicuously absent because Facebook was well aware of its growing power in the United States.[137]

Consequently, once these digital platform markets tip in one or two companies' favor, their market power is quite durable,[138] and the likelihood of an entrant displacing them soon is "low."[139]

## F. Monetizing the Data and Attention into Prediction and Manipulation Machines

So, data-opolies have durable monopoly power to extract a lot of data about us, which they can use for behavioral advertising. As FTC Commissioner Rohit Chopra said, "Behavioral advertising, unlike contextual advertising, is about targeting each individual—a demographic of one."[140]
We will explore in Chapter 4 Facebook's and Google's dominance in behavioral advertising. For now, it is important to note that behavioral advertising is not limited to targeting us with relevant ads. As Harvard Business School Professor Shoshana Zuboff notes, "We are the source of the coveted commodity; our experience is the target of extraction."[141] The ultimate goal, as Zuboff observes, is perfecting the data-opoly's "ability to influence actual behavior as it occurs in the real spaces of everyday life."[142]

Instead of selling our data, data-opolies, as attention brokers, sell our attention —"specific, tailored tranches of attention designed to meet the needs of the buyer"[143]—and the ability to predict and modify our behavior.[144]

As Silicon Valley investor Roger McNamee observed, "Surveillance, the sharing of user data, and behavioral modification are the foundation of Facebook's success. Users are the fuel for Facebook's growth and, in some cases, the victims of it."[145] As he describes it, Facebook's algorithms start by giving us what we want, but "the algorithms are trained to nudge user attention in directions that Facebook wants."[146] So, Facebook's success is not the data per se, but "stems from its mastery of surveillance and behavioral modification."[147]

Data-opolies can use your data to train their algorithms and design their services and products to keep you longer within their expanding walled

ecosystems, to motivate you to vote for one candidate or another (or not to vote),[148] to predict which ads you are more likely to click and if you are "at-risk" of shifting your brand allegiance,[149] and to "even put you on a path you did not choose."[150]

Personal data and surveillance are also key for attribution, which involves tracking what we do after seeing the behavioral ad.[151] Attribution "requires complex analysis combining different sources of user data," such as following us when we switch from our laptop to our smartphone or when we visit the retailer.[152] Here, Google's and Facebook's surveillance and data advantage give them a significant competitive advantage in assessing the ad's performance and attributing the consumer's purchase to specific ads within their advertising network.[153]

## G. Apple and Privacy

So, who is worse: The manipulator or the person who aids and abets the manipulator? Consider this question when we turn to Apple, which appears to be fighting for its users' privacy.

Apple's CEO testified before Congress in 2020 that privacy is a foundational principle that touches everything Apple does: "We build products that, from the ground up, help users protect their fundamental right to the privacy of their personal data."[154]

If that is true, why would Apple make Google the default search engine on all Apple devices, including its personal assistant Siri, for the past 15 years?[155] It is not because Google is the most privacy-sensitive search engine. If Apple wanted to protect us from surveillance, it could have chosen DuckDuckGo. Instead, to secure these defaults, Google pays Apple on a "revenue share basis."[156] It is worse than Apple receiving a fixed sum because the revenue sharing agreement aligns Apple's and Google's incentives.[157] Under this arrangement, if you search for something on your Safari browser, you probably use Google's search engine. And Apple gets a significant percentage of Google's monopoly revenues from search advertising.[158] So the more people use Siri, Spotlight, or Google on their 1.4 billion Apple devices worldwide,[159] the more personal data that Google collects, the more advertising revenue that this data helps generates, and the more money Apple receives as a result. And the monopoly profits are in the billions. In 2019 Google reportedly paid Apple $12 billion to be the default

search engine on Safari,[160] which is significant by itself and relative to Apple's 2019 net income of $55.256 billion.[161] By 2021, the amount Google paid Apple climbed to an estimated $15 billion.[162]

The competition authorities have challenged the legality of Google's payments to secure these default positions. In response, a Google official said, "Apple features Google Search in its Safari browser because they say Google is 'the best.' "[163] If that were true, why would Google pay Apple over $41 million a day for something it could get for free on the merits? Google knows that most of us stick with the default option.[164]

So while Apple wants to appear as the champion of our privacy, it profits significantly from Google's behavioral advertising—approximately 15% to 20% of Apple's worldwide net income comes from Google.[165] After Apple's and Google's CEOs met in 2018 to discuss how the companies could work together to drive search revenue growth, a senior Apple employee wrote to a Google counterpart: "Our vision is that we work as if we are one company."[166]

Apple also profits in other ways from the surveillance economy. When apps use our data to induce us to spend more time playing games and spend money on add-ons and upgrades, Apple again profits. It generally collects 30% of these in-app purchases.[167] In the first half of 2020 alone, Apple users spent $32.8 billion (about $100 per person in the United States) on in-app purchases and games.[168] From its monopolistic tax on app developers, Apple's App Store was projected to collect $17.4 billion in net revenues for its fiscal year 2020.[169] This amount includes an estimated $360 million from Epic Games' app Fortnite.[170] In 2020, Apple kicked Epic Games out of its App Store. It was not because Fortnite is, as some health experts warned, as addictive as heroin,[171] as Apple probably knows from the 116 million iOS users who spent over 2.86 billion hours playing the game just on their iPhones or iPads (about 25 hours per person).[172] Instead, Epic Games refused to pay Apple's 30% app tax. But that still leaves many other addictive apps in Apple's App Store, from which Apple profits. And as people spend more time and money on their apps, Apple's profits will only increase.[173]

Finally, even when apps are free, Apple still profits. Many apps in the Apple Store are loaded with third-party trackers, such as Facebook's.[174] As we will see in Chapter 4, these apps need to install third-party trackers to make money from behavioral ads. Apple knows that over a hundred billion dollars are spent annually on mobile ads.[175] Apple also knows that many apps in its App Store send sensitive personal information to the other data-opolies and data brokers to

profile us and predict and manipulate our behavior. Yet, Apple, for years, allowed these apps into its App Store and promoted these apps to induce us to buy its pricy devices. As Apple tells us: "Because we offer nearly two million apps—and we want you to feel good about using every single one of them."[176] Only in 2021 did Apple require apps to ask Apple users for their permission to track them across apps and websites owned by other companies. (The apps remain free to collect first-party data.)

Both the manipulator and those who aid and abet the manipulation are ethically and legally blameworthy. While Apple might wag its finger at the surveillance economy, it collects tens of billions of dollars annually from inviting these privacy offenders into its walled ecosystem.

## H. The Durability of GAFA's Power

We often hear that competition is a click away, but the reality is otherwise. The current market valuations of Google, Apple, Facebook, and Amazon suggest that investors do not anticipate disruption to their dominance. As the U.K.'s competition authority calculated, in 2020, the global returns on capital were over 40% for Google and 50% for Facebook, which are well above their cost of capital, which was 9%.[177] As Australia's competition authority found, "50–67%" of the 2019 share price for Facebook and "46–64%" of Google's 2019 share price "can be attributed to expectations for future growth."[178]

Their monopoly profits are staggering. Google's profit margins were "greater than 20% for nine out of the last 10 years [2011–2020], close to three times larger than the average for a U.S. firm."[179] As the Colorado-led states note in their monopolization complaint, "In 2019, Google made more revenue in what it characterizes as search advertising—$98 billion—than the GDP of 129 countries and the budgets of 46 States."[180]

In controlling their app stores, Google and Apple control the app distribution market and can impose a monopolistic tax on in-app revenues. As one tech executive testified before Congress, "Google and Apple have captured an almost perfect duopoly between the Android and iOS operating systems, and have in effect been able to collude to keep prices exorbitantly high for application makers (who then often pass on these fees to consumers)."[181]

Apple reaps monopoly profits from its services category, which enjoys even higher margins (63.7% in the fiscal year 2019 and 67.2% for its quarter ending in June 2020) than its products category.[182] Apple's operating margins for its app

store was estimated to be over 75% for 2018 and 2019.[183] Indeed, Apple, during the COVID-19 pandemic, was canvasing its App Store "to extract commissions" from businesses that were forced to change their business model to survive during the pandemic.[184]

Amazon extracts from third-party sellers billions of dollars in monopoly fees (on average, about 30% of each third-party sale).[185] Amazon also used the pandemic to exploit these sellers further.[186] During the pandemic, you could not get many third-party sellers' products, which Amazon deemed nonessential, but you could get Amazon's "hammocks, fish tanks, sex toys, and pool floaties."[187]

## I. Reflections

Table 1.2 ranks global companies by their market capitalization in 2020. It reveals the power of the digital platform business model as seven of the eight world's largest companies were digital platforms:

**Table 1.2** Ten Largest Companies in the World by Market Capitalization

| | **Market Capitalization in Billion U.S. Dollars (on April 30, 2020)** |
|---|---|
| Saudi Arabian Oil Company (Saudi Aramco) (Saudi Arabia) | $1,684.8 |
| ***Microsoft (United States)*** | ***$1,359*** |
| ***Apple (United States)*** | ***$1,285.5*** |
| ***Amazon (United States)*** | ***$1,233.4*** |
| ***Alphabet (United States)*** | ***$919.3*** |
| ***Facebook (United States)*** | ***$583.7*** |
| ***Alibaba (China)*** | ***$545.4*** |
| ***Tencent Holdings (China)*** | ***$509.7*** |
| Berkshire Hathaway (United States) | $455.4 |
| Johnson & Johnson (United States) | $395.3 |

*Source:* Andrea Murphy et al., *Global 2000: The World's Largest Public Companies*, Forbes (May 13, 2020), https://www.forbes.com/global2000/; *The 100 Largest Companies in the World by Market Capitalization in 2020 (in Billion U.S. Dollars)*, Statista (Dec. 1, 2020), https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/.

If one totaled the market capitalization of the world's 100 largest companies in April 2020, these seven companies accounted for 27.3% of the total. Amazon, Apple, Microsoft, and Google had the largest absolute increase in market capitalization between 2009 and 2019, with Facebook not far behind.[188] The

market capitalization of these four data-opolies, during the COVID-19 pandemic, increased further, and by September 2020, their combined value exceeded $5 trillion—"more than a third of the value of the S&P 100."[189]

America and Europe have a market power problem, which is more extreme in the tech sector.[190] The data-opolies' staggering profits represent their ability to exploit their monopoly power.[191]

While monopoly profits are exploitative, they are infrequently challenged in Europe and never challenged in the United States.[192] The courts' thinking is that the monopoly "may be the survivor out of a group of active competitors, merely by virtue of his superior skill, foresight and industry."[193] So the "successful competitor, having been urged to compete, must not be turned upon when he wins."[194]

But as we shall see next, these data-opolies did not attain and maintain their power through fair competition. They all relied on the same anticompetitive playbook.

---

1 Geoffrey West, Scale: The Universal Laws of Growth, Innovation, Sustainability, and the Pace of Life in Organisms, Cities, Economies, and Companies 402 (2018).

2 *Id*. at 397.

3 Michael A. Cusumano, Annabelle Gawer, & David B. Yoffie, The Business of Platforms: Strategy in the Age of Digital Competition, Innovation, and Power 108 (2019).

4 Majority Staff of H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial and Administrative Law, Report and Recommendations: Investigation of Competition in Digital Markets (2020), https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429 [https://perma.cc/29LN-L4BL] [hereinafter House Report] at 14, 176–80, 182 (collecting findings from other competitive authorities on Google's dominance); Complaint, United States v. Google, No. 1:20-cv-03010 (D.D.C. Oct. 20, 2020), ¶ 92, https://www.justice.gov/opa/press-release/file/1328941/download (alleging Google's monopoly power in the United States general search services market with approximately an "88 percent market share, followed far behind by Bing with about seven percent, Yahoo! with less than four percent, and DuckDuckGo with less than two percent.") [hereinafter Google Compl.]; Digital Competition Expert Panel, Unlocking Digital Competition at 25 (2019) (also known as the Furman Report), https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel [https://perma.cc/VK9M-3GV8] [hereinafter Furman Report] (noting Google's high market share in the general online search market in the United Kingdom, and globally, for more than a decade); UK Competition & Markets Authority, Online Platforms and Digital Advertising Market Study: Market Study Final Report ¶ 18 (July

1, 2020), https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digit [https://perma.cc/DA5V-RHA5] [hereinafter CMA Final Report] (noting that Google has generated around 90% or more of U.K. search traffic each year over the last 10 years and generated over 90% of U.K. search advertising revenues in 2019); Australian Competition and Consumer Commission, Digital Platforms Inquiry—Final Report at 8 (2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report [https://perma.cc/M36S-YQJ4] [hereinafter ACCC Final Report] (finding Google to have substantial market power in Australia in the supply of general search services, and supply of search advertising services, and substantial bargaining power in its dealings with news media businesses and that this power is unlikely to erode in the short to medium term); Commission Decision Case AT.39740 Google Search (Shopping), 2017 E.C. 1/2003 pt. 6.2, https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf [https://perma.cc/Y8W4-ZBAS] (finding Google, since 2007, holding a dominant position in each national market for general search, apart from in the Czech Republic, where Google has held a dominant position since 2011).

5 *Browser Market Share Worldwide—January 2021*, StatCounter https://gs.statcounter.com/browser-market-share (last visited Feb. 28, 2021) [https://perma.cc/E6UT-6ZLX]; House Report at 127 (finding the browser market highly concentrated, with Google's Chrome browser and Apple's Safari controlling roughly 80% of the browser market, with Chrome the leader in the U.S. desktop browser market (58.6% market share), followed by Safari (15.8%), and Safari the leader on mobile devices (55.5%) followed by Chrome (37.4%)).

6 Commission Decision Case AT.40099 Google Android, 2018 E.C. 1/2003, https://ec.europa.eu/competition/antitrust/cases/dec_docs/40099/40099_9993_3.pdf [https://perma.cc/3H6F-C3UW] (finding since 2011, Google holding a dominant position in the worldwide market (excluding China) for the licensing of smart mobile operating systems based on Google's market share, the existence of barriers to entry and expansion, the lack of countervailing buyer power, and the insufficient indirect constraint from non-licensable smart mobile operating systems (such as Apple's iOS)).

7 House Report at 15 (Google controlling 80% of mapping market).

8 House Report at 174.

9 Newley Purnell, *Cash May Be King in India, but Google Is Prince of Mobile Payments*, Wall St. J. (Sept. 19, 2019), https://www.wsj.com/articles/cash-may-be-king-in-india-but-google-is-prince-of-mobile-payments-11568885404 [https://perma.cc/S9VP-69XX].

10 Alphabet Inc., Q1 2019 Earnings Call Transcript (Apr. 29, 2019), https://abc.xyz/investor/static/pdf/2019_Q1_Earnings_Transcript.pdf?cache=ebdc584 [https://perma.cc/ZA99-GWZX].

11 House Report at 12, 93, 133 (noting that Facebook, in its internal documents, acknowledges that "it has high reach, time-spent, and significantly more users than its rivals in this market"); Press Release, Bundeskartellamt, Bundeskartellamt Prohibits Facebook

from Combining User Data from Different Sources (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2 https://perma.cc/L9PC-Y48K; Press Release, Bundeskartellamt, Preliminary Assessment in Facebook Proceeding: Facebook's Collection and Use of Data from Third-Party Sources Is Abusive (Dec. 19, 2017), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2 [https://perma.cc/PUS6-SRFS]; Furman Report at 26–27; ACCC Final Report at 9, 84 (finding Facebook to have in Australia substantial and durable market power in the supply of social media services and display advertising services, and substantial and durable bargaining power in its dealings with news media businesses); Complaint ¶¶ 2, 41 & 64, Federal Trade Commission v. Facebook, No. 1:20-cv-03590-CRC (D.D.C. Dec. 9, 2020), https://www.ftc.gov/enforcement/cases-proceedings/191-0134/facebook-inc-ftc-v [https://perma.cc/8GRR-9566] [hereinafter FTC Facebook Compl.] (alleging that Facebook has maintained a dominant share of the U.S. personal social networking market (in excess of 60%) since 2011); Complaint ¶ 68, New York v. Facebook, No. 1:20-cv-03589-JEB (D.D.C., Dec. 9, 2020), https://ag.ny.gov/press-release/2020/attorney-general-james-leads-multistate-lawsuit-seeking-end-facebooks-illegal [https://perma.cc/NLY2-MF6A] [hereinafter States Facebook Compl.], (alleging that Facebook "touted to its advertising clients that 'Facebook is now 95% of all social media in the US' ").

12 *The Top 20 Valuable Facebook Statistics—Updated October 2020*, Zephoria Digital Marketing, https://zephoria.com/top-15-valuable-facebook-statistics/ (last visited Feb. 26, 2021) [https://perma.cc/8P6A-TBY3].

13 *Best of 2019: The Year's Top Apps*, Apple, https://apps.apple.com/us/story/id1484100916 (last visited Feb. 26, 2021) [https://perma.cc/DJD6-L73A].

14 Furman Report at 30 (recognizing that Amazon "is dominant in a meaningfully distinct sector of online retail, for example as an online marketplace, particularly for relatively low-value and/or homogenous products").

15 Jeff Desjardins, *Amazon's Dominance in Ecommerce*, Visual Capitalist (Aug. 17, 2018), https://www.visualcapitalist.com/chart-shows-amazons-dominance-ecommerce/ [https://perma.cc/GJD4-786H]; *see also* House Report at 15 ("Although Amazon is frequently described as controlling about 40% of U.S. online retail sales, this market share is likely understated, and estimates of about 50% or higher are more credible.").

16 *Amazon.com Announces First Quarter Results*, Business Wire (Apr. 30, 2020, 4:01 PM), https://www.businesswire.com/news/home/20200430005943/en/ [https://perma.cc/YW9H-Z5K7]. The 26% increase was from its first quarter of 2019.

17 Stacy Mitchell, Ron Knox, & Zach Freed, *Report: Amazon's Monopoly Tollbooth*, Institute for Local Self-Reliance 2 (July 2020), https://ilsr.org/amazons_tollbooth/ [https://perma.cc/MY48-M7X4].

18 House Report at 251 & 319.

19 House Report at 114.

20 *Market Capitalization of Apple*, https://companiesmarketcap.com/apple/marketcap/

(last visited Feb. 26, 2021) [https://perma.cc/8V9J-ZSV3].

21 S. O'Dea, *Market Share of Mobile Operating Systems in the United States from January 2012 to December 2019*, Statista (Feb. 27, 2020), https://www.statista.com/statistics/272700/market-share-held-by-mobile-operating-systems-in-the-us-since-2009/. House Report at 16, 100 (noting that Google's Android and Apple's iOS are the "two dominant mobile operating systems" and combined "run on more than 99% of all smartphones in the world") & 335.

22 *See* European Commission, Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), at p. 14 (Dec. 15, 2020), https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf, https://perma.cc/G87S-Q88U:

> Core platform services, at the same time, feature a number of characteristics that can be exploited by their providers. These characteristics of core platform services include among others extreme scale economies, which often result from nearly zero marginal costs to add business users or end users. Other characteristics of core platform services are very strong network effects, an ability to connect many business users with many end users through the multi-sidedness of these services, a significant degree of dependence of both business users and end users, lock-in effects, a lack of multi-homing for the same purpose by end users, vertical integration, and data driven-advantages. All these characteristics combined with unfair conduct by providers of these services can have the effect of substantially undermining the contestability of the core platform services, as well as impacting the fairness of the commercial relationship between providers of such services and their business users and end users, leading to rapid and potentially far-reaching decreases in business users' and end users' choice in practice, and therefore can confer to the provider of those services the position of a so-called gatekeeper.

23 Glossary of Industrial Organisation Economics and Competition Law, compiled by R. S. Khemani and D. M. Shapiro, commissioned by the Directorate for Financial, Fiscal and Enterprise Affairs, OECD (1993); CMA Final Report ¶ 23.

24 *See, e.g.*, Complaint, United States v. United Technologies, No. 1:20-cv-00824 (D.D.C. Mar. 26, 2020), https://www.justice.gov/atr/case-document/file/1262896/download [https://perma.cc/R5KK-Y75Y].

25 Jacques Crémer, Yves-Alexandre de Montjoye, & Heike Schweitzer, Special Advisers' Report: Digital Policy for the Digital Era at 20 (2019), https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf [https://perma.cc/NV44-U3R2] [hereinafter EU Special Advisers Report]; *see also* ICN Unilateral Conduct Working Group, Report on the Results of the ICN Survey on Dominance/Substantial Market Power in Digital Markets at 5 (July 2020), https://www.internationalcompetitionnetwork.org/wp-content/uploads/2020/07/UCWG-Report-on-dominance-in-digital-markets.pdf [hereinafter

ICN Study]; Digital Markets Act at 14 (among the characteristics of the core platform services are "extreme scale economies, which often result from nearly zero marginal costs to add business users or end users").

26 CMA Final Report at ¶ 3.56; Complaint ¶ 22, United States v. Google, No. 1:20-cv-03010 (D.D.C. Oct. 20, 2020), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws, https://perma.cc/E5KS-YJV3 [hereinafter Google Compl.] (alleging that "[d]eveloping a general search index of this scale, as well as viable search algorithms, would require an upfront investment of billions of dollars" and that the "costs for maintaining a scaled general search business can reach hundreds of millions of dollars a year"); *see also id*. at ¶ 35 ("Google has long recognized that without adequate scale its rivals cannot compete. Greater scale improves the quality of a general search engine's algorithms, expands the audience reach of a search advertising business, and generates greater revenue and profits").

27 House Report at 79 (noting how many large webpages block most crawlers, which as a result significantly limits new search engine entrants, like Findx, a privacy-oriented search engine).

28 CMA Final Report at ¶ 3.56.

29 House Report at 179–80; CMA Final Report at ¶ 3.55 (finding that "Google's index contains around [500–600 billion] pages and Microsoft's index contains around [100–200 billion] pages"); EU Special Advisers Report at 20:

> With increasing returns to scale, competition between two firms producing the same product will not allow them to cover their costs. Indeed, were they to cover their (total) costs, they would have to price above the cost of serving an additional consumer (the marginal cost) and each of them would find it profitable to lower their price to steal the other's clients. As a consequence, no firm, unless armed with a much superior and cheaper technology, would *want* to enter a market dominated by an incumbent, even when this incumbent is making large profits.

30 ACCC Final Report at 76 (finding Google and Facebook are insulated "from dynamic competition to a considerable degree, by barriers to entry and expansion, advantages of scope as well as its acquisition strategies. Accordingly, while dynamic competition provides a degree of competitive constraint, large-scale entry is unlikely to occur at least in the short- to medium-term, ensuring that this constraint arising from dynamic competition remains somewhat weak.").

31 Furman Report at 39.

32 FTC Facebook Compl. ¶ 6 (noting that internal documents "confirm that it is very difficult to win users with a social networking product built around a particular social 'mechanic' (i.e., a particular way to connect and interact with others, such as photo-sharing) that is already being used by an incumbent with dominant scale"); *see also* ACCC Final Report at 9 (concluding that while "the threat of new entry may, in theory, provide a competitive constraint on Facebook, the considerable scale and reach of Facebook (over 20

times that of Myspace at its peak) appears to protect it from dynamic competition").

33 Roger McNamee, Zucked: Waking Up to the Facebook Catastrophe 32 (2019).

34 *Id.*

35 *Economics A–Z*, The Economist https://www.economist.com/economics-a-to-z/n#node-21529705 (last visited Feb. 27, 2021) [https://perma.cc/U4YL-9QSS].

36 For a discussion of different network effects, *see* Maurice E. Stucke & Allen P. Grunes, Big Data and Competition Policy (2016) at ¶¶ 11.04–13.39 (2016). *See also* McNamee, *supra* note 33, at 47.

37 Furman Report, *supra* note 4; OECD, Rethinking Antitrust Tools for Multi-Sided Platforms (Apr. 6, 2018), https://www.oecd.org/competition/rethinking-antitrust-tools-for-multi-sided-platforms.htm, [https://perma.cc/D7YL-VP5B] (noting how cross-platform network effects can magnify the competitive constraints that exist, while also raising entry barriers for potential rivals and restricting the emergence of new competitive constraints, and creating barriers to multi-homing); Digital Markets Act at 15; House Report at 40–41.

38 House Report at 13.

39 *Id.* at 143.

40 *Id.*

41 The increase in utility as others join the platform, however, is not necessarily linear, as Metcalfe discussed for communication technologies. Cusumano et al., Business of Platforms, *supra* note 3. Of course, as critics of Metcalfe's law note, not all connections are equally valuable, and diminishing returns exist. Andrew Odlyzko & Benjamin Tilly, *A Refutation of Metcalfe's Law and a Better Estimate for the Value of Networks and Network Interconnections* (2006), https://www.researchgate.net/publication/228829389_A_refutation_of_Metcalfe%27s_Law_a For example, you may derive greater value when your neighbors join the platform than someone across the globe. Nonetheless, as more people join the platform, it increases the likelihood that one's utility will increase somewhat—whether an amusing anecdote from a person in Thailand, a photo from Kenya, or interesting scholarship from Turkey or Brazil.

42 *See* House Report at 141 (Facebook internal document characterizing the network effects of Facebook, WhatsApp, and Messenger as "very strong" and that social apps have tipping points such that "either everyone uses them, or no-one uses them"); FTC Facebook Compl. ¶ 6 ("Even an entrant with a 'better' product often cannot succeed against the overwhelming network effects enjoyed by a dominant personal social network."); States Facebook Compl. ¶ 41 (alleging that the "most significant barrier to entry into the Personal Social Networking Services market is network effects," "because a core purpose of a Personal Social Networking Service is to connect and engage with a network of friends and family, it is very difficult for a new entrant to displace a dominant established network without already having built a comparable network for users to connect and engage").

43 Ohio v. Am. Express Co., 138 S. Ct. 2274, 2277, 201 L. Ed. 2d 678 (2018); *see also* Furman Report at 35.

44 United States v. Microsoft Corp., 84 F. Supp. 2d 9, 20 (D.D.C. 1999); Case T-201/04, *Microsoft Corp. v. Commission*, 2007 E.C.R. II-3601, ¶1061, https://eur-lex.europa.eu/legal-

content/EN/ALL/?uri=CELEX:62004TJ0201 [https://perma.cc/56JU-TGX4] ("The more people that use the platform, the more there will be invested in developing products compatible with that platform, which, in turn reinforces the popularity of that platform with users.").

45 *Desktop Operating System Market Share Worldwide*, StatCounter GlobalStats, https://gs.statcounter.com/os-market-share/desktop/worldwide#monthly-200901-202008 (last visited Feb. 27, 2021).

46 House Report at 117 (noting how infrastructure providers of cloud computing "benefit from network effects—the more customers on a platform, the more third parties build services that integrate well with that platform leading to more services to attract customers") & 320.

47 House Report at 225 (noting how Google's browser "is likely to remain dominant because it benefits from network effects" since "[w]eb developers design and build for the Chrome browser because it has the most users, and users, in turn, are drawn to Chrome because webpages work well on it").

48 Commission Decision of 18 July 2018 in Case AT. 40099—Google Android, https://ec.europa.eu/competition/antitrust/cases/dec_docs/40099/40099_9993_3.pdf [https://perma.cc/56K7-Q2TB] [hereinafter EC Android Decision] ¶ 464 (finding that "the worldwide market for the licensing of smart mobile device OSs is characterised by network effects," which arise "because, when deciding which licensable smart mobile OS to develop for, app developers consider the revenue potential of that OS and since they 'earn their profits mainly by app downloads, mobile OSs with a large user base are considered more attractive by app developers' "); House Report at 105 (noting that the "most important factor that developers consider before building apps for an OS is the install base of the OS—how many users have devices running the OS that can install the app" and that "developers will not build apps for an OS with few users," which "reinforces the power of dominant mobile operating systems") & 123.

49 *See, e.g.*, ACCC Final Report 3.2; United States v. Bazaarvoice, Inc., No. 13-CV-00133-WHO, 2014 WL 203966, at *21 (N.D. Cal. Jan. 8, 2014) ("A critical asset in building a successful social commerce network is to have the largest audience possible because that is how advertisers and marketers and brands think about the value they get.") (internal quotations omitted).

50 Julia Angwin, Surya Mattu, & Terry Parris Jr., *Facebook Doesn't Tell Users Everything It Really Knows About Them*, ProPublica (Dec. 27, 2016, 9:00 AM), https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them [https://perma.cc/3KYH-LYCW]; Julia Angwin, Madeleine Varner, & Ariana Tobin, *Facebook Enabled Advertisers to Reach "Jew Haters,"* ProPublica (Sept. 14, 2017, 4:00 PM), https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters [https://perma.cc/2D8H-3SKD]; Alex Kantrowitz, *Google Allowed Advertisers to Target People Searching Racist Phrases*, BuzzFeed News (Sept. 15, 2017, 2:15 PM), https://www.buzzfeednews.com/article/alexkantrowitz/google-allowed-advertisers-to-target-

jewish-parasite-black [https://perma.cc/3ZM7-2E6A].

51 *Report Data or Content Errors on Google Maps*, Google Maps Help, https://support.google.com/maps/answer/3094088?hl=en (last visited Feb. 27, 2021) [https://perma.cc/RKF8-YB5H].

52 House Report at 109 (quoting a market participant on how "Google's dominant position in search and advertising incentivizes businesses to closely monitor and maintain the accuracy of their information in Google's systems, 'leading to a dynamic by which Google enjoys a free, crowdsource effort to improve and maintain their data's quality,' thereby improving the quality of Google Maps").

53 This is also a problem for users of Google Maps. Shane Hickey, *Google Maps Postcode Error Leads Delivery Drivers on Wild Pizza Chase: A Mix-Up on the Tech Giant's Service Has Meant Three Years of Frustration for Simon Borghs, and Highlights Our Reliance on the Data Private Companies Hold*, The Guardian (Dec. 20, 2020), https://www.theguardian.com/money/2020/dec/20/google-maps-postcode-error-leads-delivery-drivers-on-wild-pizza-chase [https://perma.cc/L3M3-KVUV].

54 Shoshana Zuboff, The Age of Surveillance Capitalism 155 (2019).

55 House Report at 125 (noting that as "a voice assistant improves its 'understanding' of its user, it may increase the costs associated with switching to another platform," and as one market participant noted "the user may become more dependent on that particular voice assistant and be far less likely to use a rival voice assistant that has not yet 'caught up' with the user's preference").

56 McNamee, *supra* note 33, at 76.

57 *Id*. at 76–77 (discussing how algorithms through trial and error can identify other people with similar characteristics, "Lookalike Audience," whom advertisers can target to expand sales).

58 House Report at 80–81; Stucke & Grunes, *supra* note 36, at 172–81; European Commission Press Release Memo 17/1785, *Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service* (June 27, 2017), http://europa.eu/rapid/press-release_MEMO-17-1785_en.htm [https://perma.cc/95D5-TE2F] (discussing high barriers to entry in these markets, in part because of network effects: "the data a search engine gathers about consumers can in turn be used to improve results").

59 Digital Markets Act at 27; Stucke & Grunes, *supra* note 36, at 170–81; Commission Decision of June 27, 2017 (Case AT. 39740--Google Search (Shopping)), https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf [https://perma.cc/NH5J-APP4] [hereinafter Google Shopping case], ¶¶ 287–88.

60 ICN Study at 28.

61 Digital Markets Act at 27–28.

62 Google Shopping case ¶ 288; CMA Final Report at ¶ 3.27; House Report at 179 (noting how "in 2010, one Google employee observed, 'Google leads competitors. This is our bread-and-butter. Our long-tail precision is why users continue to come to Google. Users

may try the bells and whistles of Bing and other competitors, but Google still produces the best results.' "); Complaint, Colorado v. Google, No. 1:20-cv-03715-APM (D.D.C. Dec. 17, 2020), https://coag.gov/app/uploads/2020/12/Colorado-et-al.-v.-Google-PUBLIC-REDACTED-Complaint.pdf [hereinafter Colo. Google Compl.], ¶ 91.

63 CMA Final Report ¶ 3.68.

64 ICN Study at 28.

65 To test this, the U.K. competition authority analyzed all the search events seen by Google and Bing in a one-week period in the United Kingdom. What it found was that Google saw 16 times more tail inquiries than Bing. Moreover, while a relatively large proportion of Bing's tail queries were also seen in the Google dataset, a very small proportion of Google's tail queries were in the Bing dataset. So, the competition agency found that relatively uncommon queries account for a significant proportion of the queries seen by search engines, and that these "learning-by-doing" network effects benefit the dominant search engine over Bing in relation to uncommon search queries. CMA Final Report at ¶¶ 25–27.

66 CMA Final Report ¶ 3.79.

67 Zuboff, *supra* note 54, at 338–39.

68 House Report at 308.

69 Dissenting Statement of Commissioner Rohit Chopra, *In re Google LLC and YouTube, LLC* Commission File No. 1723083 (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtu [https://perma.cc/PNM6-LETP]; *see also* Zuboff, *supra* note 54, at 339.

70 Ben Popken, *As Algorithms Take Over, YouTube's Recommendations Highlight a Human Problem*, NBC News (April 19, 2018), https://www.nbcnews.com/tech/social-media/algorithms-take-over-youtube-s-recommendations-highlight-human-problem-n867596 [https://perma.cc/CG3M-722Q] (noting how YouTube's "complex 'machine learning' system, which uses trial and error combined with statistical analysis to figure out how to get people to watch more videos, figured out that the best way to get people to spend more time on YouTube was to show them videos light on facts but rife with wild speculation"); *see also* Tripp Mickle, *YouTube Algorithm Found to Push Harmful Content*, Wall St. J., (July 8, 2021).

71 Furman Report at 35 (recognizing that network effects are "not necessarily natural features of a market but can be the result of technological design decisions, such as whether to facilitate data mobility and systems with open standards").

72 CMA Final Report at ¶¶ 1, 60, 2.38, 43 (finding the "inability of smaller platforms and publishers to access user data creates a significant barrier to entry"); OECD Consumer data rights and competition conference—Note by Germany at ¶ 11 (June 12, 2020), https://one.oecd.org/document/DAF/COMP/WD(2020)32/en/pdf; Digital Markets Act at 22 (noting how the powerful platforms' "combining end user data from different sources or signing in users to different services of gatekeepers gives them potential advantages in terms of accumulation of data, thereby raising barriers to entry").

73 McNamee, *supra* note 33, at 9; *see also* Furman Report at 9 (recognizing "the central

importance of data as a driver of concentration and barrier to competition in digital markets"); ICN Study at 23–24; FTC Facebook Compl. ¶ 6; States FTC Compl. ¶ 41; House Report at 17, 37–38, 40–41, 42–44; Stucke & Grunes, *supra* note 36, 310 ¶¶ 2.04–2.29; OECD Policy Roundtables, *Big Data: Bringing Competition Policy to the Digital Era*, DAF/COMP(2016)14, at 5, https://www.oecd.org/competition/big-data-bringing-competition-policy-to-the-digital-era.htm [https://perma.cc/AW2C-RLRK]. While policymakers are recognizing the importance of attention and data in digital markets, they haven't in the past, and as a result allowed anticompetitive mergers and conduct. *See* Tim Wu, *The Attention Economy and the Law*, 82 Antitrust L.J. 771 (2019).

74 House Report at 42.

75 House Report at 147 (internal footnotes omitted); *see also* States Facebook Compl. ¶ 3 ("The more data Facebook accumulates by surveilling the activities of its users and the more time the company convinces users to spend engaging on Facebook services, the more money the company makes through its advertising business.").

76 CMA Final Report at ¶ 2.38.

77 Colo. Google Compl. ¶ 5.

78 House Report at 174.

79 CMA Final Report at ¶ 27; *Alphabet "Other Bets": In Search Of Google's Hidden Gems*, FourWeekMBA, https://fourweekmba.com/google-bets/#What_is_Access (last visited Feb. 27, 2021).

80 Rob Copeland et al., *Paging Dr. Google: How the Tech Giant Is Laying Claim to Health Data*, Wall St. J. (Jan. 11, 2020), https://www.wsj.com/articles/paging-dr-google-how-the-tech-giant-is-laying-claim-to-health-data-11578719700 [https://perma.cc/5F2Z-7ZL2].

81 Rob Copeland, *Google's "Project Nightingale" Gathers Personal Health Data on Millions of Americans*, Wall St. J. (Nov. 11, 2019), https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790 [https://perma.cc/RV7V-DLEZ]. To address the European Commission's concerns, Google agreed to limit its use of Fitbit health and wellness data in Europe. Google will not use the Fitbit data collected from users in Europe for Google Ads, including search advertising, display advertising, and advertising intermediation products. Google will also store Fitbit's user data in a "data silo," that is separate from any other Google data that is used for advertising. Europeans can also grant or deny Google's other services from using the health and wellness data. European Commission, Press Release, *Commission Clears Acquisition of Fitbit by Google, Subject to Conditions* (Dec. 17, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484.

82 Mike Colias, *Ford to Use Google's Android System in Most Cars*, Wall St. J. (Feb. 2, 2021), https://www.wsj.com/articles/ford-to-use-google-s-android-system-in-most-cars-by-2023-11612199574 [https://perma.cc/67HT-42UV]; Mike Colias, *GM Turns to Google for In-Car Apps, Voice Commands*, Wall St. J. (Sept. 5, 2019), https://www.wsj.com/articles/gmturns-togooglefor-in-car-apps-voice-commands-11567692000 [https://perma.cc/CV2L-AHF5].

83 Geoffrey A. Fowler, *The Spy in Your Wallet: Credit Cards Have a Privacy Problem*,

Washington Post (Aug. 26, 2019), https://www.washingtonpost.com/technology/2019/08/26/spy-your-wallet-credit-cards-have-privacy-problem/ [https://perma.cc/CD5C-HEKK].

84 Colo. Google Compl. ¶ 35.

85 John Fitzgerald, *Amazon Surveils Closed Facebook Groups, Flex Drivers Claim*, Jackson v. Amazon.com, 27 No. 12 Westlaw Journal Class Action 06 (Jan. 26, 2021) (contract delivery drivers for Amazon.com Inc.—known as Flex drivers—claiming in a federal lawsuit that the company employs a surveillance team—the "Orwellian-sounding Advocacy Operations Social Listening Team"—that surreptitiously monitors their posts in closed Facebook groups).

86 FTC Facebook Compl. ¶ 48.

87 *See, e.g.*, States Facebook Compl. ¶¶ 127 (alleging that Facebook "degraded Instagram users' privacy by matching Instagram and Facebook Blue accounts so that Facebook could use information that users had shared with Facebook Blue to serve ads to those users on Instagram"), 177 (alleging how Facebook changed WhatsApp's terms of service and privacy policy and eroded the preacquisition promises it had made, by combining "user data across the services by linking WhatsApp user phone numbers with accounts on Facebook Blue, enabling WhatsApp user data to be used across all Facebook products," so that Facebook Blue users "who had declined to give their phone numbers to Facebook suddenly found their phone numbers connected to their Facebook Blue accounts anyway") & 238–41; *Place Your Facebook Ads on Mobile Apps with Audience Network*, https://www.facebook.com/business/marketing/audience-network (last visited Feb. 27, 2021) [https://perma.cc/S3QM-M5L8].

88 According to Facebook, over one billion people see an Audience Network ad every month. *Place Your Facebook Ads on Mobile Apps with Audience Network*, *supra* note 87. Moreover, 3.21 billion people were monthly active persons on Facebook's platforms, in the third quarter of 2020, which the company defines as registered and logged-in users of Facebook, Instagram, Messenger, and/or WhatsApp visited at least one of these Family products through a mobile device application or using a web or mobile browser in in the last 30 days as of the date of measurement. Facebook Q3 2020 Results, at 6, https://s21.q4cdn.com/399680738/files/doc_financials/2020/q3/FB-Q3-2020-Earnings-Presentation.pdf [https://perma.cc/94K6-RD49].

89 Michal Kosinski, David Stillwell, & Thore Graepel, *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 Proc. Nat'l Acad. Sci. 5802 (2013), https://doi.org/10.1073/pnas.1218772110 [https://perma.cc/2LR4-4782].

90 N.Y. State Dept. of Financial Services, Report on Investigation of Facebook Inc. Data Privacy Concerns (Feb. 18, 2021), https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf [hereinafter, NY State Facebook Report]; Bundeskartellamt, Case Summary, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing, at 10 (Feb. 15, 2019), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufs

22-16.pdf?__blob=publicationFile&v=4 [hereinafter Bundeskartellamt Facebook Case Summary]; ACCC Final Report at 86; Zuboff, *supra* note 54, at 159–61 (discussing the evolution of this tracking feature, which Facebook first called a programming bug, when it was in fact a feature).

91 Bundeskartellamt Facebook Case Summary at 10.

92 Cianan Brennan, *Google Fined over Online Data Breach*, Times (London) (Jan. 22, 2019), https://www.thetimes.co.uk/article/google-fined-over-online-data-breach-hnpcd0lcf [https://perma.cc/KC8Z-NLWX]; Shweta Ganjoo, *Facebook Tracks Android Users Even If You Don't Have Facebook App Installed, or Don't Have FB Account*, India Today (Jan. 30, 2019), https://www.indiatoday.in/technology/news/story/facebook-tracks-android-users-even-if-you-don-t-have-facebook-app-installed-or-don-t-have-fb-account-1442499-2019-01-30 [https://perma.cc/R94L-J9H3].

93 NY State Facebook Report at 4–5, 12. Facebook reported to the NY Department of Finance that from November 21–28, 2020, "a daily average of approximately 25 million events sent by health apps triggered" its system to screen sensitive health information, "which represents only approximately 2.5% of the daily total number of events sent by health apps during that same time."

94 Karen Hao, *How Facebook Got Addicted to Spreading Misinformation: The Company's AI Algorithms Gave It an Insatiable Habit for Lies and Hate Speech. Now the Man Who Built Them Can't Fix the Problem*, MIT Tech. Rev. (Mar. 11, 2021).

95 Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, Wall St. J. (Feb. 22, 2019), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636 [https://perma.cc/YVB2-ZDF8]; NY State Facebook Report at 2 (finding that Facebook did indeed receive sensitive user data from third parties, in contravention of Facebook's own internal policies, particularly in the area of medical and health information).

96 Although Facebook had a policy that app developers should not transmit sensitive health data to Facebook, "there were many examples where the developers violated that policy and Facebook did indeed—unwittingly, it contends—receive, store, and analyze sensitive data." NY State Facebook Report at 7. Nor did Facebook track whether apps were complying with its policy or punish apps for violating its policy. *Id.* at 16.

97 House Report at 263.

98 House Report at 262.

99 House Report at 283.

100 House Report at 265.

101 House Report at 255.

102 Jennifer Wills, *6 Ways Amazon Uses Big Data to Stalk You*, Investopedia (Oct. 5, 2020), https://www.investopedia.com/articles/insights/090716/7-ways-amazon-uses-big-data-stalk-you-amzn.asp [https://perma.cc/UGZ3-YWGV].

103 *Id*.

104 Dorian Lynskey, *"Alexa, Are You Invading My Privacy?"—The Dark Side of Our*

*Voice Assistants*, The Guardian (Oct. 9, 2019), https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants [https://perma.cc/3NYM-9SHY]; *see also* House Report at 315 (noting how Amazon "uses its market power to collect third-party voice application data" from manufacturers of smart-home devices).

105 Karen Hao, *Inside Amazon's Plan for Alexa to Run Your Entire Life*, MIT Tech. Rev. (Nov. 5, 2019), https://www.technologyreview.com/2019/11/05/65069/amazon-alexa-will-run-your-life-data-privacy/.

106 *Id.*

107 Charlotte Jee, *Amazon Wants You to Be Surrounded with Alexa—Wherever You Are*, MIT Tech. Rev. (Sept. 26, 2019), https://www.technologyreview.com/2019/09/26/132868/amazons-new-products-show-it-wants-alexa-to-always-be-with-you/.

108 Hao, *supra* note 105.

109 *Amazon Fire TV Devices*, Amazon, https://www.amazon.com/Amazon-Fire-TV-Family/b?ie=UTF8&node=8521791011 (last visited Feb. 27, 2021) [https://perma.cc/9SML-KTE7].

110 Hooman Mohajeri Moghaddam, *Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices*, Freedom To Tinker (Sept. 18, 2019), https://freedom-to-tinker.com/2019/09/18/watching-you-watch-the-tracking-ecosystem-of-over-the-top-tv-streaming-devices/ [https://perma.cc/HA3C-4M7V].

111 Kate Cox, *Amazon's Ring App Shares Loads of Your Personal Info, Report Finds*, Ars Technica (Jan. 28, 2020), https://arstechnica.com/tech-policy/2020/01/amazons-ring-app-shares-loads-of-your-personal-info-report-finds/ [https://perma.cc/YHW4-ZQRQ]; *Ring Privacy Notice*, https://shop.ring.com/pages/privacy-notice [https://perma.cc/KR5C-GLU9] (last visited Feb. 27, 2021); Letter from Senator Edward J. Markey to Jeffrey Bezos, CEO of Amazon.com, Inc. (Sept. 5, 2019), https://www.markey.senate.gov/download/ring-law-enforcement-2019 [https://perma.cc/3E6L-LUGS]; Caroline Haskins, *How Ring Transmits Fear to American Suburbs—Why Do We Surveil Ourselves?*, Vice (Dec. 6, 2019), https://www.vice.com/en/article/ywaa57/how-ring-transmits-fear-to-american-suburbs [https://perma.cc/F3EH-5WUD].

112 Bill Budington, *Ring Doorbell App Packed with Third-Party Trackers*, Electronic Frontier Foundation (Jan. 27, 2020), https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers [https://perma.cc/43CS-D7EA].

113 Kellen Browning, *Amazon Unveils Drone That Films Inside Your Home. What Could Go Wrong?*, N.Y. Times (Sept. 24, 2020), https://www.nytimes.com/2020/09/24/technology/amazon-ring-drone.html [https://perma.cc/TY4K-NBXY]; *Ring Support Center: Always Home Camera*, https://support.ring.com/hc/en-us/articles/360050068591 (last visited Feb. 27, 2021) [https://perma.cc/WF83-46T7].

114 Ring (@ring), Twitter (Sept. 25, 2020, 1:49 AM),

https://twitter.com/ring/status/1309369425653506048.

115 *Ring Support Center: Always Home Camera*, https://support.ring.com/hc/en-us/articles/360050068591-Always-Home-Cam-Information (last visited Feb. 27, 2021) [https://perma.cc/43K5-3B7Q].

116 Ben Saunders, *Who's Using Amazon Web Services? [2020 Update]*, Contino (Jan. 28, 2020), https://www.contino.io/insights/whos-using-aws [https://perma.cc/US7K-LUYS].

117 House Report at 323 (noting how market participant who spoke with the Subcommittee staff had evidence that AWS engaged in this cross-business data sharing) & 324 (noting that if an Amazon employee could access an AWS customer's encryption keys, they "could potentially see the contents of a customer's application, including proprietary code, business transactions, and data on their users"). Moreover, the data can be of competitive significance enabling Amazon to identify and squelch nascent competitive threats. House Report at 324.

118 Wills, *supra* note 102.

119 Zack Whittaker, *I Asked Apple for All My Data. Here's What Was Sent Back*, Zero Day (May 24, 2018), https://www.zdnet.com/article/apple-data-collection-stored-request/ [https://perma.cc/5SW9-QV7C].

120 Apple, *Privacy: Your California Privacy Disclosures*, https://www.apple.com/legal/privacy/california/ (last visited Feb. 27, 2021) [https://perma.cc/3LY3-HT7S].

121 Sebastian Herrera, *Facebook to Counter Apple Privacy Update with Its Own Prompt*, Wall St. J. (Feb. 2, 2021), https://www.wsj.com/articles/facebook-to-counter-apple-privacy-update-with-its-own-prompt-11612191604.

122 Dan Levy, VP Ads and Business Products at Facebook, *Speaking Up for Small Businesses* (Dec. 16, 2020), https://about.fb.com/news/2020/12/speaking-up-for-small-businesses/ [https://perma.cc/SK9K-D4SN].

123 *Id.* ("Apple's personalized ad platform isn't subject to the new iOS 14 policy."). Some of Facebook's other claims, however, that Apple's decision will hurt small businesses, have been attacked. Bart de Langhe & Stefano Puntoni, *Facebook's Misleading Campaign Against Apple's Privacy Policy*, Harvard Bus. Rev. (Feb. 2, 2021), https://hbr.org/2021/02/facebooks-misleading-campaign-against-apples-privacy-policy [https://perma.cc/4YJV-FTG9].

124 Apple, *Apple Privacy Policy*, https://www.apple.com/legal/privacy/en-ww/ (last visited Feb. 27, 2021) [https://perma.cc/RF4G-R4SN].

125 Apple, *California Privacy Disclosures*, https://support.apple.com/en-us/HT210807 (last visited Feb. 27, 2021) [https://perma.cc/MY99-FPD4]; Apple, *Apple Advertising & Privacy*, https://support.apple.com/en-us/HT205223 (last visited Feb. 27, 2021) [https://perma.cc/NLJ5-SWBG]; Apple, *App Store & Privacy*, https://support.apple.com/en-us/HT210584 (last visited Feb. 27, 2021) [https://perma.cc/9FZB-RYUY].

126 O'Dea, *supra* note 21; House Report at 211–12.

127 Alexander Kunst, *How Often Do You Use Apple Devices?*, Statista (Sept. 23, 2019), https://www.statista.com/statistics/702996/apple-device-usage-frequency-in-us/; Harsh

Chauhan, *Apple's iPhone Will Dominate Smartphones in 2020. Here's Why*, The Motley Fool (Dec. 31, 2019), https://www.fool.com/investing/2019/12/31/apples-iphone-will-dominate-smartphones-2020-why.aspx [https://perma.cc/LW7M-ZBGA].

128 Apple, *App Store & Privacy*, *supra* note 124.

129 Whittaker, *supra* note 119.

130 *See* Apple 2020 Form 10-K, https://s2.q4cdn.com/470004039/files/doc_financials/2020/ar/_10-K-2020-(As-Filed).pdf, at 21. Apple's net sales in 2020 from Apple Services, which include sales from advertising, the App Store, and cloud services, was $53.768 billion, a 35% increase from its 2018 levels. Services in 2020 was the second largest category after iPhones (whose net sales declined 16% from 2018 levels) and accounted for 20% of total net sales in 2020. In 2018, Apple Services accounted for 15% of Apple's net sales.

131 House Report at 37–38; Furman Report at 4 (noting how "in many cases tipping can occur once a certain scale is reached, driven by a combination of economies of scale and scope; network externalities whether on the side of the consumer or seller; integration of products, services and hardware; behavioural limitations on the part of consumers for whom defaults and prominence are very important; difficulty in raising capital; and the importance of brands"); Unilateral Conduct Working Group, July 2020, *supra* note 25, at 5, 27; Digital Markets Act at 1 & 20 (noting that "whereas over 10 000 online platforms operate in Europe's digital economy . . . a small number of large online platforms capture the biggest share of the overall value generated" and how the "same specific features of core platform services make them prone to tipping: once a service provider has obtained a certain advantage over rivals or potential challengers in terms of scale or intermediation power, its position may become unassailable and the situation may evolve to the point that it is likely to become durable and entrenched in the near future. Undertakings can try to induce this tipping and emerge as gatekeeper by using some of the unfair conditions and practices regulated in this Regulation.").

132 Felix Richter, *Smartphone OS: The Smartphone Duopoly*, Statista (May 20, 2019), https://www.statista.com/chart/3268/smartphone-os-market-share/.

133 *Number of Apps Available in Leading App Stores as of 4th Quarter 2020*, Statista (Feb. 25, 2021), https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/.

134 Furman Report at 29, 40; House Report at 104.

135 Furman Report Point 1.55, p. 29.

136 States Facebook Compl. ¶ 66.

137 States Facebook Compl. ¶ 67.

138 ACCC Final Report, Point 2.36, pp. 58, 76, 78 (concluding that Google and Facebook are insulated from dynamic competition to a considerable degree, by barriers to entry and expansion, advantages of scope as well as its acquisition strategies); Digital Markets Act at 1 ("A few large platforms increasingly act as gateways or gatekeepers between business users and end users and enjoy an entrenched and durable position, often as a result of the creation

of conglomerate ecosystems around their core platform services, which reinforces existing entry barriers.").

139 CMA Final Report at ¶ 6.6.

140 Dissenting Statement of Commissioner Rohit Chopra, *supra* note 69; *see also* Furman Report at 115 (noting how the programmatic online advertising model's "data-driven nature means that those digital platforms with the greatest scale, scope and timeliness of data about the consumer are in a very strong position to derive value from matching that consumer with the advertiser"); CMA Final Report at ¶ 5.166 ("The more data and the higher the quality of the data a platform holds, the better equipped it is to provide advertisers with exactly what they want.").

141 Zuboff, *supra* note 54, at 133.

142 *Id.* at 154; *see also* McNamee, *supra* note 33, at 43.

143 Tim Wu, *Blind Spot: The Attention Economy and the Law*, 82 Antitrust L.J. 771, 788 & 789 (2019).

144 Zuboff, *supra* note 54, at 294. As one 2019 study found, those "who are heavier users of Facebook and those who have used the site the longest are more likely to be listed in a larger number of personal interest categories," and 40% of the Facebook users who use the platform multiple times a day were listed in 21 or more categories used to target them with ads. Paul Hitlin & Lee Rainie, *Facebook Algorithms and Personal Data*, Pew Research Center (Jan. 16, 2019), https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/ [https://perma.cc/6P64-P764].

145 McNamee, *supra* note 33, at 5.

146 *Id.* at 9.

147 *Id.*

148 Cambridge Analytica is alleged to have used Facebook data to dissuade some citizens from voting. Craig Timberg & Isaac Stanley-Becker, *Cambridge Analytica Database Identified Black Voters as Ripe for "Deterrence," British Broadcaster Says*, Washington Post (Sept. 28, 2020), https://www.washingtonpost.com/technology/2020/09/28/trump-2016-cambridge-analytica-suppression/ [https://perma.cc/D22M-2FKZ]. For Facebook's randomized controlled trial of political mobilization messages delivered to 61 million Facebook users during the 2010 U.S. congressional elections to measure messages "directly influenced political self-expression, information seeking and real-world voting behaviour of millions of people," *see* Robert M. Bond et al., *A 61-Milion-Person Experiment in Social Influence and Political Mobilization*, 489 Nature 295–98, (2012), http://fowler.ucsd.edu/massive_turnout.pdf [https://perma.cc/PP5Z-BQLQ]. For some of the concerns about Google's and Facebook's ability to influence voting, *see* David Shultz, *Could Google Influence the Presidential Election?*, Science (Oct. 25, 2016), https://www.sciencemag.org/news/2016/10/could-google-influence-presidential-election [https://perma.cc/L2TF-V6KJ]. For some of the congressional concerns about the platforms' censoring disfavored voices, *see* Ken Buck, House Judiciary Committee, Subcommittee on Antitrust, Commercial, and Administrative Law, *The Third Way*,

https://buck.house.gov/sites/buck.house.gov/files/wysiwyg_uploaded/Buck%20Report.pdf [https://perma.cc/6WH3-TLQ7].

149 Zuboff, *supra* note 54, at 279 (discussing internal Facebook document about its ability "to predict future behavior," including "loyalty predictions").

150 *Id.* at 294–309 (quoting a senior engineer and outlining three key mechanisms for behavioral modification: *tuning*, through nudges and choice architecture; *herding*, which involves "foreclosing action alternatives and thus moving behavior along a path of heightened probability that approximates certainty"; and *conditioning*, and Facebook's experimentation on users); *see also* Betsy Morris, *The New Tech Avengers*, Wall St. J. (June 29, 2018), https://www.wsj.com/articles/the-new-tech-avengers-1530285064; Levi Sumagaysay, *Former Google, Facebook Employees Step Up Battle Against Tech Addiction*, Mercury News (San Jose) (Feb. 5, 2018), http://bayareane.ws/2EIqLTB; Nellie Bowles, *Early Facebook and Google Employees Form Coalition to Fight What They Built*, N.Y. Times (Feb. 4, 2018), https://nyti.ms/2GJoKHg [https://perma.cc/LX4M-V4EL]; Tia Ghose, *What Facebook Addiction Looks Like in the Brain*, LiveScience (Jan. 27, 2015), https://www.livescience.com/49585-facebook-addiction-viewed-brain.html [https://perma.cc/X4NY-NKUM].

151 CMA Final Report at ¶ 5.345.

152 CMA Final Report at ¶ 5.352.

153 CMA Final Report at ¶¶ 41 & 5.353; UK Competition & Markets Authority, Online Platforms & Digital Advertising: Market Study Interim Report (2019), https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pd [hereinafter CMA Interim Report] at ¶¶ 5.144. 5.275, 5.286; Colo. Google Compl. ¶ 92 ("Google's data gathering apparatus is unrivaled and enables Google to collect consumer data from Google's search engine, its dominant Chrome browser, more than 100 million U.S. Android mobile users, Google Assistant, and more than one billion Google account holders from the United States and across the globe. Because of the unique data sources Google owns through its conglomerate of integration and anticompetitive contracts, Google can accurately track a consumer as they switch among devices or move from web to app, and travel in the physical world."); FTC Facebook Compl. ¶ 49 (alleging Facebook's "preeminent ability to target users with advertising due to its scale, its high level of user engagement, and its ability to track users both on and off Facebook properties to measure outcomes").

154 *Hearing on Online Platforms and Market Power Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. (July 29, 2020) (Statement of Tim Cook, Chief Executive Officer of Apple Inc. at 3), https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-Wstate-CookT-20200729.pdf.

155 One exception is that until September 2017, Apple used Microsoft Bing for web search results in the Siri and Spotlight (on Mac and including Search within iOS) access points, but eventually switched to Google for web search results for these search access

points. CMA Final Report Appendix H at ¶ 37.

156 CMA Final Report at ¶ 3.107 n. 132; *see also* Google Compl. ¶¶ 47, 175, 182.

157 Google Compl. ¶ 122 ("[b]y paying Apple a portion of the monopoly rents extracted from advertisers, Google has aligned Apple's financial incentives with its own").

158 CMA Final Report at ¶ 3.98.

159 Neil Cybart, *Apple's Billion Users*, Above Avalon (May 30, 2019), https://www.aboveavalon.com/notes/2019/5/30/apples-billion-users [https://perma.cc/UA2Z-SU8N].

160 ACCC Final Report at 10, 30 (recommending changes to search engine and internet browser defaults so that Google provides Australian users of Android devices with the same options being rolled out to existing Android users in Europe: the ability to choose their default search engine and default internet browser from a number of options); CMA Final Report at ¶ 89 & ¶ 3.106 (finding that in 2019, Google paid Apple £1.2 billion for default positions in the United Kingdom alone, which represented over 17% of Google's total annual search revenues in the United Kingdom).

161 Apple 2019 Form 10-K, https://s2.q4cdn.com/470004039/files/doc_financials/2019/ar/_10-K-2019-(As-Filed).pdf at 29 [https://perma.cc/NPG5-EQST].

162 Johan Moreno, *Google Estimated To Be Paying $15 Billion To Remain Default Search Engine On Safari*, Forbes (Aug. 27, 2021).

163 Kent Walker, *A Deeply Flawed Lawsuit That Would Do Nothing to Help Consumers*, The Keyword (Oct. 20, 2020), https://blog.google/outreach-initiatives/public-policy/response-doj/ [https://perma.cc/2D74-S4JV].

164 EC Android Decision ¶ 633 (quoting internal Google document); Google Compl. ¶¶ 47 (alleging that "Google observed in a 2018 strategy document, 'People are much less likely to change [the] default search engine on mobile' "), 149 (Google executive stating that "most users just use what comes on the device") & 119 (alleging that "Google's documents recognize that 'Safari default is a significant revenue channel;' " that "losing the deal would fundamentally harm Google's bottom line"; that "Google views the prospect of losing default status on Apple devices as a 'Code Red' scenario. In short, Google pays Apple billions to be the default search provider, in part, because Google knows the agreement increases the company's valuable scale; this simultaneously denies that scale to rivals.").

165 Google Compl. ¶ 118; Colo. Google Compl. ¶ 108.

166 Google Compl. ¶ 120. But it isn't just Apple. Google has search advertising revenue share agreements with all the other key gateways to the internet, giving billions of dollars to Android device manufacturers (like Samsung, LG, and Motorola), other companies that offer web browsers (like Opera and Mozilla's Firefox), and U.S. mobile carriers like T-Mobile, Verizon, and AT&T, to ensure its search engine is the default. Colo. Google Compl. ¶¶ 43, 123. Google's Senior VP responded that "[its] agreements with Apple and other device makers and carriers are no different from the agreements that many other companies have traditionally used to distribute software." Walker, *supra* note 165.

167 In late 2020, Apple introduced a Small Business Program, where Apple reduced its

commission to 15% for developers making less than one million dollars. *See, e.g.*, European Commission Press Release IP/20/1075, *Antitrust: Commission Opens Investigation into Apple Practices Regarding Apple Pay* (June 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1075 [https://perma.cc/P27P-7KGK]; European Commission Press Release IP/20/1073, *Antitrust: Commission Opens Investigations into Apple's App Store Rules* (June 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073 [https://perma.cc/YS7S-PSJS]; Digital Markets Act at 28 (¶ 57) (noting that "gatekeepers which provide access to software application stores serve as an important gateway for business users that seek to reach end users," and "the imbalance in bargaining power" between the gatekeepers and app developers, "those gatekeepers should not be allowed to impose general conditions, including pricing conditions, that would be unfair or lead to unjustified differentiation"); Complaint, Epic Games v. Google, No. 3:20-cv-05671 (N.D. Cal. Aug. 13, 2020), https://cdn.vox-cdn.com/uploads/chorus_asset/file/21759099/file0.243586135368002.pdf [https://perma.cc/KRV4-8WCG]; Complaint, Epic Games v. Apple, No. 4:20-CV-05640-YGR (N.D. Cal. Aug. 13, 2020), https://cdn2.unrealengine.com/apple-complaint-734589783.pdf [https://perma.cc/26VW-AG2T]; House Report at 219–23, 336, & 340.

168 *28 Mobile App Statistics to Know in 2020*, MindSea, https://mindsea.com/app-stats/ (last visited Feb. 28, 2021) [https://perma.cc/RZC5-3PHZ].

169 House Report at 345.

170 Jon Fingas, *Apple Earned $360 Million from Fortnite Before Pulling the Plug*, Android Authority (Aug. 14, 2020), https://www.androidauthority.com/apple-fortnite-ios-revenue-1148204/ [https://perma.cc/S2GN-DSJ7]; Epic Games, Inc. v. Apple Inc., No. 4:20-CV-05640-YGR, 2020 WL 5993222, at *11 (N.D. Cal. Oct. 9, 2020).

171 Sylvie Tremblay, *This Is Why Fortnite Is So Addictive*, Sciencing (Dec. 15, 2018), https://sciencing.com/this-is-why-fortnite-is-so-addictive-13715436.html [https://perma.cc/J6JL-9A7Q].

172 *Epic Games*, 2020 WL 5993222, at *11.

173 *Worldwide Mobile App Revenues in 2014 to 2023*, Statista (Feb. 4, 2021), https://www.statista.com/statistics/269025/worldwide-mobile-app-revenue-forecast/ [https://perma.cc/6ANF-J9V7].

174 Sara Morrison, *The Hidden Trackers in Your Phone, Explained*, Vox (July 8, 2020), https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location (noting how tracking via Software Development Kits "is firmly, perhaps inextricably, entrenched in the app ecosystem"); NY State Facebook Report at 17.

175 Morrison, *supra* note 176 ($190 billion in 2019).

176 Apple App Store, https://www.apple.com/app-store/ (last visited Feb. 28, 2021) [https://perma.cc/6QLP-E6NT].

177 CMA Final Report at ¶¶ 12 & 2.78.

178 ACCC Final Report at 7 (based on the share price for Alphabet and Facebook on June 20, 2019).

179 House Report at 175.

180 Colo. Google Compl. ¶ 8.

181 *Hearing on Online Platforms and Market Power Part 5: Competitors in the Digital Economy Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. 70 (Jan. 17, 2020) (Statement of David Heinemeier Hansson, CTO & Cofounder, Basecamp at 23), https://www.govinfo.gov/content/pkg/CHRG-116hhrg40788/pdf/CHRG-116hhrg40788.pdf; *see also* House Report at 95–98 (discussing the lack of competitive constraints on the power Apple and Google have over the software distribution marketplace on their mobile ecosystems, how Apple and Google can control which apps users discover and can install, how this dominance enables Apple and Google "to establish terms and conditions app developers have to comply with, leaving developers with the choice of complying or losing access consumers," including charging a 30% commission when users install the app).

182 House Report at 337.

183 Epic Games, Inc. v. Apple Inc., No. 4:20-CV-05640-YGR, 2021 WL 4128925, at *27 (N.D. Cal. Sept. 10, 2021).

184 House Report at 351 & 350 (noting how Apple during the pandemic began canvasing the App Store to require app developers to implement its "in-app purchases" feature, entitling Apple to take 30% of in-app sales).

185 House Report at 256–58; 268–72, 274.

186 House Report at 261:

> As the COVID-19 pandemic pushes more American shoppers online, Amazon's market power has grown. Evidence shows that Amazon is willing to use its increased market power in e-commerce during this crisis to exert pressure on suppliers and favor its own first-party products over those sold by third-party sellers. Amazon initially responded to the sudden surge in sales by refusing to accept or deliver non-essential supplies from its third-party sellers—a stance that would seem reasonable except that Amazon continued to ship its own non-essential products while restricting third-party sellers' ability to use alternative distribution channels to continue selling through Prime.

187 House Report at 287.

188 PwC, Global Top 100 companies by market capitalization (July 2019).

189 House Report at 10. By August 2020, these four companies and Microsoft comprised nearly 23% of the S&P 500 Index's total value. This was far higher than the period between 1980 and 2019 when the top five firms, on average, represented 13% of the index's total value.

190 Ufuk Akcigit et al., *Rising Corporate Market Power: Emerging Policy Issues*, Int'l Monetary Fund Staff Discussion Note, at 10 (Mar. 2021), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2021/03/10/Rising-Corporate-Market-Power-Emerging-Policy-Issues-48619 [hereinafter IMF Market Power

Report] (noting that while concentration levels and markups have increased among all broad industries, the increase in markups among firms in the healthcare and technology industries is more than three times larger than among firms in the industrials and consumer goods industries).

191 CMA Final Report at ¶ 2.80; FTC Facebook Compl. ¶ 4 (characterizing Facebook's 2019 profits of over $18.5 billion).

192 Spencer Weber Waller, *The Monopolization/abuse Offense*, 20 Loy. Consumer L. Rev. 167, 169 (2008) (noting that while Europe's Article 102 reaches exploitive abuses, such as monopoly pricing or discriminatorily high pricing by a dominant firm, it is rarely prosecuted, whereas section 2 of the Sherman Act, under the Supreme Court's construction, does not reach monopoly pricing).

193 United States v. Aluminum Co. of Am., 148 F.2d 416, 430 (2d Cir. 1945).

194 *Id.*

# 2
# Understanding the Data-opolies' Anticompetitive Playbook

So how did these data-opolies become so powerful, and how did they leverage their dominance into other markets? Some believe that these powerful platforms take advantage of preexisting market forces, such as network effects, passively. The companies' executives are, in effect, the superior surfers. They pick the right surfboard for the right wave and shift their weight and feet while riding the wave for that extra boost of acceleration and momentum. The data-opolies picked the right services—whether Google Maps, Apple iTunes, Amazon Prime, or Facebook Messenger—adjusted their services along the way, and used the underlying network effects to propel to dominance. That is legal under EU and U.S. antitrust law.

But in synthesizing the newly uncovered evidence (including the data-opolies' internal documents), a more chilling and sobering reality emerges: these companies do not use network effects passively; they can create these effects and use them offensively to wipe out potential threats. There is a pattern in (i) what markets these data-opolies expand and (ii) how they leverage their dominance into these markets. So, whether cloud computing, online shopping, or search results, we see a similar pattern of anticompetitive behavior. Rather than unrelated acts, they are part of the data-opolies' playbook to acquire and sustain a durable competitive advantage. We will explore three common tactics that the data-opolies employ:

- First, besides hoarding data to sustain their competitive advantage, the platforms employ a *nowcasting radar* to identify nascent competitive threats and opportunities, a tool that earlier monopolies lacked.
- Second is their *Acquire-Copy-or-Kill (ACK) Strategy*. Once the data-opoly identifies a nascent competitive threat, it can acquire them. If start-ups, like Snap, rebuff the acquisition, the data-opoly can use network effects offensively to copy the start-ups' innovative features. Alternatively, the data-opoly can kill them with myriad exclusionary and predatory tactics.
- Third is how the data-opolies follow a similar pattern of *colonizing the next generation of ecosystems* where we might eventually migrate, such as digital assistants and wearables. Under their *Venus Flytrap Strategy*, data-opolies open the ecosystem to attract developers, consumers, and manufacturers. After the market tips in their favor, they close the ecosystem and widen the competitive moat.

## A. The "Gift That Keeps on Giving": The Nowcasting Radar

Imagine a weapon that provides your firm with near-perfect market intelligence, where your company can identify market trends and any nascent competitive threats. Unlike earlier monopolies, Google, Apple, Facebook, and Amazon have this weapon, which we call the *nowcasting radar*.[1] A lot of data flows through their ecosystems, including (i) commercially sensitive data from app developers, merchants, and businesses who advertise on their platforms, and (ii) our personal data, such as our activity on apps and the products and services we buy online. From this data, data-opolies can see how and where we spend our time, identify trends, and target early on any potential threats to their business model or power.[2]

The internal corporate documents uncovered by Congress in its investigation of Big Tech show how these data-opolies use this data to provide themselves multiple competitive advantages.[3]

In controlling the largest online shopping platform, Amazon compiles data about us and has inside access to competitively sensitive information about the millions of sellers on its platform, their products, and their transactions with customers.[4] Amazon uses this data to identify sales and shopping trends. Amazon then copies popular-selling items and sells them under its private label. Or Amazon tells the product's manufacturer to sell the product to Amazon instead of the third-party merchant.[5] When the U.S. Congress specifically asked Amazon whether it was doing this, its Associate General Counsel testified no.[6] That representation was

false[7] and possibly perjurious.[8] A former Amazon employee told Congress, “It’s a candy shop, everyone can have access to anything they want.”[9] As Representative Pramila Jayapal, who represents Amazon’s hometown of Seattle, told Amazon’s CEO: “So you might allow third-party sellers onto your platform. But if you’re monitoring the data to make sure that they’re never going to get big enough that they can compete with you, that is the concern that the [Congressional] committee has.”[10] It is also a concern for antitrust enforcers. In late 2020, the European Commission announced its preliminary findings that Amazon abused its dominance by systemically using nonpublic, commercially sensitive information of independent sellers who sell on Amazon’s marketplace to benefit Amazon’s own competing retail businesses.[11]

To further appreciate how this near-perfect market intelligence can chill innovation and competition, consider Google’s “Lockbox” Project. The Congressional Antitrust Report recounts how Google used the data flowing through its Android mobile operating system to monitor competing apps closely:

Since at least 2012, Google has collected installation metrics for third-party apps, which it combined with data analyzing search queries.

These early documents outline the early stages of Google's "Lockbox," a project to collate data that provided Google with a range of competitor insights and market intelligence, ranging from an understanding of how installation of the Amazon app corresponded to a trend in Amazon shopping queries to a close tracking of trends relating to Candy Crush and Angry Birds.

While Lockbox began as a way to collect data on the installation of apps, Google quickly realized it could harness it to yield other insights as well. One document from 2013 identified a list of additional data points that the company desired, including "[m]ore signals (including uninstalls and device app mapping)" and "reliable and long term app usage data," for which the document noted Google Play Services could help. In short, Google began seeking out ways to collect specific usage data that enabled Google to track not just which apps a user has, but also how frequently they use the apps and for how long.

Documents obtained by the Subcommittee suggest that by 2015, Google's Lockbox data had succeeded in tracking more than just install rates. Google's internal reports show that Google was tracking in real-time the average number of days users were active on any particular app, as well as their "total time spent" in first- and third-party apps. Google subsequently used this data to benchmark the company's first-party apps against third-party apps, suggesting that Google was using Lockbox data to assess the relative strengths and weaknesses of its own offerings. Google's documents show how Lockbox furnishes Google with near-perfect market intelligence, which Google has used to inform strategic moves and potential business transactions.[12]

While Google was launching its Lockbox nowcasting radar in 2012, Facebook was internally discussing ways to significantly improve its nowcasting radar to understand whether start-ups were potential friends or foes, and like Google to "inspire [its] next moves."[13]

Facebook in 2013 acquired the Onavo Protect app to better spy on users and identify competitive threats. Ironically Facebook touted to users the app's privacy features, security alerts, and access to a virtual private network (VPN) service.[14] What Facebook did not tell the app's users was how it was using their data for "detailed insights into consumers' online activity and [to] track the popularity of rival websites and apps."[15] Facebook's self-described "early bird warning system" enabled it to identify "fast-growing apps that could potentially threaten Facebook's market position or enable it to protect and expand its dominance."[16] Australia's competition authority noted the competitive significance of this personal data:

> With such data from Onavo, Facebook had been able to effectively determine the popularity of apps and implement similar features into its own existing apps, create new apps that mirror the popular apps and purchase promising new start-ups or competing businesses.
>
> The ACCC considers that if Facebook had the ability to track consumer use of rival apps, this could have provided Facebook with a significant competitive advantage and facilitated a strategy of acquiring potential rivals, or competing suppliers with a large user base. This would have further enhanced Facebook's market power in the relevant markets.[17]

After Apple removed Facebook's Onavo from its app store in 2018, and after the Australian competition authority raised concerns about Onavo, Facebook said it would end the Onavo program.[18] It didn't. Instead, in 2019, Facebook "repurposed Onavo's source code for use in a new VPN app called 'Facebook Research' which was available as a direct download to users on both Android and iOS."[19] Facebook targeted its market surveillance app to teenagers and young adults, who, in exchange for up to $20 per month, granted Facebook access to all of their mobile app usage and browser traffic.[20] But after Apple kicked this "research" app out of its app store, Facebook stopped recruiting new users for this surveillance program.[21] But, in collecting data off of millions of websites, Facebook still has other nowcasting radars to scour "the landscape for potential competitors to eliminate, hobble, or keep out of the hands of well-resourced firms that might enhance their competitive significance."[22]

In kicking Facebook's surveillance apps out of its App Store, Apple looks like the privacy hero. But Apple is accused of using personal data from its ecosystem to advantage itself and unfairly disadvantage rivals.[23] For example, the European Commission is investigating whether Apple's control over its app store enables it to glean commercially sensitive data about what its competitors are doing. Apple's music subscription service, for example, competes against Spotify and other apps. In controlling the app store, Apple quickly learns of its rivals' offers to induce users to switch to (or remain with) their music apps.[24] In controlling the app store and any purchases of products and services offered by the rival apps, Apple has "full control over the relationship with customers of its competitors subscribing in the app."[25] So, the concern is that Apple can cut off its competitors' access to "important customer data while Apple may obtain valuable data about the activities and offers of its competitors."[26]

Consequently, the nowcasting radar is, as Facebook's Sheryl Sandberg

described Onavo, the "gift that keeps on giving."[27] The data-opolies use the "near-perfect market intelligence" *offensively* (to favor their products, services, and apps and disadvantage competing products and services) and *defensively* (to aim their sniper rifle at potential threats as well as weaker rivals).

## B. Data-opolies' Acquire-Copy-or-Kill (ACK) Strategy

Once the data-opoly identifies a nascent competitive threat, it typically employs an Acquire-Copy-or-Kill (ACK) strategy.

### 1. Acquisitions

As Facebook's CEO wrote in an internal e-mail, "it is better to buy than compete."[28] And buy they did. Since 1998, Google, Amazon, Facebook, and Apple have collectively purchased over 500 companies.[29] Google alone "purchased well over 260 companies—a figure that likely understates the full breadth of Google's acquisitions, given that many of the firm's purchases have gone unreported."[30]

The acquisition strategy helps the data-opoly maintain its dominance in at least five ways:

> *First*, it extinguishes the competitive threat and widens the protective moat around the data-opoly.[31]
> *Second*, in acquiring the maverick, the data-opoly keeps these threats "out of the hands of other firms that are well-positioned to use them to compete," including another data-opoly.[32]
> *Third*, the acquisition prevents competitors or potential competitors "from having access to next generation technology that might threaten" the data-opoly.[33]
> *Fourth*, the acquisitions can create "kill zones" by chilling other firms' incentives to enter or invest in that particular space.[34]
> *Fifth*, the acquisitions enable data-opolies to use network effects offensively and deprive rivals of gaining scale.[35]

Not one antitrust agency sought to block any of these acquisitions, which is troubling given the incriminating evidence that came out in the congressional inquiry, as well as the subsequent investigations into Facebook by the FTC and state attorneys general.[36] One wonders what the competition authorities were doing when they originally reviewed these mergers. Ultimately, we paid the price

with less competition, less investment, less innovation, and fewer choices.[37]

## 2. Copy to Deprive Scale

If the start-up rebuffs the acquisition, it could incur the data-opoly's wrath. As one market participant told Congress, "if you stepped into Facebook's turf or resisted pressure to sell, Zuckerberg would go into 'destroy mode' subjecting your business to the 'wrath of Mark.' "[38]

Sounds fanciful? Consider Snapchat's internal dossier called "Project Voldemort," which documented Facebook's various anticompetitive tactics to disadvantage the start-up.[39] In 2013, Snap rebuffed Facebook's $3 billion offer. After that, Facebook introduced the Instagram Stories feature, which "was 'nearly identical to the central feed in Snapchat, which [was] also called Stories.' "[40] Instagram Stories, within one year of its introduction, "had more daily active users (200 million) than Snapchat Stories (161 million)." By 2018, Instagram Stories had doubled the number of its users over rival Snapchat.[41] Facebook reportedly discouraged "popular account holders, or influencers, from referencing Snap on their accounts on Instagram," and Snap executives "suspected that Instagram was preventing Snap content from trending on its app."[42]

Snap illustrates how a dominant platform can use network effects offensively by copying the start-up's innovative features to deprive it of scale.[43] Even if the start-up offers better features or privacy protections, many people will not switch unless they can persuade their friends to switch.[44] Data-opolies count on this "stickiness." As an internal survey prepared for Facebook's senior management team explained:

> "[p]eople who are big fans of [Google+] are having a hard time convincing their friends to participate because . . . switching costs would be high due to friend density on Facebook."[45]

Facebook's Mark Zuckerberg had a brilliant insight. For every service and product, there are a limited number of innovative features that are immediately available. So when the data-opoly copies a rival app's innovative features, it becomes harder for users to convince their friends to switch. Here is Zuckerberg outlining his strategy:

> [T]here are network effects around social products and a finite number of different social mechanics to invent. Once someone wins at a specific mechanic, it's difficult for others to supplant them without doing something different. It's possible someone beats Instagram by building something that is better to the point that they get network migration, but this is harder as long as Instagram keeps running as a product . . . one way of looking at this is that what we're really buying is time. Even if some new competitors springs[sic] up, buying Instagram now . . . will give us a year or more to integrate their dynamics before anyone can get close to their scale again. Within that time, if we incorporate the social mechanics they were using, those new products won't get much traction since we'll already have their mechanics deployed at scale.[46]

Essentially the data-opoly cannibalizes rather than innovates.[47] It widens the "kill-zone" since few, if any, start-ups would want to invest in products and services that a data-opoly could simply copy.

## 3. Kill the Threat

If acquisitions or copying do not eliminate the threat, the data-opolies can use myriad anticompetitive means to prevent the start-up from achieving scale. A data-opoly, for example, can cut off the rivals' oxygen supply by doing the following:

- kicking the rivals off its platform (such as delisting their apps from its app store or their products),
- stealing (or what is called scraping) the rivals' content from their websites and apps,
- reducing interoperability with the rivals' apps or websites, or
- engaging in self-preferencing (where the data-opoly promotes its products and services, while making it harder for us to find and use competing offerings).[48]

You might recall the video-sharing platform Vine, whose life was as short-lived as its six-second videos. Many reasons contributed to the app's failure, but a significant one was Facebook. The whole purpose of a video-sharing platform is to share videos with friends and family easily. To do so, Facebook allows users to easily find their Facebook friends on other platforms, including Twitter's Vine platform, through Facebook's "Find Contacts" feature. The interoperability helps Facebook users easily find their friends on this new platform, and it helps the new platform expand (and take advantage of the network effects). But by early

2013, Facebook, through its nowcasting radar Onavo, was already tracking internally Vine's upward trajectory.[49] Recognizing "that access to its social graph provided other applications with a tool for significant growth," Facebook began excluding nascent threats from its social graph.[50] With its CEO's approval, Facebook removed Vine's access to its "Find Contacts" feature, thereby making it harder for Facebook users to find their friends on Vine. Consistent with its ACK strategy, Facebook's Instagram copied Vine's short-video feature. In 2016, Twitter discontinued Vine.[51]

As the antitrust enforcers alleged, Facebook, for many years, wielded interoperability as a club: if an app or website dared to compete with Facebook by providing personal social networking, offering functions that were similar to Facebook's, offering mobile messaging, or helping any other app that competed against Facebook, then it was cut off,[52] effectively killing the potential threat.[53]

Another popular tactic is self-preferencing, whereby the data-opolies favor their inferior products and services over better, more relevant offerings.[54] When a platform only distributes content, goods, or services, it has little, if any, incentive (absent bribes, kickbacks, or payments) to favor one company over another. That changes when the platform vertically integrates and begins offering products under its label (Amazon), specialized search offerings (such as Google's flights, hotels, or restaurant reviews), and its own apps (such as Apple music). Now the company may favor its offerings while disadvantaging rivals'.

The best-documented example involves Google. The company internally recognized that its "comparison shopping" service was inferior.[55] As one Google employee observed, "if Google ranked its own content according to the same criteria that it applied to competitors, 'it will never rank.' "[56] So, Google countermanded its search engine algorithm. It favorably positioned and displayed on the first page of its search results Google Shopping, its comparative shopping service. It demoted its rivals' superior offerings to the fourth page of search results or even further down.[57] Why? This self-preferencing dries up nearly all the traffic to the rivals' websites.

To see why, suppose you do a Google search on your personal computer and get 25 pages of results. Which results do you typically click? Most likely, those on the first page. Nearly 95% of all clicks, the European Commission found, were the top 10 listings on the first page of Google's search results. Few people venture to the second page (the top result on page 2 received only 1% of all clicks).[58] Far fewer venture to the third and fourth pages (which received less

than 1% of all clicks).[59] Even on the first page, ranking is critical. Simply moving the top result (even if it is more relevant) to the third position reduces the number of clicks "by about 50%."[60] Demoting a rival to the fourth page of results is like secreting them to online Siberia. Rival comparative shopping websites in the United Kingdom saw their traffic decline by 85%; German websites saw a 92% decline in traffic—basically from a million visitors a day to 80,000.[61] The Commission fined Google €2.42 billion and ordered it to not engage in self-preferencing, which the European general court affirmed in 2021.

Self-preferencing is "network effects in reverse."[62] By reducing search traffic to its rivals' comparison-shopping services or restaurant reviews websites (like Yelp), Google causes them to have fewer consumers, which leads to fewer listings and less revenue, which leads to reduced investment—which causes traffic to decline further.[63] To avoid this downward spiral brought about by Google's self-preferencing, the rivals must recover their lost traffic. Often their only option is by advertising on Google with paid search ads.[64] By forcing its competitors to advertise on its platforms, Google saps its rivals' profits while gleaning additional competitively sensitive data about its rivals, thereby strengthening the data-opoly's nowcasting radar.[65]

But it gets worse. To further thwart rivals from capturing more ad revenues, Google, at times, scraped (basically stole) their sites' content. Google gave these third-party websites a Hobson's choice: either "permit Google to take their content, or else be removed from Google's search results entirely."[66] Removal from Google's search results is a death sentence to many businesses. As one market participant testified in the congressional antitrust hearings, Yahoo, Bing, and DuckDuckGo all could drop his company "from their listings tomorrow and we'd barely notice," but "[w]e lose our listing in Google and we may go out of business."[67]

Ultimately, we pay the price from the data-opolies' self-preferencing. Throughout the congressional investigation, numerous third parties reported how:

> self-preferencing and discriminatory treatment by the dominant platforms forced businesses to lay off employees and divert resources away from developing new products and towards paying a dominant platform for advertisements or other ancillary services. They added that some of the harmful business practices of the platforms discouraged investors from supporting their business and made it challenging to grow and sustain a business even with highly popular products. Without the opportunity to compete fairly, businesses and entrepreneurs are dissuaded from investing and, over the long term, innovation suffers.[68]

## C. Colonizing the Next-Generation Ecosystems

The poet Delmore Schwartz complained to a friend about being mistreated by people they both knew. His friend replied, "You're a paranoid." The poet responded, "Even paranoids have enemies . . ."[69]

So too, data-opolies are paranoid of firms, which could become threats.[70] They recognize that we can shift from their existing platforms to new ones, which also exhibit extreme returns to scale and multiple data-driven network effects. So when Facebook took over the campus of the former tech firm Sun Microsystems, Zuckerberg said he kept Sun's "sign out front, on the back of ours, to remind us that things change fast in tech. I've long believed that the nature of our industry is that someday a product will replace Facebook. I want us to be the ones that build it, because if we don't, someone else will."[71]

One fear is missing disruptive market trends. By 2014, for example, many U.S. adults were spending more time on their smartphones (on average 34 hours per month) than on their personal computers (27 hours per month on average).[72] Microsoft monopolized the personal computer operating system market for decades. But it also developed an operating system for handheld personal computers in 1996, a decade before Apple's revolutionary launch of its iPhone in 2007[73] and the first Android phone (T-Mobile G1) in 2008. But the monopolist, according to a former Nokia engineer, "underestimated Google and the value of services like Gmail, search, and Maps on mobile."[74] When Microsoft sought to catch up with Apple's and Android's mobile operating systems with its Windows 10 smartphone,[75] it was too late. The Windows phone had too few customers to attract app developers and thus had too few apps to attract new customers.[76]

So too, we'll likely migrate from our smartphones, where Google and Apple control the leading operating systems, and spend more time on other platforms. In its 2019 annual report, Google warned how users are increasingly shifting

their access to the internet through devices other than desktop computers, "including mobile phones, smartphones, laptops and tablets, video game consoles, voice-activated speakers, wearables, automobiles, and television set-top devices."[77] One concern for Google is that its "products and services may be less popular on these new interfaces."[78] Facebook echoes this concern in its 2019 annual report[79] and internally.[80] Thus, the data-opolies do not build products or platforms but "ecosystems." As Google's CEO told investors in 2019, "If you look at an ecosystem like Android, this is what we do. And so that's going to be a focus for us."[81]

A key lesson from the data-opolies' playbook is to be among the first to expand their ecosystems to where we might migrate and use the network effects offensively to advantage themselves while excluding others. Figure 2.1 reflects the other ecosystems Google is eying:

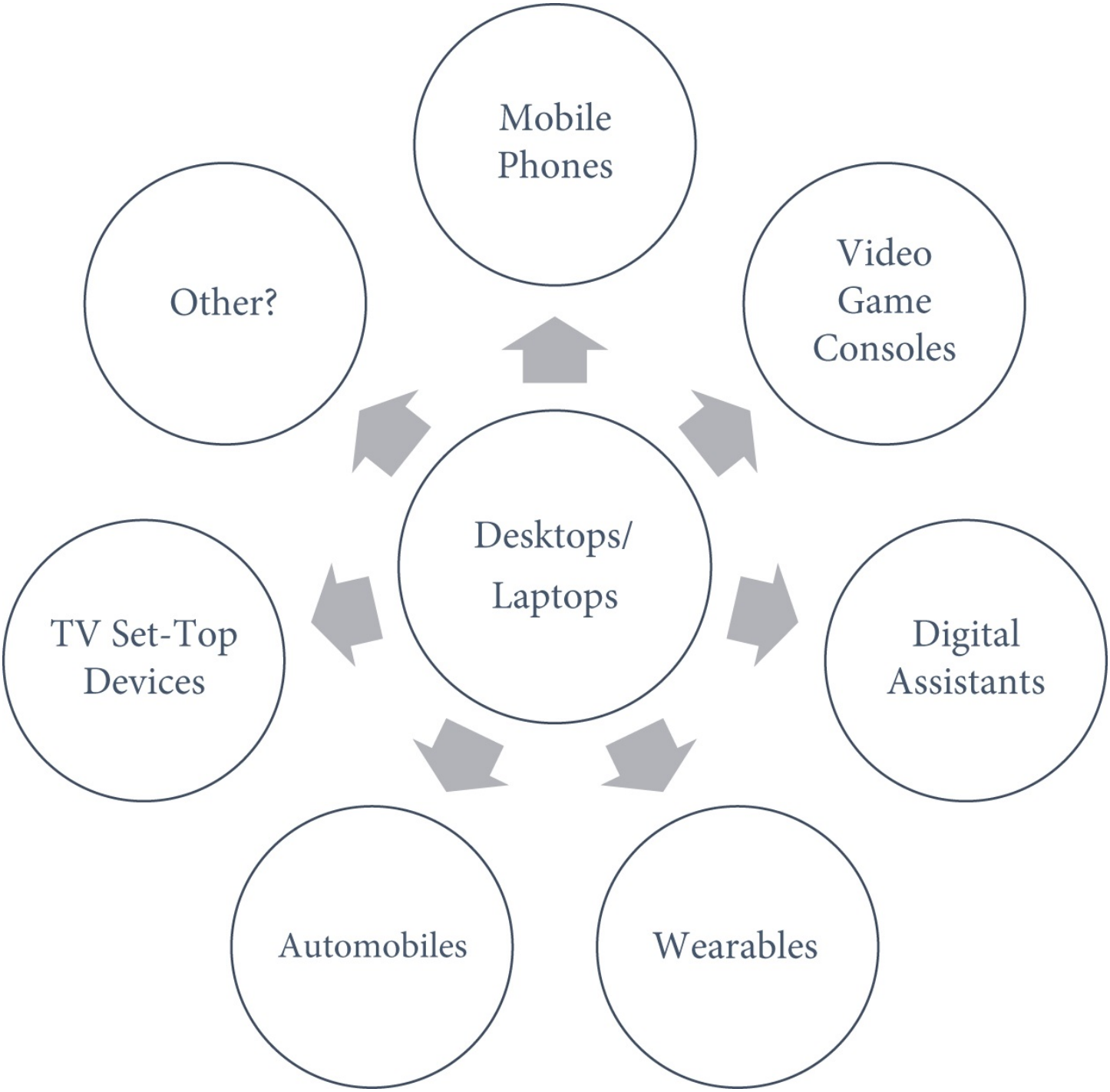


**Figure 2.1** Other Ecosystems Google is Eying

In colonizing these ecosystems, the data-opolies often deploy a Venus Flytrap Strategy. The Venus Flytrap (*Dionaea muscipula*) is a well-known carnivorous plant native to the Carolinas.[82] To attract insects, the herb secretes a sweet sap. Once the plant's leaves snap shut, the entrapped insects have little chance to escape. "The prey would need to overpower the 'escaping' force, which is very strong and can reach up to 4 N."[83]

So too, the data-opolies open their newly colonized platforms with

inducements to attract advertisers, app developers, users, and smart device manufacturers. After dominating that ecosystem, the data-opoly snaps the once open-source environment shut: the data-opoly imposes upon the entrapped sellers, developers, advertisers, and users anticompetitive terms and fees.[84] To dominate its mobile phone ecosystem, Google deployed the Venus Flytrap Strategy in the following three steps, as the United States alleged:

> In 2007, Google released the Android code for free under an open-source license. Being "open source" means that anyone can access the source code and use it to make their own, modified operating system—a "fork." This was key to Android's adoption.
>
> First, Google's apparent lack of control over an open-source operating system attracted skeptical manufacturers and carriers of mobile phones to use Android instead of the other choices then available. As the Android team leader observed to Google's board of directors, "Google was historically seen as a threat" to these distributors. But an open-source model suggested that they—and not Google—would ultimately retain control over their devices and the app ecosystem on those devices.
>
> Second, once enough major distributors agreed to use Android, the operating system attracted developers looking for wide distribution of their apps. As more app developers focused their efforts on designing Android apps, Android became more attractive to consumers, which in turn led even more developers to design for Android. The result was a must-have ecosystem of Android apps.
>
> Third, to help the Android ecosystem achieve critical mass and to advance the network effects, Google "shared" its search advertising and app store revenues with distributors as further inducement to give up control. As one senior executive explained about Android Market, an earlier name for Google's app store, "Android Market is a bitter pill for carriers, and generous revenue share is the sugar that makes it go down smoother." In other words, beginning over ten years ago, Google used revenue sharing to attract partners to Android; and Google uses revenue sharing to keep them locked in today.
>
> By 2010, the Android team leader noted that "Android is poised for world domination —the success story of the decade." He was right; the strategy worked.[85]

Once Android became dominant, running on approximately 75% of the world's mobile devices,[86] Google closed its ecosystem and collected monopoly rents and personal data from the entrapped developers and smartphone manufacturers. If smartphone manufacturers wanted interoperability with Google's apps and wanted Google's app store loaded on their phones (a must for any smartphone to be commercially viable), they had to use Google's version of Android (not a competing version). They also had to preload and feature Google's search

engine, browser, and other apps (and not competitors'). Google also imposes an app tax on developers (ranging between 15 and 30%)[87] and is alleged to require apps to hand over their users' personal data.[88]

Google repeated the Venus Flytrap Strategy in other ecosystems. Its search engine, once "a 'turnstile' to the rest of the web," is now "a 'walled garden' that increasingly keeps users within its sites."[89]

For years, Google Maps was open. It "offered a free tier of the Maps API [application programming interface], incentivizing developers to build their apps with Google Maps."[90] After acquiring its only significant rival, Waze, Google controlled an estimated 81% of the market for navigation mapping services.[91] With its dominance secured, Google in 2018 closed this ecosystem and changed its pricing plan for its core mapping APIs[92]—resulting in an effective price increase of 1,400%.[93]

Google is now colonizing the next generation of ecosystems to ensure that its search engine will be the preferred (or only) option.[94]

Consider smart speakers, which will connect with many smart household appliances that we will eventually buy. As Google internally recognizes, the "[v]oice platform will become the future of search."[95] Smart speakers by 2020 already had a "35% U.S. household penetration," which was predicted to grow "to 75% by 2025."[96] As users migrate to digital assistants and voice-activated speakers, the leading platforms will capture more of our attention and data and have many opportunities to predict and manipulate our behavior.[97]

Just as we saw with smartphones, the aim is to use network effects offensively by rapidly increasing the user base to attract more developers and smart appliance manufacturers to its ecosystem. Google is wooing developers and smart appliance manufacturers, capturing already nearly 70 categories of smart devices, including "water purifiers, refrigerators, pressure cookers, lights, fans, doors, windows, and even bathtubs," already working with its platform.[98]

Besides using our voice commands for search, these speakers will likely become the essential platform for our home's many smart appliances.[99] This is of apparent interest to Amazon, whose goal, according to a senior vice president, "is to try to create a kind of open, neutral ecosystem for Alexa . . . and make it as pervasive as possible."[100] So Amazon is also busily attracting developers and smart appliance manufacturers to develop skills for its Alexa devices in 23 areas, including the following:

- asking your credit card to make payments (which is among Alexa's 576 Business & Finance skills),
- helping you learn a language, or inspiring you with a passage from the Bible (among Alexa's 3000 + Education & Reference skills),
- picking a restaurant or choosing a meal for you (among Alexa's 573 Food & Drink skills), and
- asking WebMD about sensitive health issues (among Alexa's 545 Health & Fitness skills).[101]

Consistent with the Venus Flytrap Strategy, Amazon "does not charge third-party device manufacturers for access to its integration services, which promotes rapid adoption of Alexa in a larger number of devices, which, in turn, drives greater adoption by consumers."[102] But we can see where this is going, especially with Google and Amazon patenting "voice-sniffer algorithms" that listen to our conversations.[103] Amazon's patent enables smart devices to store and process, without any prompts, "both positive and negative triggers [that] can be used to tailor the user's advertising profile; if a negative trigger word is used, such as 'hate,' this will indicate that the user is unlikely to respond well to that subject being advertised."[104]

As of January 2020, Amazon controlled over half the U.S. smart speaker market at 53%, followed by Google at 30.9%, Apple at 2.8%, and Sonos at 4.7%.[105]

Ordinarily, a smart speaker can have multiple digital assistants, some of which may be more privacy focused than Google Home, Apple's Siri (which relies on Google for search), and Amazon's Alexa. Rather than saying "Hey Google" on our Sonos speaker, we could ask a more privacy-focused assistant to find the health risks of a particular medicine. This "multi-homing," while technologically feasible, would also threaten Google's search monopoly and its hold on our attention and data.[106] So, Google prohibits multi-homing—even on third-party speakers. Google's ban is anticompetitive, as the CEO of the smart speaker Sonos told Congress:

> Google has gone so far as to dictate what features we can have in our products. To take a particularly egregious and anti-consumer example, Sonos has developed the technical ability to host multiple voice assistants on its smart speakers simultaneously, which we call voice concurrency. In a product using this technology, you can call upon whichever voice assistant you want (including more than just the two dominant assistants) and the system will channel you into your chosen service automatically. This is a feature that customers told us they wanted and which requires complex engineering, and we worked hard to invent it. But Google demanded as a condition of having Google Assistant in our products that we never allow concurrency with another general voice assistant.[107]

Google is alleged to have prevented smart device manufacturers from responding to Alexa or more privacy-friendly digital assistants.[108] To further foreclose other voice assistants, Google has entered into partnerships with mobile devices, home appliances (such as smart televisions and smart speakers), and carmakers.[109]

Meanwhile, Amazon leverages its dominance in online shopping to promote its smart speakers (pricing them, at times, below cost) and prevent rivals from advertising theirs.[110]

The point of this exclusionary and predatory behavior is to hinder rivals from attracting users and developers and channel the network effects in the data-opoly's favor. Eventually, we are left with one or two data-opolies controlling all the smart appliances—whether our vacuum cleaner or refrigerator—and our data as well.[111] It is unclear that many of us even want these smart devices from Silicon Valley.[112] But even if one could avoid Google, Siri or Alexa during one's lifetime, their digital assistant will likely be beside the hospital bed to record any dying declaration.[113]

Many of us are, or will soon be, driving internet-connected cars with a digital assistant. So, the data-opolies want to ensure that their services (such as search engine, maps, and digital assistant) are the default in our next car. Why leave it up to competition, when Google can use its anticompetitive playbook. As the states allege in their antitrust complaint:

> Google's strategy with automobiles follows its playbook in mobile. Google offers carmakers a free Android operating system with a bundle of Google proprietary applications, including Google Assistant, Google Play Store, and Google Maps, known as Google Automotive Services, or "GAS." Carmakers, in exchange for the operating system and Google's proprietary bundle of applications, agree to restrictive and exclusionary terms, providing Google de facto exclusivity for Google Assistant and therefore its general search services within cars, further protecting Google from competition. Had Google not taken control over this interface, rival voice assistants like Alexa or new entrants could enable the use of different underlying general search engines, including relying on multiple kinds of search.[114]

After Toyota announced that it will include Android Auto in its 2020 vehicles, Google told investors, "all of the top 10 car makers now support Android Auto."[115]

As we increasingly rely on wearables, Apple and Google (after acquiring Fitbit in 2021) will likely dominate that ecosystem. The personal health data, especially for Google, could open several avenues (using health as a form of vertical search) and reinforce its dominance in behavioral advertising. So to capture this segment and our data, Google, the United States alleged in its Complaint, "has similarly restrictive agreements with smart watch manufacturers: its agreements to license Google's 'free' smart watch operating system (Wear O.S.) prohibit manufacturers from preinstalling any third-party software, including any rival search services."[116]

To the extent we are not watching videos or shows on their platforms, the data-opolies have expanded their ecosystem to television set-top devices, where Google's Android-powered devices, Amazon Fire, and Apple TV, are already seeking to capture the traffic and affect our viewing. For example, as they rely on behavioral advertising, Roku's and Amazon's Fire streaming devices are cheap alternatives to smart TVs.[117] So, as we saw, Amazon tracks viewers on 687 of the top 1,000 Amazon Fire TV channels; the dominant trackers on Roku's devices are Google and Facebook (with "Google's doubleclick.net appearing on 975 of the top 1,000 Roku channels).[118] This surveillance increases the data-opolies' competitive advantage.

Facebook views the metaverse as the successor to the mobile Internet, so its goal is to transition from a social media company to a metaverse company. So much so, the company announced in 2021 its new company name "Meta." The company is spending billions to develop a platform and app store for virtual reality apps.[119] Apple and Microsoft are also seeking to develop metaverse

platforms.[120]

By quickly colonizing these next-generation ecosystems, the data-opolies can leverage their monopoly power, and use the economies of scale and network effects offensively to improve the odds that they remain on top, widen their data and attention advantage over rivals, and hedge against potential dynamic disruption.[121] Of course, not every offering by a data-opoly is a hit (as the "KilledbyGoogle.com" website attests). But many of their failures were not ecosystems where we were expected to migrate and where the data-opolies could use network effects offensively. Granted, the data-opolies could miss a trend, and some new data-opoly could occupy Facebook's campus (keeping the Sun Microsystems sign as a warning). But with near-perfect market surveillance from their nowcasting radars, the odds of this happening are low. If some new ecosystem is grabbing more of our attention and data, expect the data-opolies to either acquire, copy, or kill it.[122]

## D. Reflections

Data-opolies can use their power both offensively (by giving themselves an advantage over competitors and undermining competition in neighboring markets)[123] and defensively (to protect their most profitable services from competition).[124] Smaller firms, to survive, must carefully navigate to avoid the data-opolies' crosshairs. Who would want to storm the beachhead knowing that their movements are being watched and that every step brings them closer to the sniper rifle? The results, as venture capitalists described to Congress, are "innovation kill zones" that insulate "dominant platforms from competitive pressure simply because investors do not view new entrants as worthwhile investments."[125] Ultimately millions of third-party sellers, app developers, and website publishers live in fear, as their economic livelihood depends on a few data-oplies' "unaccountable and arbitrary power."[126]

As the innovation kill zone spreads, the data-opolies will unleash their prediction and manipulation tools in other industries, where they can reap greater profits. Consider health care. Insurers can eliminate uncertainty by monitoring, shaping, and influencing behavior.[127] National health expenditures in the United States were approximately 18% of GDP in 2020 (up from 5% in 1960).[128] The data-opolies, not surprisingly, are expanding into the health fields[129] while lobbying against state-level protections of bio-metric data and privacy.[130] As one

market participant noted, “These companies have to enter the health space to improve their valuations—there’s nowhere else they can go.”[131]

Few, if any, companies can now effectively challenge the data-opolies’ surveillance and manipulation tools with countermeasures to protect our privacy and autonomy.[132] With the data-opolies’ power increasing during the pandemic, absent policy interventions, they will extend their long shadow, acquiring, copying, or killing off potential threats, chilling innovation, taxing businesses reliant on their platforms, and extracting even more data to improve their algorithms’ ability to manipulate us. The good news is that policymakers are taking notice.

---

1 Maurice E. Stucke & Allen P. Grunes, Big Data and Competition Policy ¶ 18.28 (2016).

2 *See, e.g.*, Majority Staff of H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial and Administrative Law, Report and Recommendations: Investigation of Competition in Digital Markets (2020), https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429 [https://perma.cc/29LN-L4BL] [hereinafter House Report] at 160 (noting how Facebook “used its data advantage to create superior market intelligence to identify nascent competitive threats and then acquire, copy, or kill these firms,” how Facebook “selectively enforced its platform policies based on whether it perceived other companies as competitive threats,” and how Facebook “advantaged its own services while weakening other firms”), 43 (noting how “[p]ersistent data collection can also create information asymmetries and grant firms access to non-public information that gives them a significant competitive edge” including enabling “the dominant platforms to track nascent competitive threats”), 217 (finding that “Android gives Google unparalleled access to data on its users and developers,” which “includes information that Google can monetize through its ad business, as well as strategic intelligence that lets Google track emerging competitors and general business trends”); Complaint, Colorado v. Google, No. 1:20-cv-03715-APM (D.D.C. Dec. 17, 2020), https://coag.gov/app/uploads/2020/12/Colorado-et-al.-v.-Google-PUBLIC-REDACTED-Complaint.pdf [hereinafter Colo. Google Compl.] ¶¶ 53 (alleging how “by virtue of its monopoly power, Google extracts from some specialized vertical providers massive amounts of proprietary customer data that Google can then use to compete against them”) & 15 (noting how internal Google communications “reveal that Google exploits information asymmetries and closely tracks real-time data across markets, which—given Google’s scale—provide it with near-perfect market intelligence”).

3 House Report at 379.

4 European Commission Press Release IP/20/2077, Antitrust: Commission Sends Statement of Objections to Amazon for the Use of Non-public Independent Seller Data and Opens Second Investigation into Its E-commerce Business Practices (Nov. 10, 2020),

https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077 [hereinafter 2020 EC Amazon Press Release] (noting how Amazon "has access to non-public business data of third party sellers such as the number of ordered and shipped units of products, the sellers' revenues on the marketplace, the number of visits to sellers' offers, data relating to shipping, to sellers' past performance, and other consumer claims on products, including the activated guarantees"]; House Report at 283. The company is also accused of using data from its investment fund for start-ups to help develop competing products. Dana Mattioli & Cara Lombardo, *Amazon Met with Startups About Investing, Then Launched Competing Products*, Wall St. J. (July 23, 2020), https://www.wsj.com/articles/amazon-tech-startup-echo-bezos-alexa-investment-fund-11595520249.

5 2020 EC Amazon Press Release; House Report at 275–79 (hearing during its investigation "repeated concerns that Amazon leverages its access to third-party sellers' data to identify and replicate popular and profitable products from among the hundreds of millions of listings on its marketplace" to "copy the product to create a competing private-label product" or "identify and source the product directly from the manufacturer to free ride off the seller's efforts, and then cut that seller out of the equation").

6 House Report at 277 (Amazon employee testified: "We do not use [third-party sellers'] individual data when we're making decisions to launch private brands.").

7 Dana Mattioli, *Amazon Scooped Up Data from Its Own Sellers to Launch Competing Products*, Wall St. J., Apr. 23, 2020, https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015; House Report at 277.

8 Letter to Amazon's CEO Andy Jassy from Representatives Jerrold Nadler et al., dated Oct. 18, 2021, https://judiciary.house.gov/uploadedfiles/letter_-_amazon_misrepresentations_-_10.18.21.pdf; House Report at 253 (noting how several senior members of the House Judiciary Committee told the company that "statements Amazon made to the Committee about the company's business practices appear to be misleading, and possibly criminally false or perjurious"). When confronted about its earlier representation, Amazon's CEO "could only respond: 'I can't answer that question yes or no . . . we have a policy against using seller-specific data to aid our private-label business, but I can't guarantee you that that policy has never been violated.' " House Report at 278.

9 House Report at 279.

10 Jason Del Rey, *Jeff Bezos's Antitrust Grilling Was a Reminder of Amazon's Power over Its Sellers*, Vox (July 29, 2020), https://www.vox.com/recode/2020/7/29/21346584/jeff-bezos-amazon-antitrust-hearing-congressional-testimony-power-to-make-or-break-small-merchants.

11 2020 EC Amazon Press Release.

12 House Report at 218 (internal footnotes omitted).

13 House Report at 161 (internal Facebook document stating "I keep seeing the same suspects (instagram, pinterest, . . .) [sic] both on our competitive radar / platform strategy as wins . . . I think having the exact data about their users [sic] engagement, value they derive from [Facebook] . . . would help us make more bold decisions on whether they are friends or foes. Back to your thread about 'copying' vs. 'innovating' we could also use this info to

inspire our next moves.”).

14 Australian Competition and Consumer Commission, Digital Platforms Inquiry—Final Report (2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report [https://perma.cc/M36S-YQJ4] [hereinafter ACCC Final Report] at 81 (to attract users, Facebook highlighted its app’s privacy features: “Onavo Protect for iPhone and iPad helps keep you and your data safe when you go online, by blocking potentially harmful websites and securing your personal information”); Sam Schechner et al., *EU Deepens Antitrust Inquiry into Facebook’s Data Practices*, Wall St. J. (Feb. 6, 2020), https://www.wsj.com/articles/eu-deepens-antitrust-inquiry-into-facebooks-data-practices-11580994001; Sam Schechner & Parmy Olson, *Facebook Feared WhatsApp Threat Ahead of 2014 Purchase, Documents Show*, Wall St. J. (Nov. 6, 2019), https://www.wsj.com/articles/facebook-feared-whatsapp-threat-ahead-of-2014-purchase-documents-show-11573075742 (discussing internal Facebook documents that reveal how Facebook used its strength in monitoring and controlling data flows to help it buy WhatsApp, the world’s most popular messaging app); Georgia Wells & Deepa Seetharaman, *Snap Detailed Facebook’s Aggressive Tactics in ‘Project Voldemort’ Dossier*, Wall St. J. (Sept. 24, 2019), https://www.wsj.com/articles/snap-detailed-facebooks-aggressive-tactics-in-project-voldemort-dossier-11569236404.

15 ACCC Final Report at 83.

16 House Report at 161–62; *see also* Complaint, Federal Trade Commission v. Facebook, No. 1:20-cv-03590-CRC (D.D.C. Dec. 9, 2020), https://www.ftc.gov/enforcement/cases-proceedings/191-0134/facebook-inc-ftc-v [https://perma.cc/8GRR-9566] [hereinafter FTC Facebook Compl.] ¶ 75 (alleging that by acquiring Onavo, Facebook “obtained control of data that it used to track the growth and popularity of other apps, with an eye towards identifying competitive threats for acquisition or for targeting under its anticompetitive platform policies,” and as a December 2013 internal slide deck noted: “With our acquisition of Onavo, we now have insight into the most popular apps. We should use that to also help us make strategic acquisitions.” Facebook “also used Onavo data to generate internal ‘Early Bird’ reports for Facebook executives, which focused on ‘apps that are gaining prominence in the mobile eco-system in a rate or manner which makes them stand out.’ ”); Complaint ¶ 146, New York v. Facebook, No. 1:20-cv-03589-JEB (D.D.C., Dec. 9, 2020), https://ag.ny.gov/press-release/2020/attorney-general-james-leads-multistate-lawsuit-seeking-end-facebooks-illegal [https://perma.cc/NLY2-MF6A] [hereinafter States Facebook Compl.].

17 ACCC Final Report at 83.

18 ACCC Final Report at 82.

19 ACCC Final Report at 83.

20 ACCC Final Report at 83.

21 ACCC Final Report at 83 (noting that “it has been reported that existing Facebook Research studies will continue to operate”).

22 States Facebook Compl. ¶¶ 181–82; *see also* House Report at 148 (discussing how 8.3 million distinct websites “interconnecting with the Facebook Platform” gave “the company

the ability to prioritize access to its social graph—effectively picking winners and losers online" and how these "tools also gave Facebook advanced data insights into other companies' growth and usage trends," such as "a daily report on metrics for Facebook Login included daily and monthly active users for companies interconnecting with Facebook, referral traffic, and daily clicks, among other metrics") & 162 (noting how in acquiring Giphy, a platform for sharing GIFs online and through messaging apps, for $400 million in May 2020, Facebook would gain "competitive insights into other messaging apps"); FTC Facebook Compl. ¶ 75 (alleging that Facebook "continues to track and evaluate potential competitive threats using other data").

23 Coalition for App Fairness, *Issue: The App Store Is Ruled by Anti-competitive Policies*, https://appfairness.org/issues/anti-competition/ (last visited Mar. 1, 2021) [https://perma.cc/E38B-MBL3].

24 European Commission Press Release IP/20/1073, Antitrust: Commission Opens Investigations into Apple's App Store Rules (June 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073 [hereinafter EC Apple Press Release].

25 EC Apple Press Release, *supra* note 24.

26 EC Apple Press Release, *supra* note 24; *see also* House Report at 363 & 365.

27 States Facebook Compl. ¶ 147.

28 FTC Facebook Compl. ¶ 72.

29 House Report at 392.

30 House Report at 174.

31 House Report at 11, 149 (noting how Facebook's "internal documents indicate that the company acquired firms it viewed as competitive threats to protect and expand its dominance in the social networking market" and how "Facebook's senior executives described the company's mergers and acquisitions strategy in 2014 as a 'land grab' to 'shore up our position' ").

32 States Facebook Compl. ¶ 185.

33 States Facebook Compl. ¶ 185.

34 House Report at 49 (noting study "that in the wake of an acquisition by Facebook or Google, investments in startups in the same space 'drop by over 40% and the number of deals falls by over 20% in the three years following an acquisition' ") (quoting Raghuram Rajan, Sai Krishna Kamepalli, & Luigi Zingales, *Kill Zone* at 5 (Univ. Chicago Becker Friedman Inst. Econ., Working Paper No. 2020-19), https://ssrn.com/abstract=3555915 [https://perma.cc/XL2B-7R6K]); *see also* Ufuk Akcigit et al., *Rising Corporate Market Power: Emerging Policy Issues*, Int'l Monetary Fund Staff Discussion Note, at 7 (Mar. 2021), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2021/03/10/Rising-Corporate-Market-Power-Emerging-Policy-Issues-48619 [hereinafter IMF Market Power Report] (finding that "M&As by dominant firms are associated with lower business dynamism at the industry level, with acquiring firms increasing their market power following the transaction and competitors' growth and research and development taking a hit").

35 House Report at 143. Facebook's CEO told the company's Chief Financial Officer in 2012 that network effects and winner-take-all markets were a motivating factor in acquiring competitive threats like Instagram, and stressed the competitive significance of having a first-mover advantage in terms of network effects in acquiring WhatsApp. In the context of market strategies for competing with the then independent startup WhatsApp, Mr. Zuckerberg told the company's growth and product management teams that "being first is how you build a brand and a network effect." *Id.*

36 Indeed, the FTC and DOJ often failed to investigate these mergers in any detail by even requesting additional documents and information from the parties. *See*, *e.g.*, House Report at 11 ("In the overwhelming number of cases, the antitrust agencies did not request additional information and documentary material under their pre-merger review authority in the Clayton Act, to examine whether the proposed acquisition may substantially lessen competition or tend to create a monopoly if allowed to proceed as proposed. For example, of Facebook's nearly 100 acquisitions, the Federal Trade Commission engaged in an extensive investigation of just one acquisition: Facebook's purchase of Instagram in 2012.").

37 IMF Market Power Report at 6–8; States Facebook Compl. ¶ 185.

38 States Facebook Compl. ¶ 6.

39 Wells & Seetharaman, *supra* note 14.

40 House Report at 164.

41 House Report at 164–65.

42 Wells & Seetharaman, *supra* note 14.

43 House Report at 363 & 365 (noting how developers "alleged that Apple abuses its position as the provider of iOS and operator of the App Store to collect competitively sensitive information about popular apps and then build competing apps, or integrate the popular app's functionality into iOS" and its double standard, where "the Apple Developer Agreement provides Apple the right to replicate third-party apps," but "Apple's Guidelines direct developers not to 'copy another developer's work' and threaten removal of apps and expulsion from the Developer Program for those that do"); FTC Facebook Compl. ¶ 91; Betsy Morris & Deepa Seetharaman, *The New Copycats: How Facebook Squashes Competition from Startups*, Wall St. J. (Aug. 9, 2017), https://www.wsj.com/articles/the-new-copycats-how-facebook-squashes-competition-from-startups-1502293444; Roger McNamee, Zucked: Waking Up to the Facebook Catastrophe 63 (2019) (noting that "Facebook's secret sauce was its ability to imitate and improve upon the ideas of others, and then scale them").

44 FTC Facebook Compl. ¶¶ 65–66.

45 House Report at 145 (noting how in 2012, Facebook internally recognized that people's significant time investment on Facebook building their identity and connections on the platform increased the company's "stickiness"); *see also* States FTC Compl. ¶ 42.

46 House Report at 143.

47 Reed Albergotti, *How Apple Uses Its App Store to Copy the Best Ideas*, Washington Post (Sept. 5, 2019), https://www.washingtonpost.com/technology/2019/09/05/how-apple-uses-its-app-store-copy-best-ideas/ [https://perma.cc/QEP5-KQH7].

48 *See, e.g.*, European Commission, Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) at 2 (Dec. 15, 2020), https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf [https://perma.cc/G87S-Q88U] [hereinafter Digital Markets Act] (noting how the enforcement experience under EU competition rules, numerous expert reports and studies and the results of the European Commission's Open Public Consultation show that "a few large digital platforms act as gateways for business users to reach their customers and vice-versa"; and "gatekeeper power of these large digital platforms is often misused by means of unfair behaviour vis-à-vis economically dependent business users and customers"); House Report at 184–87 (Google's scraping), 187–93 (Google's self-preferencing), 283, 311–13, 326, 330 (Amazon's self-preferencing), 362–65 (Apple's self-preferencing), 326 (Amazon degrading interoperability to eliminate cross-platform products with Amazon-only AWS products), & 375 (Apple limiting interoperability "by restricting how digital voice assistants work on Apple devices and how Siri works with non-Apple devices, and by using Siri to guide users to its own products and services"); European Commission Press Release IP/17/1784, Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service (June 27, 2017), https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784 [hereinafter EC Google Shopping Press Release].

49 UK Disinformation and 'Fake News': Final Report, Feb. 18, 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179106.htm ¶¶ 112 & 113 (discussing a Facebook presentation, titled "Industry Update," given on Apr. 26, 2013, showing market analysis driven by Onavo data, comparing data about apps on users' phones and mining that data to analyze Facebook's competitors, including Vine, Twitter, Path, and Tumblr).

50 House Report at 163 & 166–70 (discussing how Facebook weaponized access to its platform, and how a former employee who handled Facebook's platform management said that Facebook unevenly enforced its platform policies based on the degree of another firm's competition with Facebook and whether it could extract concessions from other firms. According to this former employee, Facebook was primarily concerned with whether a company was "a competitive threat," and it "was biasing its enforcement actions against [firms] they saw as competitors").

51 UK Competition & Markets Authority, Online Platforms and Digital Advertising Market Study: Market Study Final Report ¶ 3.231 (July 1, 2020), https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digit [https://perma.cc/DA5V-RHA5] [hereinafter CMA Final Report]; Damian Collins M.P., Chair of the Digital, Culture, Media, and Sport Committee of the UK Parliament, Note: Summary of Key Issues from the Six4Three Files, https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf; Chris Hughes, *It's Time to Break Up Facebook*, N.Y. Times (May 9, 2019),

https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html [https://perma.cc/4ABN-LN7M] (noting how Facebook's decision hobbled Vine).

52 FTC Facebook Compl. ¶¶ 23 ("In order to communicate with Facebook (i.e., send data to Facebook Blue, or retrieve data from Facebook Blue) third-party apps must use Facebook APIs. For many years—and continuously until a recent suspension under the glare of international antitrust and regulatory scrutiny—Facebook has made key APIs available to third-party apps only on the condition that they refrain from providing the same core functions that Facebook offers, including through Facebook Blue and Facebook Messenger, and from connecting with or promoting other social networks.") & 152–59.

53 FTC Facebook Compl. ¶¶ 25–26 (alleging that "announcing these anticompetitive conditions changed the incentives of third-party apps that relied upon the Facebook ecosystem, by deterring them from including features and functionalities that might compete with Facebook or from working in certain ways with other firms that compete with Facebook," which "suppresses the emergence of threats to Facebook's personal social networking monopoly" and that "enforcing the anticompetitive conditions by terminating access to valuable APIs hinders and prevents promising apps from evolving into competitors that could threaten Facebook's personal social networking monopoly") & 151 (alleging that an "internal Facebook slide deck dated January 2014 dealing with Facebook Platform policies directly acknowledged the importance of API access, asking whether Facebook was '[c]omfortable altering / killing prospects of many startups' "); States FTC Compl. ¶ 15 (alleging that Facebook's policy "thwarted particular competitive threats and more broadly, it told developers in no uncertain terms that valuable access to Facebook's APIs was conditioned on their staying away from Facebook's turf in personal social networking services, thus chilling, deterring, and suppressing competition"). A federal district court, however, dismissed these claims under the belief that the federal antitrust law does not reach these practices, even if they are anti-competitive. New York v. Facebook, Inc., No. CV 20-3589 (JEB), 2021 WL 2643724, at *2 (D.D.C. June 28, 2021) (holding that the States' Section 2 challenge to Facebook's policy of preventing interoperability with competing apps failed to state a claim under current antitrust law, as there is nothing unlawful about having such a policy, and even if it did, such revocations of access occurred over five years before the filing of the complaint, and thus could not furnish a basis for the injunctive relief); Fed. Trade Comm'n v. Facebook, Inc., No. CV 20-3590 (JEB), 2021 WL 2643627, at *2 (D.D.C. June 28, 2021) (stating that Facebook's interoperability policies, even if anti-competitive, cannot form the basis for Section 2 liability). The states thereafter appealed that decision, and the FTC filed an amended complaint.

54 *See, e.g.*, House Report at 311–12 (discussing how Amazon's Alexa favors Amazon's private label products) & 353–62 (discussing Apple's self-preferencing its apps and browser over rival products, and reserving access to APIs and certain device functionalities for its apps).

55 Commission Decision Case AT.39740 Google Search (Shopping), 2017 E.C. 1/2003 ¶¶

80–82, https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf [https://perma.cc/Y8W4-ZBAS]; House Report at 187–88 & 191.

56 House Report at 190.

57 Commission Decision Case AT.39740 Google Search (Shopping).

58 EC Google Shopping Press Release.

59 Commission Decision Case AT.39740 Google Search (Shopping) at Table 19.

60 EC Google Shopping Press Release.

61 EC Google Shopping Press Release; *see also* Commission Decision Case AT.39740 Google Search (Shopping) ¶¶ 460 & 465**.**

62 House Report at 190.

63 House Report at 189–90.

64 House Report at 192.

65 House Report at 192.

66 House Report at 184–87.

67 House Report at 181.

68 House Report at 382–83; *see also* CMA Final Report at ¶ 3.228 (finding that data-opolies can "worsen smaller competitors' offerings to consumers by degrading the functionalities enabled through interoperability or removing the service entirely").

69 *See* Leonard Lyons, *The Lyons Den*, The Morning Call (Paterson, NJ), Aug. 19, 1966, at 14.

70 *See, e.g.*, House Report at 213 (noting how Google "began investing in the mobile ecosystem because it recognized that the rise of smartphone usage threatened to disintermediate Google Search"); 309 (noting that one of "Amazon's strategic goals for Alexa has been to use its voice assistant to reinforce the company's dominance in e-commerce and strengthen its presence in offline retail"); FTC Facebook Compl. ¶¶ 11–13 (alleging how Instagram became an "existential threat to Facebook Blue's personal social networking monopoly" as people switched from desktop computers to mobile phones) & 69–70 (alleging that Facebook understands that "the most significant competitive threats to Facebook Blue may come not from near clones of Facebook Blue, but from differentiated products that offer users a distinctive way of interacting with friends and family for which Facebook Blue is not optimized" and that "Facebook Blue's personal social networking monopoly is most vulnerable at moments of disruption and transition, when a competitor may be better placed than Facebook Blue to exploit changes in technology or consumer behavior").

71 *Hearing on Online Platforms and Market Power Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. (July 29, 2020) (Testimony of Mark Zuckerberg, Facebook, Inc.), https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-Wstate-ZuckerbergM-20200729.pdf.

72 Greg Sterling, *Nielsen: More Time on Internet through Smartphones Than PCs*,

Marketing Land (Feb. 11, 2014), https://marketingland.com/nielsen-time-accessing-internet-smartphones-pcs-73683 [https://perma.cc/VRN5-KGYV].

73 *Windows Phone: A History*, MobiForge, https://mobiforge.com/timeline/windows-phone-history (last visited Mar. 1, 2021) [https://perma.cc/2UFT-VCKX].

74 Liam Tung, *Here Are the Real Reasons Windows Phone Failed, Reveals Ex-Nokia Engineer*, ZD Net (July 29, 2019), https://www.zdnet.com/article/here-are-the-real-reasons-windows-phone-failed-reveals-ex-nokia-engineer/ [https://perma.cc/LWC5-Y2RH].

75 *Windows Phone: A History,* https://mobiforge.com/timeline/windows-phone-history.

76 Commission Decision of July 18, 2018 in Case AT. 40099—Google Android, https://ec.europa.eu/competition/antitrust/cases/dec_docs/40099/40099_9993_3.pdf [https://perma.cc/56K7-Q2TB] [hereinafter EC Android Decision] ¶¶ 292 & 665.

77 Alphabet Inc. 2019 Form 10-K, https://www.sec.gov/Archives/edgar/data/1652044/000165204420000008/goog10-k2019.htm, at 13.

78 Alphabet Inc., *supra* note 77.

79 Facebook Inc. 2019 Form 10-K, https://sec.report/Document/0001326801-20-000013/, at 11 (identifying the risk that "users adopt new technologies where our products may be displaced in favor of other products or services, or may not be featured or otherwise available").

80 FTC Facebook Compl. ¶ 8 (alleging that "Facebook's leadership has learned and recognized that the sharpest competitive threats to Facebook Blue come not from 'Facebook clones,' but from differentiated services and during periods of transition").

81 Alphabet Inc., Q2 2019 Earnings Call Transcript, July 25, 2019, https://abc.xyz/investor/static/pdf/2019_Q2_Earnings_Transcript.pdf?cache=0d95fdf [https://perma.cc/VQ3G-7ND3].

82 U.S. Fish & Wildlife Serv., Venus Flytrap: Under Endangered Species Act Review (June 2017), https://www.fws.gov/southeast/pdf/fact-sheet/venus-flytrap.pdf [https://perma.cc/VG29-QCH5].

83 Alexander G. Volkov et al., *Venus Flytrap Biomechanics: Forces in the Dionaea Muscipula Trap*, 170 J. Plant Physiology 25 (2013), https://doi.org/10.1016/j.jplph.2012.08.009, http://www.sciencedirect.com/science/article/pii/S017616171200332X.

84 *See, e.g.*, Chris Jay Hoofnagle, Federal Trade Commission Privacy Law and Policy 353–54 (2016) (discussing powerful platforms' bait-and-switch privacy policies); States FTC Comp. ¶ 14:

> As part of its strategy to thwart competitive threats, Facebook pursued an open first—closed later approach in which it first opened its platform to developers so that Facebook's user base would grow and users would engage more deeply on Facebook by using third-party services. This strategy significantly boosted engagement on Facebook, enhanced the data it collected, and made the company's advertising business even more profitable. Later, however, when some of those third-party services appeared to present competitive threats to Facebook's monopoly, Facebook changed its practices and policies to close the application programming interfaces ("APIs") on which those services relied, and it took additional actions to degrade and suppress the quality of their interconnections with Facebook.

85 Complaint ¶¶ 60–64, United States v. Google, No. 1:20-cv-03010 (D.D.C. Oct. 20, 2020), https://www.justice.gov/opa/press-release/file/1328941/download [hereinafter Google Compl.].

86 House Report at 211.

87 House Report at 98–99.

88 Complaint ¶¶ 5 & 25, Epic Games v. Google, No. 3:20-cv-05671 (N.D. Cal. Aug. 13, 2020), https://cdn.vox-cdn.com/uploads/chorus_asset/file/21759099/file0.243586135368002.pdf [https://perma.cc/KRV4-8WCG] (alleging that "Google inserts itself as an intermediary between each seller and each buyer for every purchase of digital content within the Android ecosystem, collecting for itself the personal information of users, which Google then uses to give an anti-competitive edge to its own advertising services and mobile app development business").

89 House Report at 194.

90 House Report at 239.

91 *Id.*

92 House Report at 239 (Google introducing "a single 'pay-as-you-go' pricing plan for the core mapping APIs").

93 *Id.* (noting that the net result of this shift "dramatically reduced the number of free Maps API calls a firm could make—from 25,000 per day to around 930 per day").

94 Google Compl. ¶ 12 (alleging that "Google is now positioning itself to dominate search access points on the next generation of search platforms: internet-enabled devices such as smart speakers, home appliances, and automobiles (so-called internet-of-things, or IoT, devices)").

95 Google Compl. ¶ 141; *see also* Jack Nicas, *Google Touts New AI-Powered Tools*, Wall St. J., May 19, 2016, B1, B4 (in discussing its digital personal assistant, Google's CEO said, "We want users to have an ongoing two-way dialogue with Google").

96 House Report at 122.

97 Shoshana Zuboff, The Age of Surveillance Capitalism 260 (2019) (noting that the dominant speaker will have a "potentially insurmountable competitive advantage in its ability to corner

and kidnap the dominant share of human experience").

98 Prabhakar Thakur, *Google Assistant Now Officially Supports TVs, Media Remotes, Set-Top Boxes*, Gadgets 360 (Apr. 14, 2020), https://gadgets.ndtv.com/tv/news/google-assistant-support-tv-media-remote-set-top-box-documentation-2211509 [https://perma.cc/3SPW-KMZQ].

99 House Report at 122 (reporting that market participants "emphasize that smart speakers represent an essential 'hub' or gateway for smart homes and are driving voice-assistant adoption").

100 Zuboff, *supra* note 97, at 268.

101 The other categories are Home Services, Kids, Lifestyle, Local, Movies & TV, Music & Audio, News, Novelty & Humor, Productivity, Shopping, Smart Home, Social, Sports, Travel & Transportation, Utilities, and Weather. *Alexa Skills Guide*, Amazon, https://www.amazon.com/b/ref=UTF8&node=15144553011/ (last visited Mar. 1, 2021) [https://perma.cc/5QAK-5D48].

102 House Report at 307.

103 *Amazon Files Patent for 'Voice Sniffer' Algorithm for Smart Speakers*, Engineering & Technology (Apr. 4, 2018), https://eandt.theiet.org/content/articles/2018/04/amazon-files-patent-for-voice-sniffer-algorithm-for-smart-speakers/ [https://perma.cc/48DL-X332]; U.S. Patent Application No. 20,160,260,135 (filed Sept. 8, 2016), https://pdfaiw.uspto.gov/.aiw?docid=20160260135&PageNum=7.

104 *Amazon Files Patent for 'Voice Sniffer' Algorithm for Smart Speakers*, *supra* note 103.

105 Bret Kinsella, *Amazon Smart Speaker Market Share Falls to 53% in 2019 with Google the Biggest Beneficiary Rising to 31%, Sonos Also Moves Up*, Voicebot.ai (Apr. 28, 2020), https://voicebot.ai/2020/04/28/amazon-smart-speaker-market-share-falls-to-53-in-2019-with-google-the-biggest-beneficiary-rising-to-31-sonos-also-moves-up/ [https://perma.cc/K2AW-SBLS].

106 Google Compl. ¶ 164 (alleging that "Google uses its control over hardware products—including smart speakers and Google Nest smart home products—to protect its general search monopoly. Google recognizes that its '[h]ardware products also have HUGE defensive value in virtual assistant space AND combatting query erosion in core Search business.' Looking ahead to the future of search, Google sees that 'Alexa and others may increasingly be a substitute for Search and browsers with additional sophistication and push into screen devices.' ").

107 *Hearing on Online Platforms and Market Power Part 5: Competitors in the Digital Economy Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. 70 (Jan. 17, 2020) (Written Testimony of Patrick Spence, Chief Executive Officer, Sonos, Inc., at 12–13), https://www.govinfo.gov/content/pkg/CHRG-116hhrg40788/pdf/CHRG-116hhrg40788.pdf.

108 Google Compl. ¶ 163 (alleging that Google "refuses to license its Google Assistant to IoT device manufacturers that would host another voice assistant simultaneously").

109 Google Compl. ¶ 140; Colo. Google Compl. ¶¶ 130, 133–36.

110 House Report at 302 & 314; Dana Mattioli, Patience Haggin, & Shane Shifflett, *Amazon Restricts How Rival Device Makers Buy Ads on Its Site*, Wall St. J. (Sept. 22, 2020), https://www.wsj.com/articles/amazon-restricts-advertising-competitor-device-makers-roku-arlo-11600786638.

111 Apple also leverages its platform's default digital assistant Siri "to strengthen consumer engagement with its own services and apps," by using as a default Apple Music when asked to play music or Apple Maps when asked for directions. House Report at 376.

112 Zuboff, *supra* note 97, at 224 (quoting marketing director of a Silicon Valley firm that sells software to link smart devices that the demand is "all push, not pull" and that most consumers "do not feel a need for these devices").

113 In 2021, Clearwater, Fla.-based BayCare Health System began deploying Amazon Alexa devices in 2,500 rooms across its 14 hospitals. Jackie Drees, *7 Recent Big Tech Partnerships in Healthcare: Apple, Amazon, Google & More*, Becker's Hospital Review (Jan. 25, 2021), https://www.beckershospitalreview.com/digital-transformation/7-recent-big-tech-partnerships-in-healthcare-apple-amazon-google-more.html [https://perma.cc/WF55-UHMJ].

114 Colo. Google Compl. ¶ 138.

115 Alphabet Inc., Q1 2019 Earnings Call Transcript, Apr. 29, 2019, https://abc.xyz/investor/static/pdf/2019_Q1_Earnings_Transcript.pdf?cache=ebdc584.

116 Google Compl. ¶ 162.

117 Hooman Mohajeri Moghaddam, *Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices*, Freedom to Tinker (Sept. 18, 2019), https://freedom-to-tinker.com/2019/09/18/watching-you-watch-the-tracking-ecosystem-of-over-the-top-tv-streaming-devices/ [https://perma.cc/HA3C-4M7V].

118 Moghaddam, *supra* note 117.

119 Oculus for Developers, https://developer.oculus.com (last visited Mar. 1, 2021) [https://perma.cc/NT6Z-UQY4].

120 Imran Hussain, *Apple to Compete Against Oculus with VR Headset, AR Glasses Coming Later*, iThinkDifferent, Jan. 21, 2021, https://www.ithinkdiff.com/apple-oculus-vr-headset-ar-glasses-later/ [https://perma.cc/EG23-NQT8].

121 *See* Digital Markets Act at 15 (noting how a "small number of large providers of core platform services have emerged with considerable economic power" as these gatekeepers typically "feature an ability to connect many business users with many end users through their services which, in turn, allows them to leverage their advantages, such as their access to large amounts of data, from one area of their activity to new ones").

122 House Report at 125 (noting that during its investigation, "several companies shared concerns that voice assistant platforms would be able to use this vantage to glean competitive insights from third-party voice applications or smart appliances that are performing well. As a result, platforms could use that data to acquire competitive threats or integrate their features into the company's product.").

123 CMA Final Report at ¶ 58 (hearing "numerous complaints about this form of activity,

for example that Facebook is using its position in social media to leverage into adjacent markets, or that Google is using its position in general search to undermine competition in different forms of specialised search, including online travel agents and shopping comparison services").

124 Summary of European Commission Case AT.40099 Google Android, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52019XC1128(02), ¶ 27 (finding that Google's four different forms of anticompetitive conduct all pursued "an identical objective of protecting and strengthening Google's dominant position in general search services and thus its revenues via search advertisements").

125 House Report at 18 (noting that investors have said "that they avoid funding entrepreneurs and other companies that compete directly or indirectly with dominant firms in the digital economy" and that "a prominent venture capital investor explained that due to these factors, there is a strong economic incentive for other firms to avoid head-on competition with dominant firms"). *See also id*. at 47 (noting the "mounting evidence that the dominance of online platforms has materially weakened innovation and entrepreneurship in the U.S. economy"); Hughes, Op-ed (noting that "despite an extended economic expansion, increasing interest in high-tech start-ups, an explosion of venture capital and growing public distaste for Facebook, no major social networking company has been founded since the fall of 2011").

126 House Report at 19 & 74.

127 Zuboff, *supra* note 97, at 216.

128 John Elflein, *U.S. National Health Expenditure as Percent of GDP from 1960 to 2020*, Statista, June 8, 2020, https://www.statista.com/statistics/184968/us-health-expenditure-as-percent-of-gdp-since-1960/ [https://perma.cc/X9FC-M78L].

129 *See, e.g.*, Alphabet Inc. 2019 Form 10-K, https://abc.xyz/investor/static/pdf/20200204_alphabet_10K.pdf?cache=cdd6dbf Google Annual Report at 1, 5 & 64 (noting that Verily, Google's life science and healthcare company "with a mission to make the world's health data useful so that people enjoy healthier lives" is "developing tools and platforms to improve health outcomes"); Laura Dyrda, *15 Things to Know About Amazon's Healthcare Strategy Heading Into 2020*, Becker's Health IT, Jan. 6, 2020, https://www.beckershospitalreview.com/healthcare-information-technology/15-things-to-know-about-amazon-s-healthcare-strategy-heading-into-2020.html; Sebastian Herrera et al., *Amazon to Go National on Health*, Wall St. J. (Mar. 18, 2021) at B1; *Big Tech in Healthcare: Here's Who Wins and Loses as Alphabet, Amazon, Apple, and Microsoft Target Niche Sectors of Healthcare*, Insider Intelligence, Feb. 14, 2021, https://www.businessinsider.com/2-14-2021-big-tech-in-healthcare-report.

130 Zuboff, *supra* note 97, at 125.

131 Alex Christian, *Big Tech and Joe Wicks Go Head-to-Head as Digital Fitness Bulks Up*, Wired (Feb. 1, 2021), https://www.wired.co.uk/article/joe-wicks-fitness-big-tech [https://perma.cc/7TSC-VCUD].

132 House Report at 48 (quoting a venture capital firm that "[t]o the extent that a firm

successfully offers a service to give people tools to control their privacy, ‘Google or Facebook are going to want to pull that back as fast as they possibly can. They don’t want you aggressively limiting their extremely valuable information collection.’ ”).

# 3
# How Data-opolies Have Exploited the Current Legal Void, and What's Being Proposed to Fix It

When the CEOs of Google, Apple, Facebook, and Amazon all testified in 2020 before Congress, some dubbed it Big Tech's big tobacco moment. Yet, each CEO had a compelling narrative of why his company was unlike the monopolies of old.

Ordinarily, we equate monopolies with higher prices. Unlike some pharmaceuticals or local cable monopolies, data-opolies do not charge consumers exorbitant fees. Facebook's CEO testified how his company's "services create a lot of value in people's lives, and our business model means we can offer them for free."[1]

Google's CEO Sundar Pichai added how "[s]urvey research found that free services like Search, Gmail, Maps, and Photos provide thousands of dollars a year in value to the average American."[2] On the advertising side, Pichai testified how digital advertising rates had declined 40% over the past decade "with these savings passed down to consumers through lower prices."[3]

Amazon's CEO touted his company's low prices and superior service: "by focusing obsessively on customers, we are internally driven to improve our services, add benefits and features, invent new products, lower prices, and speed up shipping times—before we have to."[4] Amazon's consumer-first approach, Jeff Bezos told Congress, was working with eighty percent of Americans having a favorable impression of the company overall.[5]

Apple's CEO testified of his company's pathbreaking innovation and building "things that make us proud."[6] Google's and Facebook's CEOs added how their companies spend billions of dollars annually on research and development.[7]

Under the conventional antitrust rubric, free or low prices, better quality, and innovation do not equal monopolization. Yet, in a rare display of bipartisanship, the members of Congress unanimously requested additional rounds to grill the four CEOs. At the hearing's end, the verdict was grim. The subcommittee chair, David N. Cicilline, concluded that each company has monopoly power. Some need to be broken up. All need to be regulated and held accountable, and Congress may need to develop new tools to rein them in.

In their annual reports, the data-opolies identify intense competition as a risk factor. Despite these claims, their monopolies are secure. Even in 2020, while being under investigation on both sides of the Atlantic, Google coerced distributors into contracts that were "even more exclusionary than the agreements they replaced."[8] In the third quarter of 2020, while many companies were hurting financially from the pandemic, Google, Apple, Facebook, and Amazon raked in "$38 billion in profits on nearly $240 billion in revenue."[9] The likely wave of small- and medium-sized enterprise bankruptcies from the ongoing pandemic will further increase market concentration.[10]

Given the data-opolies' durable market power, policymakers have begun inquiring about their risks. The light-touch antitrust policies of the past 40 years have failed. The emerging consensus is that the data-opolies are expanding rather than shrinking. They will continue to leverage their power into other markets. The digital platform economy will not perform efficiently or in our interest. There are multiple market failures.

Another concern is that the legal system moves too slow relative to the technological changes. As the California legislature noted when enacting the California Consumer Privacy Act of 2018, the "law has not kept pace with these developments and the personal privacy implications surrounding the collection, use, and protection of personal information."[11] Although the European Commission brought several monopolization cases against Google, they did not dent Google's market power or deter its abuses.[12] So, in late 2020, the European Commission proposed far-reaching obligations on these data-opolies precisely because the "gatekeeper-related problems are currently not (or not effectively) addressed by existing EU legislation or national laws of Member States."[13] Likewise, Congress in 2021 introduced six new bills to reinvigorate competition in the digital platform economy.

If the current laws cannot address these market failures, what can be done?

## A. "We Need More Competition."

That is the common refrain by policymakers when discussing the digital economy. The belief is that the proposed policies will address the market failures; promote contestable and competitive digitals markets; and benefit consumers from more innovation, more options, and better privacy protections.

Although antitrust enforcers focused in the past few decades on price effects, one long-standing and well-accepted concern of market power, generally, and

monopolies, in particular, is degraded quality.[14] While the quality of the data-opolies' products and services can increase on some parameters due to network effects or innovation, quality can deteriorate on other important parameters, such as privacy. When a data-opoly's business model depends on harvesting and exploiting personal data, its incentives change. It will reduce privacy protections below competitive levels and collect personal data above competitive levels.[15]

Consequently, policymakers increasingly recognize that companies can compete on privacy and protecting data.[16] The collection of too much personal data can be the equivalent of charging an excessive price.[17] As the U.K. competition agency noted, "The collection and use of personal data by Google and Facebook for personalised advertising, in many cases with no or limited controls available to consumers, is another indication that these platforms do not face a strong enough competitive constraint."[18] Thus, data-opolies exploit their market power by extracting a lot of personal data from consumers.[19] Besides collecting more data than they could if competition were working and nontoxic (more on that in the next chapter), data-opolies can degrade quality in other ways. Facebook and Google, for example, have increased the number of ads that we see.[20]

## B. Ensuring a Contestable and Fair Digital Sector

How do policymakers increase competition where network effects and extreme economies of scale can lead to winner-take-all markets? Let us consider the various jurisdictions' proposals to deter data-opolies and promote competition. Some policies, as we will see, target the data-opolies' anticompetitive playbook. Others seek to ameliorate their anticompetitive effects; a few address the source of their power.

The aim, as European policymakers observed, "is to ensure a contestable and fair digital sector in general and core platform services in particular," that promotes "innovation, high quality of digital products and services, fair and competitive prices, as well as a high quality and choice for end users in the digital sector."[21]

Let us review the main remedies proposed as of 2021.

### 1. A More Proactive Review of Dominant Platforms

Enforcers and policymakers need to update their game. The 2020 Congressional

Antitrust Report is as much an indictment on the U.S. antitrust enforcers as the data-opolies. In its investigation, the House Antitrust Subcommittee "uncovered evidence that the antitrust agencies failed, at key occasions, to stop monopolists from rolling up their competitors and failed to protect the American people from abuses of monopoly power. Forceful agency action is critical."[22]

We are already witnessing an antitrust resurgence with the announcement of task forces in 2019 by the U.S. Department of Justice and Federal Trade Commission;[23] administrative[24] and legislative hearings;[25] investigations and prosecutions by numerous state attorney's general;[26] more investigations by the European Commission,[27] EU Member States;[28] and competition authorities in Australia,[29] India, Argentina, Brazil, Korea, and the United Kingdom. The cases against Google and Facebook, the first significant monopolization cases in the United States over 20 years, follow the European Commission's three cases against Google and Germany's case against Facebook, with more prosecutions likely.

Competition agencies are also creating specialized task forces to focus on digital platforms[30] and proposing regular and continuous monitoring of the digital economy.[31]

## 2. Updating and Strengthening the Competition Laws

One problem in the United States is the Supreme Court's rambling through the wilds of economic theory. The lower courts incorporate the Court's dicta, making it harder to enforce the antitrust laws. As the House Republicans noted in their separate report, it "is appropriate for Congress to remind the agencies and the courts of the original Congressional intent behind the antitrust laws, including that our enforcement agencies should be able to bring cases, like a review of Facebook's acquisition of Instagram, based on potential competition doctrine without facing impossible evidentiary burdens."[32]

One recommendation is to reassert antitrust's anti-monopoly goals.[33] Data-opolies' anticompetitive actions pose economic, social, and political risks. So, Congress should "consider reasserting the original intent and broad goals of the antitrust laws, by clarifying that they are designed to protect not just consumers, but also workers, entrepreneurs, independent businesses, open markets, a fair economy, and democratic ideals."[34] To rehabilitate U.S. monopolization law, the Congressional Report, among other things, recommended incorporating Europe's abuse of dominance standard.[35] U.S. policymakers have also sought to revitalize

the antitrust doctrines that the U.S. courts have marginalized, including

- the monopoly leveraging theory (to deter data-opolies from leveraging their power to colonize new ecosystems),[36]
- duty to deal/essential facilities doctrine (so that data-opolies cannot hinder or eliminate other services' interoperability with their platforms, such as Facebook killing the video-sharing platform Vine),[37]
- tying claims (to prevent data-opolies from bundling their "must-have" products (e.g., Google Play app store) with other apps and services (e.g., Google's search engine, Chrome browser, and other apps), thereby denying manufacturers and consumers choice and foreclosing rivals),[38]
- predatory pricing (to prevent the data-opolies' below-cost pricing aimed at eliminating rivals, such as Amazon's tactics against Diapers.com),[39]
- stronger standards against the data-opolies' self-preferencing their products and services (so that Google cannot favor its vertical searches, such as Google Flights, Google Hotel Ads, and Google Local Search One-Boxes, by placing them prominently at the top of the search results, where the user is more inclined to click),[40] and
- stronger standards against anticompetitive product designs.[41]

The House Congressional Report also recommends cutting back much of the Supreme Court's dicta that have mired antitrust enforcement.[42] So, rather than having to prove market power with circumstantial evidence (such as the plaintiff showing the defendant's high market share in a relevant antitrust market, a lengthy, uncertain process that primarily benefits expert economists), the agencies and courts can rely on direct evidence of monopoly power (such as evidence that the company is coercing others to do things they could not dictate in a competitive market).[43]

Policymakers are also considering new theories of harm under the existing laws, including "the use of covert tracking and data collection to exclude competitors."[44]

### 3. Measures to Deter Data Hoarding

As we will explore in Chapter 7, the policy proposals seek to increase the flow of data to rivals by, among other things,

- promoting multi-homing by users,
- targeting data-opolies' use of defaults to entrench their market power (such as Google paying Apple $12 billion to be the default search engine on Safari),[45]
- reducing users' switching costs by improving data portability[46] and interoperability,[47] and
- imposing, at times, a duty for data-opolies to share data with rivals while safeguarding individuals' privacy interests.[48]

Jurisdictions are also considering digital services taxes.[49] Inspired by the economist Paul Romer's op-ed, a Maryland state senator introduced a digital advertising tax to generate revenue and incentivize the data-opolies to change their business model.[50] If it survives legal challenge, the Maryland tax law would be the first of its kind in the United States.[51]

## 4. Improving Privacy Protections

The consensus among policymakers is that the current notice-and-consent privacy policies have failed. Policymakers differ on what measures must be undertaken. But they recognize that more robust privacy protections are necessary so that individuals can regain their control over their privacy and data and prevent data-opolies from collecting far more data than they could if competition were healthy.[52]

Under the proposed Digital Markets Act, the data-opolies cannot combine the personal data from their many services and third parties without the individual's consent.[53] The powerful gatekeepers would have to provide the European Commission more information on how they are profiling individuals.[54] The Commission's proposed Digital Services Act would also impose transparency obligations on online advertising.

## 5. Targeting Killer Acquisitions

Every jurisdiction that has studied these digital platform markets has called for greater antitrust scrutiny of data-driven and platform-related mergers and acquisitions. Although the European Commission approved the Google/Fitbit merger with behavioral conditions (as Fitbit had a smaller presence in the EU), the United States and Australia were as, of 2021, still investigating the acquisition.[55]

If you watched any of the CSI (Crime Scene Investigation) television shows, you would see forensic investigators flawlessly and rapidly solve crimes with futurist technologies and ample evidence. Now some courts expect the competition agencies to prove mergers' harm with the same degree of precision.[56] This economic undertaking is impossible when a data-opoly acquires a nascent competitive threat. To cancel *CSI Antitrust*, policymakers have proposed the following:

- legislative changes to the standard for reviewing conglomerate transactions,[57]
- lessening the agency's burden of proof to challenge horizontal mergers,[58]
- invigorating vertical merger law,[59] and
- lowering the reporting thresholds for pre-merger review.[60]

Would the agency have to prove that, but for the acquisition, the nascent competitor would have been a successful entrant? Not under one proposal.[61] Instead, there would be "a presumption against acquisitions of startups by dominant firms, particularly those that serve as direct competitors, as well as those operating in adjacent or related markets."[62] Fundamentally, "any acquisition by a dominant platform would be presumed anticompetitive unless the merging parties could show that the transaction was necessary for serving the public interest and that similar benefits could not be achieved through internal growth and expansion."[63]

## 6. Ex Ante Codes of Conduct Enforced by a Regulatory Agency

Antitrust enforcement often is too slow, happens too infrequently to be relied upon, and is incomplete—focusing on exclusionary, but not exploitative, practices. Many companies live in fear today of the data-opolies. A change in the dominant platform's algorithm can reduce their visibility, whether in the app store, news feed, search results, or online shopping platform, and dry up the traffic to their website, app, or products. Waiting for the antitrust enforcer is futile. So the aim here is to improve the process for quickly redressing the market participants' complaints involving these gatekeepers and counter their superior bargaining power over advertisers, website publishers, app developers, news organizations, and individuals. The codes of conduct would operate more like posted speed limits, which are easier to enforce than ex-post standards of

whether drivers were traveling at unsafe or unreasonable speeds.

It is difficult, outside of copyright, trademark, and patent law, to prevent dominant firms from copying their rivals. So, these codes of conduct turn to the *K* in the ACK strategy by making it harder for data-opolies to kill off smaller rivals and wield their gatekeeper power against those that rely on their platforms.[64]

For example, Europe's proposed Digital Markets Act complements, rather than amends competition law, by imposing 7 automatic obligations on gatekeepers, 11 additional obligations, subject to the Commission's specifications, and potentially more obligations that the Commission could impose under its proposed market investigation tool. These obligations seek to deter many of the data-opolies' abuses, such as self-preferencing, using rivals' data to unfairly compete against them, and tying arrangements. Gatekeepers, as defined under the Act,[65] would "carry an extra responsibility to conduct themselves in a way that ensures an open online environment that is fair for businesses and consumers, and open to innovation by all, by complying with specific obligations laid down in the draft legislation."[66]

## 7. Expanding the Antitrust Enforcer's Toolbox to Prevent the Platforms from Colonizing and Dominating New Ecosystems

Network effects can lead to winner-take-most markets. We saw how the mobile operating system market went from multiple competitors in 2010 to a duopoly eight years later. Thus, companies are tempted to rely on anticompetitive tactics to tip the market in their favor. Even if they are caught, the market cannot quickly tip back to being competitive (just consider Android's stronghold despite several monopolization prosecutions).

Rather than waiting for the colonized platforms (like wearables or digital assistants) to tip to one or two data-oplies, policymakers are considering new competition tools "to intervene before the market tips irreversibly."[67] Among the tools are interim measures (such as a cease-and-desist order while the agency investigates the data-opoly)[68] and market sector reviews.[69] In 2021, Germany modernized its monopoly law for the digital platform economy to "shut the stable door before the horse has bolted."[70] In allowing the agency "to take even faster and more effective action," the law prohibits data-opolies "from engaging in certain types of conduct much earlier," such as self-preferencing and denying rivals access to critical data. The Act also enables the Bundeskartellamt "to

intervene in cases where a platform market threatens to 'tip' towards a large supplier."[71]

## 8. Policies to Address Specific Problems in Markets Dominated by Data-opolies

One area of concern is Google's and Apple's control over their app stores. To address the data-opolies' hefty 30% app tax, South Korea in 2021 required Google and Apple to open up their app stores to alternative payment systems and allow consumers to choose among in-app payment systems.[72]

In the United States, the proposed Open App Markets Act would also allow app developers to use alternative in-app payment systems (besides Google's and Apple's), and communicate directly with customers (including business offers). Consumers could also install third-party app stores and obtain apps outside of Google's and Apple's app store.[73] The Digital Markets Act would impose similar obligations.[74]

To resolve Japan's concerns, Apple will let developers of newspaper and media "reader" apps around the world link to an external website to set up or manage an account beginning early 2022.[75]

Other measures include increasing transparency in the online advertising markets[76] and efforts to reduce the regulatory imbalance in how the traditional news media is treated versus the digital platforms in terms of content.[77]

## 9. Structural Remedies

Behavioral remedies are generally less effective than structural remedies.[78] But the proposed Digital Markets Act opts for the former. The Commission can order divestitures and other structural remedies under the Act only when "there is no equally effective behavioural remedy or where any equally effective behavioural remedy would be more burdensome for the gatekeeper concerned than the structural remedy."[79]

Other competition authorities are weighing whether to break up the data-opolies or spin off parts of their businesses.[80] In their monopolization cases against Facebook and Google, the federal and state enforcers are requesting structural remedies.[81] The U.S. Congress is also proposing structural separations and "line of business" restrictions to redress the inherent conflicts of interest when the data-opoly vertically integrates and competes against third-party sellers on its platform (like Amazon, for example).[82]

## C. Reflections

Outside of the United States and perhaps the EU, no other jurisdiction can execute these policies unilaterally. Consider Australia, which is at the forefront of the intellectual debate and policy proposals to rein in Google and Facebook. The country in 2020 was considering legislation that would require Google and Facebook to compensate newspapers when they post the newspapers' stories.[83] Under Australia's proposed law, the data-opolies would also have to notify the newspapers of algorithm changes that materially affected the traffic to their newspapers' websites.

In 2020, Google and Facebook took on the world's 13th largest economy. First, Google employed pop-up ads warning Australians that if the law were passed, their search results would be degraded, their data would be handed over to "big news businesses," and their free services were at risk.[84] Misinformation, responded the Australian competition authority. The proposed code sought to redress the bargaining imbalance between the newspapers and data-opolies. The code would require Google and Facebook to negotiate in good faith and pay news media to use their content. Next, Google threatened to pull out its search engine. As U.S. Senator Amy Klobuchar noted,

> They are literally taking on a government of a major country, in Australia. When the prime minister says, "Hey, we're going to start making you guys pay for content," and they say back, "No, you're not. We're going to withdraw from your market and you'll have no search engine."[85]

Google, however, in mid-February 2021, began signing agreements with Australia's major news outlets.

As for Facebook, well –

Image 3.1 shows the Facebook page of Australia's national newspaper before February 18, 2021:

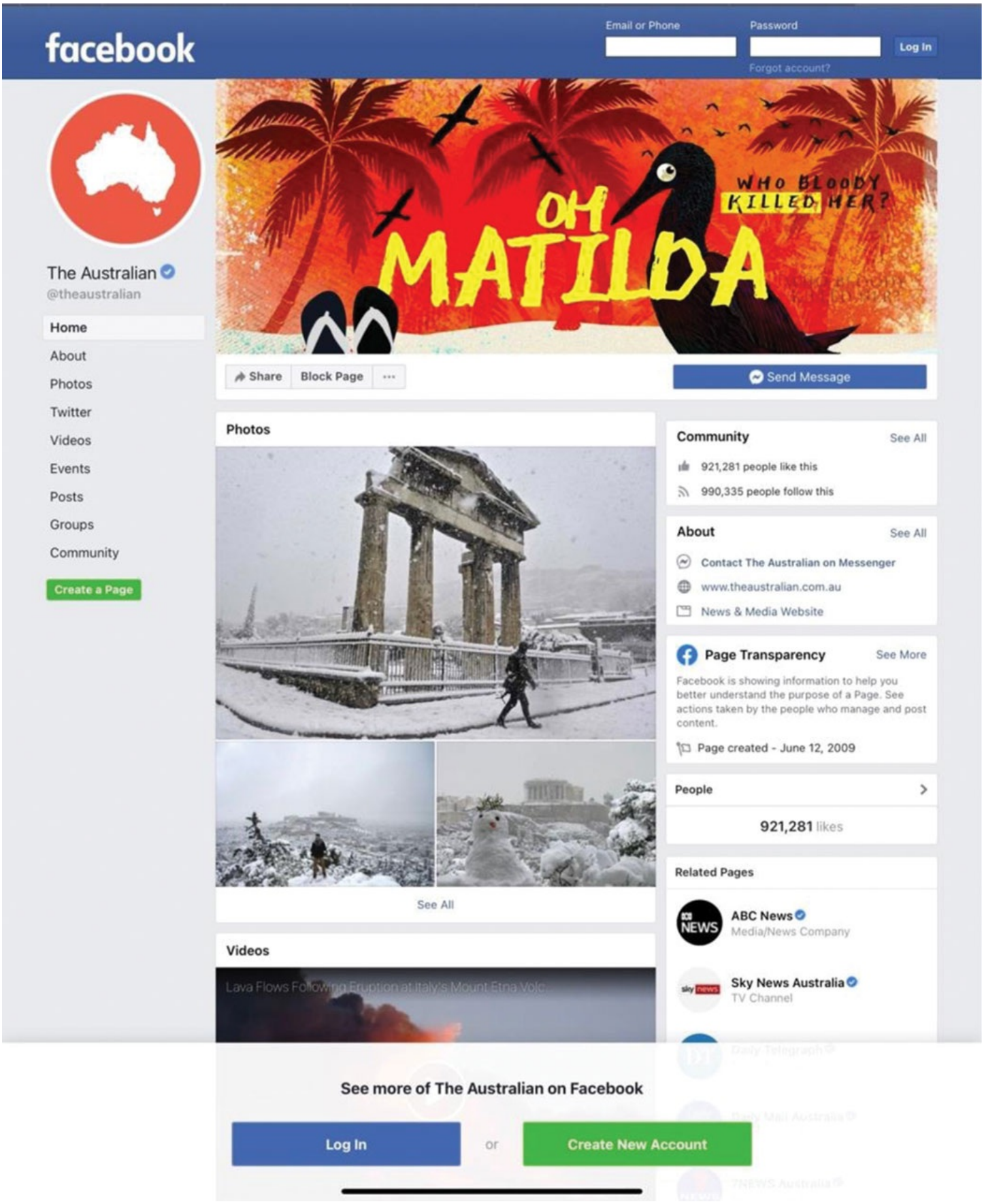


**Image 3.1** *The Australian* newspaper's Facebook page prior to February 18, 2021

Image 3.2 is how the newspaper’s Facebook page app eared on February 18, 2021:

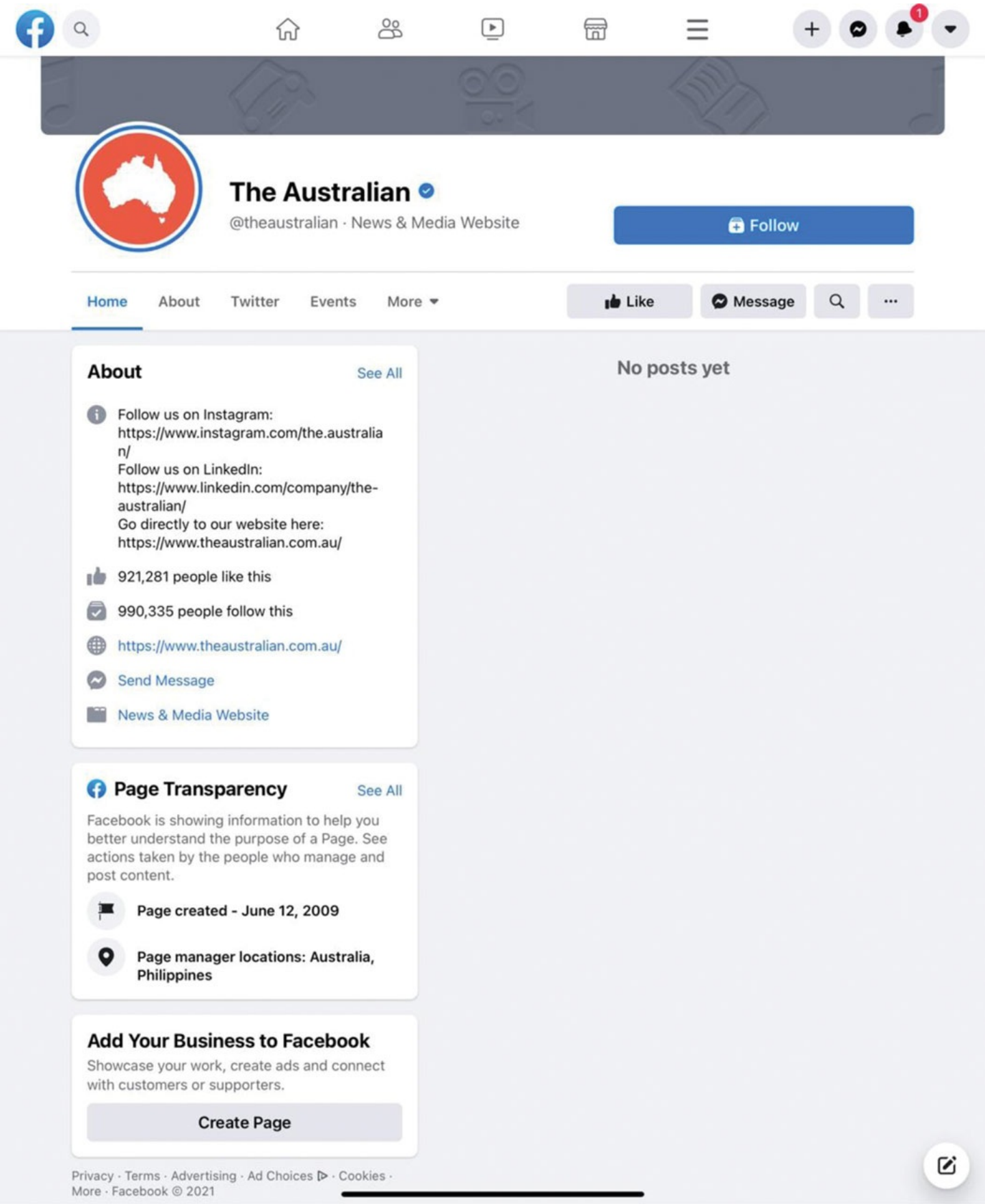


**Image 3.2** *The Australian* newspaper's Facebook page on February 18, 2021

Why blank? Rather than pay publishers for their news stories, Facebook decided to black out the "content from Australian publishers on Facebook worldwide" and made unavailable "stories from both domestic and international news content within Australia."[86] So, with a flick of a switch, *The Wall Street Journal* reported, "the Facebook pages of top Australian media outlets went completely blank."[87] But Facebook went further, as *The New York Times* reported:

> Pages for state health departments and emergency services were also wiped clean. The Bureau of Meteorology, providing weather data in the middle of fire season — blank. An opposition candidate running for office in Western Australia, just a few weeks from an election—every message, gone.
>
> Even pages for nonprofits providing information to domestic violence victims fell into the Facebook dragnet, along with those for organizations that work with the poor and vulnerable.[88]

Facebook said it erased some of these pages unintentionally. But Facebook did not "provide any further details on how it would decide which pages to restore and which to keep blocked."[89] Ultimately, Australia enacted the News Media Bargaining Code, and Facebook relented, striking deals to pay newspapers for their content.[90]

Nonetheless, as the Europeans observe, data-opolies are a global problem.[91] We cannot expect Australia to fix it alone. Privacy, consumer protection, and antitrust agencies worldwide must collaborate on a "common strategy" to rein them in.[92]

Facebook and Twitter already kicked a U.S. president off of their platforms. Whatever one's views of Donald Trump, a bipartisan concern is that the data-opolies wield too much political influence and could flex their power on other disfavored speakers and policies. Thus, we must get the right policy tools, and our countries must work together in applying them. Otherwise, many more of us will wake up one morning, like the Australians on February 18, 2021, and find what Facebook left them—"pages dedicated to aliens and UFOs: one for a community group called Say No to Vaccines; and plenty of conspiracy theories, some falsely linking 5G to infertility, others spreading lies about Bill Gates and the end of the world."[93]

---

1 *Hearing on Online Platforms and Market Power Part 6: Examining the Dominance of*

*Amazon, Apple, Facebook, and Google Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. (July 29, 2020) (Testimony of Mark Zuckerberg, Facebook, Inc.), https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-Wstate-ZuckerbergM-20200729.pdf.

2 *Hearing on Online Platforms and Market Power Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. (July 29, 2020) (Written Testimony of Sundar Pichai, Chief Executive Officer, Alphabet Inc. at 3), https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-Wstate-PichaiS-20200729.pdf [hereinafter Pichai Testimony].

3 Pichai Testimony at 3.

4 *Hearing on Online Platforms and Market Power Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. (July 29, 2020) (Statement of Jeffrey P. Bezos, Founder & Chief Executive Officer, Amazon), https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-Wstate-BezosJ-20200729.pdf [hereinafter Bezos Congressional Statement].

5 Bezos Congressional Statement.

6 *Hearing on Online Platforms and Market Power Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. (July 29, 2020) (Statement of Tim Cook, Chief Executive Officer of Apple Inc. at 3), https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-Wstate-CookT-20200729.pdf.

7 Pichai Testimony (noting that at the end of 2019, Google's R&D spending had increased almost 10 times over 10 years, from $2.8 billion to $26 billion and that Google invested over $90 billion in R&D over the prior five years); Zuckerberg Testimony (noting that Facebook invests around $10 billion per year in R&D).

8 Complaint ¶ 12, United States v. Google, No. 1:20-cv-03010 (D.D.C. Oct. 20, 2020), https://www.justice.gov/opa/press-release/file/1328941/download [hereinafter Google Compl.].

9 Rani Molla, *As COVID-19 Surges, the World's Biggest Tech Companies Report Staggering Profits*, Vox (Oct. 30, 2020), https://www.vox.com/recode/2020/10/30/21541699/big-tech-google-facebook-amazon-apple-coronavirus-profits.

10 Ufuk Akcigit et al., *Rising Corporate Market Power: Emerging Policy Issues*, Int'l Monetary Fund Staff Discussion Note, at 5 (Mar. 2021), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2021/03/10/Rising-Corporate-Market-Power-Emerging-Policy-Issues-48619 [hereinafter IMF Market Power Report].

11 California Consumer Privacy Act of 2018, ch. 55 § 2(d), 2018 Cal. Stat. 1807, 1809.

12 *See, e.g.*, Sam Schechner, *Some Google Search Rivals Lose Footing on Android System*, Wall St. J. (Sept. 28, 2020), https://www.wsj.com/articles/some-google-search-rivals-lose-footing-on-android-system-11601289860.

13 European Commission, Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), at p. 2 (Dec. 15, 2020), https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf [https://perma.cc/G87S-Q88U] [hereinafter Digital Markets Act].

14 U.S. Dep't of Justice & Fed. Trade Comm'n, Horizontal Merger Guidelines § 1 (Aug. 19, 2010), https://www.justice.gov/atr/horizontal-merger-guidelines-08192010 (noting that market power can be "manifested in non-price terms and conditions that adversely affect customers, including reduced product quality, reduced product variety, reduced service, or diminished innovation" and these non-price effects "may coexist with price effects, or can arise in their absence"); OECD, The Role and Measurement of Quality in Competition Analysis, at 22, DAF/COMP(2013)17 (Oct. 28, 2013), http://www.oecd.org/competition/Quality-in-competition-analysis-2013.pdf; Commission Decision of June 27, 2017 (Case AT. 39740--Google Search (Shopping)), https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf [https://perma.cc/NH5J-APP4] ¶ 324 (finding that Google "could alter the quality of its general search service to a certain degree without running the risk that a substantial fraction of its users would switch to alternative general search engines"); *see also* Maurice E. Stucke & Ariel Ezrachi, *When Competition Fails to Optimize Quality: A Look at Search Engines*, 18 Yale J.L. & Tech. 70 (2016).

15 Majority Staff of H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial and Administrative Law, Report and Recommendations: Investigation of Competition in Digital Markets 18 (2020), https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429 [https://perma.cc/29LN-L4BL] [hereinafter House Report] ("in the absence of adequate privacy guardrails in the United States, the persistent collection and misuse of consumer data is an indicator of market power online" and "[i]n the absence of genuine competitive threats, dominant firms offer fewer privacy protections than they otherwise would, and the quality of these services has deteriorated over time") & 51 (noting how the "best evidence of platform market power" is "not prices charged but rather the degree to which platforms have eroded consumer privacy without prompting a response from the market"); UK Competition & Markets Authority, Online Platforms and Digital Advertising Market Study: Market Study Final Report ¶¶ 2.84 & 3.151 (July 1, 2020), https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digit [https://perma.cc/DA5V-RHA5] [hereinafter CMA Final Report]; Australian Competition and Consumer Commission, Digital Platforms Inquiry—Final Report at 374 (2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report [https://perma.cc/M36S-YQJ4] [hereinafter ACCC Final Report]; Google Compl. ¶ 167 (alleging that by "restricting competition in general search services, Google's conduct has harmed consumers by reducing the quality of general search services (including dimensions

such as privacy, data protection, and use of consumer data")); Complaint ¶ 98, Colorado v. Google, No. 1:20-cv-03715-APM (D.D.C. Dec. 17, 2020), https://coag.gov/app/uploads/2020/12/Colorado-et-al.-v.-Google-PUBLIC-REDACTED-Complaint.pdf, [hereinafter Colo. Google Compl.] (alleging that "Google collects more personal data about more consumers than it would in a more competitive market as a result of its exclusionary conduct, thereby artificially increasing barriers to expansion and entry"); Complaint ¶¶ 127, 177 & 180, New York v. Facebook, No. 1:20-cv-03589-JEB (D.D.C., Dec. 9, 2020), https://ag.ny.gov/sites/default/files/state_of_new_york_et_al._v._facebook_inc._-_filed_public_complaint_12.11.2020.pdf [https://perma.cc/GYC7-44RX] [hereinafter States Facebook Compl.] (alleging Facebook's degradation in privacy protection after acquiring Instagram and WhatsApp).

16 Background Note by the Secretariat, Consumer Data Rights and Competition, OECD Doc. DAF/COMP(2020)1 (Apr. 29, 2020), https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf at ¶¶ 69, 99, 100 [https://perma.cc/SQ48-WEPD][hereinafter OECD Consumer Data Rights and Competition]; Digital Competition Expert Panel, Unlocking Digital Competition 49 (2019) (also known as the Furman Report), https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel [https://perma.cc/VK9M-3GV8] [hereinafter Furman Report]; OECD Consumer Data Rights and Competition, Note from the UK, OECD Doc. DAF/COMP/WD(2020)51 (June 2, 2020), https://one.oecd.org/document/DAF/COMP/WD(2020)51/en/pdf [https://perma.cc/76KL-DF6G] at ¶ 25 (noting how privacy and data protection rights "may constitute an aspect of service quality on which firms can differentiate themselves from their competitors" and a merger's reduction in "privacy protection may be interpreted as a reduction in quality"); *See, e.g.*, OECD Consumer Data Rights and Competition, Note from the European Union, OECD Doc. DAF/COMP/WD(2020)40 (June 3, 2020), https://one.oecd.org/document/DAF/COMP/WD(2020)40/en/pdf [https://perma.cc/C5K2-RU9V] at ¶ 51 ("Market investigations in specific cases, such as Microsoft/LinkedIn, have further supported the view that data protection standards can be an important parameter of competition, particularly in markets characterised by zero-price platform services where the undertaking has an incentive to collect as much data as possible in order to better monetise it on the other side of the platform."); Commission Decision No. M.8124 (Microsoft/LinkedIn) (Dec. 6, 2016), https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf, ¶ 350 (acknowledging that privacy was a "driver of customer choice" and "an important parameter of competition" and that companies can compete on the basis of privacy policy "to the extent that consumers see it as a significant factor of quality"); CMA Final Report at ¶ 3.158 (noting that privacy can be a parameter of competition among social media platforms); Complaint at ¶¶ 42 & 127, Federal Trade Commission v. Facebook, No. 1:20-cv-03590-CRC (D.D.C. Dec. 9, 2020), https://www.ftc.gov/system/files/documents/cases/051_2021.01.21_revised_partially_redacte [hereinafter FTC Facebook Compl.] (alleging that personal social networking providers

compete for users on a variety of factors, including privacy protection options and "WhatsApp's strong focus on the protection of user privacy would offer a distinctively valuable option for many users, and would provide an important form of product differentiation for WhatsApp as an independent competitive threat in personal social networking"); States Facebook Compl. ¶¶ 7–8.

17 OECD, Consumer Data Rights and Competition, *supra* note 16, at ¶ 100; CMA Final Report at ¶ 11 (noting that "competition problems result in consumers receiving inadequate compensation for their attention and the use of their personal data by online platforms"); OECD Big Data Report, *supra* note 16, at 16–17 ("market power may be exerted through non-price dimensions of competition, allowing companies to supply products or services of reduced quality, to impose large amounts of advertising or even to collect, analyze or sell excessive data from consumers"); Eleonora Ocello et al., *What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case*, Competition Merger Brief (Feb. 2015), at 2, 6, http://ec.europa.eu/competition/publications/cmb/2015/cmb2015_001_en.pdf (observing if a website, post-merger, "would start requiring more personal data from users or supplying such data to third parties as a condition for delivering its 'free' product" then this "could be seen as either increasing its price or as degrading the quality of its product").

18 CMA Final Report at ¶ 6.31.

19 *See, e.g.*, Press Release, Bundeskartellamt, Preliminary Assessment in Facebook Proceeding: Facebook's Collection and Use of Data from Third-Party Sources Is Abusive (Dec. 19, 2017), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2 [https://perma.cc/PUS6-SRFS] (finding that Facebook abused its dominant position "by making the use of its social network conditional on its being allowed to limitlessly amass every kind of data generated by using third-party websites and merge it with the user's Facebook account").

20 CMA Final Report at ¶¶ 5.85 (finding that "Google has been able to generate higher click-through rates and revenue per impression, through increasing ad load") & 5.188 (finding that "the number of impressions served per hour on Facebook has increased from [40–50] in 2016 to [50–60] in 2019" and that this "increase in ad load partly explains why Facebook's revenue per hour is greater than other platforms and has increased in the past four years"); Furman Report at 43 ("As advertising revenues of Google, Facebook, and more recently Amazon increase, there are signs that the volume of advertising consumers are exposed to is also on the rise."); States Facebook Compl. ¶ 250 (alleging that as a result of Facebook's unlawful conduct and harm to competition, "the quality of the user experience on the Facebook platform has been significantly degraded by, among other things, the increased ad load to which users are subjected on the Facebook platform").

21 Digital Markets Act at 33.

22 House Report at 7; *see also id.* at 387 ("It is unclear whether the antitrust agencies are presently equipped to block anticompetitive mergers in digital markets. The record of the

Federal Trade Commission and the Justice Department in this area shows significant missteps and repeat enforcement failures.").

23 Ryan Tracy, *FTC Says Several Tech Antitrust Probes Are Under Way*, Wall St. J. (Nov. 18, 2019), https://www.wsj.com/articles/ftc-says-multiple-antitrust-probes-are-under-way-11574100990.

24 Federal Trade Commission, *Hearings on Competition and Consumer Protection in the 21st Century*, https://www.ftc.gov/policy/hearings-competition-consumer-protection (last visited Mar. 2, 2021) ("examining whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection law, enforcement priorities, and policy," including hearings on multi-sided platforms, acquisitions of nascent and potential competitors in digital technology markets; privacy, big data, and competition; data security; and the FTC's approach to consumer privacy).

25 House Judiciary Committee Investigation into Competition in Digital Markets, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4382 (outlining 2021 hearings by the Congressional antitrust subcommittee to examine proposals to address gatekeeper power and lower entry barriers).

26 Complaint, Utah v. Google, No. 3:21-cv-05227 (N.D. Cal. July 7, 2021), https://www.naag.org/multistate-case/utah-et-al-v-google-llc-no-321-cv-05227-n-d-cal-july-7-2021/; Complaint, Texas v. Google, No. 4:20-cv-957 (E.D. Tex. Dec. 16, 2020), https://www.texasattorneygeneral.gov/sites/default/files/images/admin/2020/Press/20201216% [https://perma.cc/LTF3-K8XS] [hereinafter Tex. Google Compl.]; Colo. Google Complaint; States Facebook Compl.

27 The Commission has cases or investigations involving Google, Apple, Facebook, and Amazon.

28 Germany's competition authority, for example, expanded its investigation of Facebook after the country expanded its competition law "to take preventive measures which can contribute decisively to curbing the market power of the large digital platforms." Bundeskartellamt, Press Release, Amendment of the German Act against Restraints of Competition (Jan. 19, 2021), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2 nn=3591568 [hereinafter Bundeskartellamt Jan. 2021 Press Release]; Emily Braganza, *Germany Competition Regulator Extends Scope of Proceedings Against Facebook-Oculus Linkage*, Jurist (Jan. 29, 2021), https://www.jurist.org/news/2021/01/germany-competition-regulator-extends-scope-of-proceedings-against-facebook-oculus-linkage/ [https://perma.cc/WDP5-47UB]; *see also* Sam Shead, *Google Agrees to Change Global Advertising Practices as France Imposes Unprecedented $268 Million Fine*, CNBC (June 7, 2021).

29 The Australian Competition and Consumer Commission in 2019 was investigating, among other things: access restrictions imposed by a digital platform on a third-party app developer; Google's representations to some users about the control users have over Google's

collection of location data; representations by Google about its privacy policy, and the level of disclosure about subsequent privacy policy changes that enabled Google to combine or match different sets of user data; and Facebook's representations as to the nature of its services and the scope of its terms and conditions, including terms and conditions that allowed user data to be shared with third parties, and whether Facebook's terms of use and privacy policies contain unfair contract terms. ACCC Final Report at 38.

30 *See, e.g.*, ACCC Final Report at 13 & 142 (recommending the creation of a specialist digital platforms branch within the agency "to build on and develop expertise in digital markets and the use of algorithms, with the purpose of: proactively monitoring and investigating instances of potentially anti-competitive conduct and conduct causing consumer harm by digital platforms, which impact consumers, advertisers or other business users (including news media businesses); taking action to enforce competition and consumer laws relating to the conduct of digital platforms; conducting inquiries and making recommendations to Government to address consumer harm and impediments to the efficient and effective operation of the markets in which digital platforms operate, caused by market failure"); Federal Trade Commission, FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets, February 26, 2019 (announcing the creation of a task force dedicated to monitoring competition in U.S. technology markets, investigating any potential anticompetitive conduct in those markets, and taking enforcement actions when warranted); Competition Bureau of Canada, Building Trust to Advance Competition in the Marketplace—The Competition Bureau of Canada 2018–2019 Annual Plan (May 30, 2018), https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04371.html (creating a Chief Digital Enforcement Officer and building capacity in the digital enforcement, given the "increasing risks of anti-competitive behaviour that may not be easily detected using traditional methods" and prioritizing digital economy investigations with high impact and consumer focus).

31 Digital Markets Act at 12 (calling for "[r]egular and continuous . . . (i) monitoring on scope-related issues (e.g. criteria for the designation of gatekeepers, evolution of the designation of gatekeepers, use of the qualitative assessment in the designation process); (ii) monitoring of unfair practices (compliance, enforcement patterns, evolution); and (iii) monitoring as a trigger for the launch of a market investigation with the purpose of examining new core platform services and practices in the digital sector"); ACCC Final Report at 13 (noting "the opacity and complexity" of the digital markets make it difficult to detect issues and can limit the effectiveness of broad principles, and considering, as a result, whether existing investigative tools under competition and consumer law "should be supplemented with additional proactive investigation, monitoring and enforcement powers to achieve better outcomes for Australian businesses and consumers"); CMA Final Report at ¶ 7.50.

32 Ken Buck, House Judiciary Committee, Subcommittee on Antitrust, Commercial, and Administrative Law, *The Third Way*, https://buck.house.gov/sites/buck.house.gov/files/wysiwyg_uploaded/Buck%20Report.pdf

[https://perma.cc/6WH3-TLQ7].

33 House Report at 391 & 400 (citing antitrust scholars Thomas J. Horton, *Rediscovering Antitrust's Lost Values*, 16 U.N.H. L. Rev. 179 (2018); Harry First & Spencer Weber Waller, *Antitrust's Democracy Deficit*, 81 Fordham L. Rev. 2543, 2556 (2013) ("[D]espite a history of bipartisan congressional support for the importance of the antitrust laws and their enforcement, of late Congress has done little. And when it has done something, it has focused on the micro rather than the macro changes that have occurred in the field.")).

34 House Report at 392.

35 House Report at 396; *see also* Spencer Weber Waller, *The Omega Man or the Isolation of U.S. Antitrust Law*, 52 Conn. L. Rev. 123 (2020) (discussing the growing isolation of U.S. antitrust law as more than just a transatlantic divide, but the global community's rejecting the current U.S. narrow antitrust jurisprudence in favor of a broader vision of what competition law means, what legal rules are appropriate, and how they should be enforced).

36 House Report at 396–97.

37 House Report at 398; *see also* American Choice and Innovation Online Act, H.R. 3816, 117th Congress, 1st Session; American Innovation and Choice Online Act, S. 2992, 117th Congress, 1st Session; Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2021, H.R. 3849, 117th Congress, 1st Session, § 4, https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=4591 [hereinafter ACCESS Act]; States Facebook Compl. ¶¶ 213–214; FTC Facebook Compl. ¶ 155.

38 American Choice and Innovation Online Act, H.R. 3816, § 2(b); House Report at 398; *see also* Google Compl.; Tex. Google Compl.

39 House Report at 397 (recommending eliminating the Supreme Court's recoupment element, which has effectively nullified the cause of action, even with evidence of intentional predation).

40 House Report at 398–99; *see also* CMA Report Appendix P, ¶¶ 3.132–3.134; Colo. Google Compl.; American Choice and Innovation Online Act, H.R. 3816, § 2(a); The Ending Platform Monopolies Act, H.R. 3825, 117th Congress, 1st Session.

41 House Report at 398–99; *see also* CMA Report Appendix P, ¶¶ 3.132–3.134.

42 House Report at 399.

43 House Report at 399 (clarifying that "market definition is not required for proving an antitrust violation, especially in the presence of direct evidence of market power").

44 OECD, *Big Data: Bringing Competition Policy to the Digital Era Executive Summary* (Apr. 26, 2017), http://www.oecd.org/competition/big-data-bringing-competition-policy-to-the-digital-era.htm.

45 Digital Markets Act Art. 6(1)(b) (requiring gatekeepers to allow end users to un-install any preinstalled software applications (with one technical-related exception)); American Innovation and Choice Online Act § 2(b)(5); Google Compl. ¶¶ 47, 175, 182; CMA Final Report at ¶ 89.

46 *See, e.g.*, Digital Markets Act Art. 6(1)(h) (requiring gatekeeper to "provide effective portability of data generated through the activity of a business user or end user and shall, in

particular, provide tools for end users to facilitate the exercise of data portability, in line with Regulation EU 2016/679, including by the provision of continuous and real-time access"); ACCESS Act § 3 (giving the FTC new authority and enforcement tools to establish pro-competitive rules for data portability online).

47 *See, e.g.*, Digital Markets Act Art. 6(1)(c) (requiring gatekeeper to "allow the installation and effective use of third party software applications or software application stores using, or interoperating with, operating systems of that gatekeeper and allow these software applications or software application stores to be accessed by means other than the core platform services of that gatekeeper") & (f) (requiring gatekeeper to "allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services"); ACCESS Act § 4 (requiring a covered platform to maintain "a set of transparent, third-party-accessible interfaces (including application programming interfaces) to facilitate and maintain interoperability with a business user" that complies with the standards issued under the act); House Report at 384–87 (recommending that Congress consider measures to promote data interoperability and portability to encourage competition by lowering entry barriers for competitors and switching costs by consumers).

48 Digital Markets Act Art. 6(1)(j) (requiring gatekeeper to "provide to any third party providers of online search engines, upon their request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data"); CMA Final Report at ¶ 8.43; House Report at 20, 385–87.

49 Institute of Chartered Accountants in England & Wales, *Domestic Digital Services Taxes Put Pressure on OECD Proposals*, https://www.icaew.com/insights/tax-news/2020/dec-2020/domestic-digital-services-taxes-put-pressure-on-oecd-proposals (last visited Mar. 2, 2021) [https://perma.cc/AX9X-35JK].

50 David McCabe, *Maryland Approves Country's First Tax on Big Tech's Ad Revenue*, N.Y. Times (Feb. 13, 2021) [https://perma.cc/46E9-YZ3E].

51 Brian Witte, *Maryland Lawmakers Move Ahead with First Tax on Internet Ads*, NBC Washington (Feb. 12, 2021), https://www.nbcwashington.com/news/local/maryland-lawmakers-move-ahead-with-first-tax-on-internet-ads/2572674/ [https://perma.cc/9RL8-298Z] (imposing a tax based on global annual gross revenues for companies that make more than $100 million globally, and the tax rate would be 2.5% for businesses with gross annual revenue of $100 million; 5% for companies with revenue of $1 billion or more; 7.5% for companies with revenue of $5 billion or more and 10% for companies with revenue of $15 billion or more).

52 *See, e.g.*, Australian Government Response and Implementation Roadmap for the Digital Platforms Inquiry (Dec. 12, 2019), https://treasury.gov.au/publication/p2019-41708; ACCC Final Report at 34–35 (recommending updating the definition of personal information to capture potential online

identifiers of individuals; strengthening privacy notifications and consent requirements with pro-consumer privacy defaults; enabling the erasure of personal information; private causes of action for privacy violations; and higher penalties under the privacy statute); *Hearing on Online Platforms and Market Power Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. (July 30, 2020) (Statement of Margrethe Vestager Executive Vice-President, European Commission), http://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-20200729-SD007.pdf [hereinafter Vestager July 30 Statement to Congress] ("One port of call to limit the potential consumer detriment of this 'data hungriness' of large platforms is strong privacy regulation.").

53 Digital Markets Act Art. 5(a) (gatekeeper must refrain "from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679").

54 Digital Markets Act Art. 13 (requiring gatekeeper to annually "submit to the Commission an independently audited description of any techniques for profiling of consumers that the gatekeeper applies to or across its core platform services identified pursuant to Article 3" of the Act).

55 European Commission Press Release IP/20/2484, Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Conditions (Dec. 17, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484.

56 See comments of MIT Professor Nancy Rose, Declining Competition: A Transatlantic Challenge (March 15, 2021), https://www.bruegel.org/events/declining-competition-a-transatlantic-challenge/; Speech "Preserving Competition The Only Solution, Evolve," by David I. Gelfand, Deputy Assistant Attorney General for Litigation, U.S. Department of Justice, Antitrust Division, Remarks as Prepared for the Loyola 2015 Antitrust Colloquium, Chicago, Illinois (April 24, 2015), https://www.justice.gov/atr/file/518896/download.

57 Furman Report at 93 & 96–97; ACCC Final Report at 30 & 105 (recommending amending merger law to incorporate in the agency's assessment "(i) the likelihood that the acquisition would result in the removal from the market of a potential competitor; and (ii) the nature and significance of assets, including data and technology, being acquired directly or through the body corporate"); Competition and Antitrust Law Enforcement Reform Act, 117th Congress, 1st Session, https://www.klobuchar.senate.gov/public/_cache/files/e/1/e171ac94-edaf-42bc-95ba-85c985a89200/375AF2AEA4F2AF97FB96DBC6A2A839F9.sil21191.pdf.

58 The Platform Competition and Opportunity Act of 2021, H.R. 3826, 117th Congress, 1st Session (prohibiting the largest online platforms from engaging in mergers that would eliminate competitors, or potential competitors, or that would serve to enhance or reinforce

monopoly power); The Competition and Antitrust Law Enforcement Reform Act of 2021, S. 225, 117th Congress, 1st Session, https://www.govinfo.gov/content/pkg/BILLS-117s225is/pdf/BILLS-117s225is.pdf; House Report at 387–88.

59 House Report at 395–96 (recommending that "Congress explore presumptions involving vertical mergers, such as a presumption that vertical mergers are anticompetitive when either of the merging parties is a dominant firm operating in a concentrated market, or presumptions relating to input foreclosure and customer foreclosure"); Statement of Chair Lina M. Khan, Commissioner Rohit Chopra, and Commissioner Rebecca Kelly Slaughter on the Withdrawal of the Vertical Merger Guidelines, FTC File No. P810034 (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596396/statement_of_chair_l

60 Digital Markets Act Art. 12; ACCC Final Report at 10 (recommending that "large digital platforms should each agree to a protocol to notify the ACCC of proposed acquisitions that may impact competition in Australia") & 109; House Report at 388 (recommending that dominant platforms "be required to report all transactions and no HSR deadlines would be triggered").

61 Platform Competition and Opportunity Act of 2021 §§ 2(a) & (b)(3); *see also* House Report at 394–95.

62 House Report at 395.

63 House Report at 388 (recommending that Congress "consider shifting presumptions for future acquisitions by the dominant platforms"); Platform Competition and Opportunity Act of 2021 § 2(b) (shifting the burden to the acquiring covered platform operator to demonstrate "by clear and convincing evidence" that one of the proposed statute's exceptions applies).

64 *See*, *e.g.*, Paul Sandle, *Britain Proposes Tailored Competition Rules for Google and Facebook*, Reuters (Dec. 8, 2020), https://www.reuters.com/article/britain-technology-regulation/britain-proposes-tailored-competition-rules-for-google-and-facebook-idUSKBN28I1A5; 2019–2020 Parliament of the Commonwealth of Australia, House of Representatives, Treasury Laws Amendment (News Media And Digital Platforms Mandatory Bargaining Code) Bill 2020, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6652_ems_2fe103c0-0f60-480b-b878-1c8e96cf51d2/upload_pdf/JC000725.pdf;fileType=application%2Fpdf; CMA Final Report at ¶¶ 77–82, 123, 7.50 (outlining other jurisdictions' proposals); ACCC Final Report at 37 (amending the law so that unfair contract terms are identified and prohibited (not just voidable), and imposing civil pecuniary penalties when they are used in any standard form consumer or small business contract); House Report at 382–84 (recommending that Congress consider establishing nondiscrimination rules to target the powerful platforms' self-preferencing, ensure fair competition and promote innovation online) & 391 (recommending that "Congress consider prohibiting the abuse of superior bargaining power, including through potentially targeting anticompetitive contracts, and introducing due process protections for individuals and businesses dependent on the dominant platforms"); American Choice and Innovation Online Act, H.R. 3816, 117th Cong., 1st Session (seeking to "restore competition online and ensure that digital markets are fair

and open by preventing dominant online platforms from using their market power to pick winners and losers, favor their own products, or otherwise distort the marketplace through abusive conduct online"). In June 2019, the European Council of the European Union adopted a regulation that seeks to improve relationships between digital platforms and businesses, by providing businesses with a more transparent, fair and predictable online business environment, as well as an efficient system for seeking redress. Regulation (EU) 2019/1150 of June 20, 2019. *See also* Dina Srinivasan, *Why Google Dominates Advertising Markets*, 24 Stan. Tech. L. Rev. 55 (2020) (proposing porting the rules of financial market regulation to new electronic trading markets like digital advertising).

65 The Digital Markets Act would apply to gatekeepers that (a) have a significant impact on the EU internal market; (b) have a core platform service that serves as an important gateway for business users to reach end users; and (c) enjoy an entrenched and durable position in their operations or it is foreseeable that they will enjoy such a position in the near future. Core platform services include: (i) online intermediation services (e.g., marketplaces, app stores and online intermediation services in other sectors like mobility, transport or energy); (ii) online search engines; (iii) social networking; (iv) video sharing platform services; (v) number-independent interpersonal electronic communication services; (vi) operating systems; (vii) cloud services; and (viii) advertising services, including advertising networks, advertising exchanges and any other advertising intermediation services, where these advertising services are being related to one or more of the other core platform services mentioned above. Digital Markets Act Art. 2(2) & 3.

66 European Commission, Press Release, Digital Markets Act: Ensuring Fair and Open Digital Markets (Dec. 17, 2020), https://ec.europa.eu/cyprus/news_20201216_2_en.

67 European Commission Press Release IP/20/977, Antitrust: Commission Consults Stakeholders on a Possible New Competition Tool (June 2, 2020), https://ec.europa.eu/commission/presscorner/detail/en/IP_20_977; Digital Markets Act at 20.

68 Digital Markets Act Art. 22 (proposing that the Commission in case of urgency due to the risk of serious and irreparable damage for business users or end users of gatekeepers, to order interim measures against a gatekeeper on the basis of a prima facie finding of an infringement of the DMA). For an example under current EC competition law, *see* European Commission Press Release IP/19/6109, Antitrust: Commission Imposes Interim Measures on Broadcom in TV and Modem Chipset Markets (Oct. 16, 2019), https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6109; *see also* Bundeskartellamt Jan. 2021 Press Release, *supra* note 19.

69 When it has reasonable grounds for believing that competition is not working effectively in a market, the U.K. competition authority can use powers under its antitrust laws to obtain information and conduct research for "a wide consideration of issues affecting the market," including a range of outcomes, such as imposing orders to remedy anticompetitive effects, and issuing "recommendations to government, enforcement action and referral for market investigation." UK Competition and Markets Authority Press Release: CMA Launches Immediate Review of Audit Sector (Oct. 9, 2018),

https://www.gov.uk/government/news/cma-launches-immediate-review-of-audit-sector.

70 Bundeskartellamt Jan. 2021 Press Release, *supra* note 19.

71 *Id.*

72 Vlad Savov, *Google to Open App Store Payments to Comply With South Korea Law*, Bloomberg (Nov. 3, 2021), https://www.bloomberg.com/news/articles/2021-11-04/google-opening-app-store-payments-to-comply-with-south-korea-law.

73 Open App Markets Act, S. 2710, 117th Congress, 1st Session, https://www.congress.gov/bill/117th-congress/senate-bill/2710/text?r=41&s=1.

74 Digital Markets Act Art. 5(c) (allowing business users to promote offers and conclude contracts with end users, both through the gatekeeper's core platform services and through alternative channels); 5(f) (preventing gatekeepers from requiring business users or end users to use any other core platform services as a condition to access the gatekeepers' core platform service); and 6(c) (allowing the installation of third-party software applications and software application stores and allow such software to be accessed outside of the gatekeeper's core platform services).

75 Apple, Press Release, Japan Fair Trade Commission Closes App Store Investigation (Sept. 1, 2021), https://www.apple.com/newsroom/2021/09/japan-fair-trade-commission-closes-app-store-investigation/.

76 Digital Markets Act Art. 5(g) (requiring gatekeeper "to provide advertisers and publishers to which it supplies advertising services, upon their request, with information concerning the price paid by the advertiser and publisher, as well as the amount or remuneration paid to the publisher, for the publishing of a given ad and for each of the relevant advertising services provided by the gatekeeper"); CMA Final Report at ¶¶ 102–104; ACCC Final Report at 12.

77 ACCC Final Report at 32 (recommending codes of conduct on designated digital platforms to govern their relationships with news media businesses to "ensure that they treat news media businesses fairly, reasonably and transparently in their dealings with them, and provide commitments on the sharing of data with news media businesses, the early notification of changes to the ranking or display of news content, that the digital platform's actions will not impede news media businesses' opportunities to monetise their content appropriately on the digital platform's sites or apps, or on the media businesses' own sites or apps, and where the digital platform obtains value, directly or indirectly, from content produced by news media businesses, that the digital platform will fairly negotiate with news media businesses as to how that revenue should be shared, or how the news media businesses should be compensated"); House Report at 389 (recommending inquiry into legislation "to provide news publishers and broadcasters with a narrowly tailored and temporary safe harbor to collectively negotiate with dominant online platforms").

78 John E. Kwoka & Diana L. Moss, *Behavioral Merger Remedies: Evaluation and Implications for Antitrust Enforcement*, 57 Antitrust Bull. 979 (2012); John Kwoka, Mergers, Merger Control, and Remedies: A Retrospective Analysis of U.S. Policy (2014).

79 Digital Markets Act Art. 16(2).

80 CMA Final Report at ¶ 8.203 (recommending that the new agency "should have powers to implement ownership separation or operational separation," which would include "powers to monitor the effectiveness of any separation requirements, and to vary the terms of separation where necessary to ensure their ongoing effectiveness").

81 FTC Facebook Compl. at 51 (seeking "divestiture of assets, divestiture or reconstruction of businesses (including, but not limited to, Instagram and/or WhatsApp)"); States Facebook Compl. at 75. The district court dismissed the states' complaint with prejudice, which the states have appealed, and dismissed the FTC's complaint with the opportunity to amend, which the FTC did. Google Compl. ¶ 194(b); Colo. Google Compl. ¶ 233(c); Tex. Google Compl. ¶¶ 19, 357(f).

82 *See, e.g.*, The Ending Platform Monopolies Act, H.R. 3825, 117th Congress, 1st Session (prohibiting a covered platform "to own or control in a line of business other than the covered platform that (1) utilizes the covered platform for the sale or provision of products or services; (2) offers a product or service that the covered platform requires a business user to purchase or utilize as a condition for access to the covered platform, or as a condition for preferred status or placement of a business user's products or services on the covered platform; or (3) gives rise to a conflict of interest"); House Report at 378–80 (recommending exploration of structural separations that would "prohibit a dominant intermediary from operating in markets that place the intermediary in competition with the firms dependent on its infrastructure" and line of business restrictions would "generally limit the markets in which a dominant firm can engage").

83 Jacky Wong, *Google and Facebook's Trouble Down Under Will Spread*, Wall St. J. (Feb. 17, 2021), https://www.wsj.com/articles/google-and-facebooks-trouble-down-under-will-spread-11613559457.

84 Naaman Zhou, *Google's Open Letter to Australians about News Code Contains "Misinformation," ACCC Says*, The Guardian (Aug. 17, 2020), https://www.theguardian.com/technology/2020/aug/17/google-open-letter-australia-news-media-bargaining-code-free-services-risk-contains-misinformation-accc-says [https://perma.cc/NPQ6-9JE3].

85 *Marketplace Tech: New Antitrust Legislation Would Check the Power of Tech Giants*, Marketplace (Feb. 11, 2021), https://www.marketplace.org/shows/marketplace-tech/new-antitrust-legislation-would-check-the-power-of-tech-giants/ [https://perma.cc/S2AV-2FGL].

86 Jeff Horwitz, *Facebook to Prohibit Sharing of News Content in Australia*, Wall St. J. (Feb. 17, 2021), https://www.wsj.com/articles/facebook-to-prohibit-sharing-of-news-content-in-australia-11613591775.

87 Jeff Horwitz, *supra* note 87.

88 Damien Cave, *Facebook's New Look in Australia: News and Hospitals Out, Aliens Still In*, N.Y. Times (Feb. 18, 2021) https://www.nytimes.com/2021/02/18/business/media/facebook-australia-news.html [https://perma.cc/6Q3G-LCYX].

89 Elena Debré, *In Australia, Facebook Blocks News (and Everything Remotely Newsworthy)*, Slate (Feb. 18, 2021), https://slate.com/technology/2021/02/australia-facebook-

news-blackout.html [https://perma.cc/6GWL-5QFS].

90 Michelle Toh, *Facebook Signs Deal with Murdoch's News Corp Australia After Media Law*, CNN Business (Mar. 16, 2021), https://www.msn.com/en-us/news/world/facebook-signs-deal-with-murdochs-news-corp-australia-after-media-law/ar-BB1eCX56.

91 Digital Markets Act at 2 & 5 (noting how these powerful "gatekeepers typically operate cross-border, often at a global scale and also often deploy their business models globally" and need for coordination at EU level).

92 OECD Consumer Data Rights and Competition, *supra* note 16, at ¶ 193 (quoting Wolfgang Kerber, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection*, J. Intell. Prop. L. & Prac. 856 (2016), http://dx.doi.org/10.1093/jiplp/jpw150); *see also Common Understanding of G7 Competition Authorities on "Competition and the Digital Economy, Paris, 5th June 2019,"* (https://www.ftc.gov/system/files/attachments/press-releases/ftc-chairman-supports-common-understanding-g7-competition-authorities-competition-digital-economy/g7_common_understanding_7-5-19.pdf) [https://perma.cc/7HH3-BLXR] (calling for the promotion of greater international cooperation and convergence); ACCC Final Report at 29 (noting that "[c]oordination across national borders is critical" to address the "competition and consumer concerns that arise from the conduct of the leading digital platforms, given their global operations," and how the ACCC's proposed digital platforms branch would "work closely with equivalent teams at overseas competition agencies and overseas consumer agencies," as this coordination "will enable competition and consumer agencies to learn from each other, enhance cross-border enforcement and, where appropriate, share information and align their approaches to meet the same objectives"); Yan Carrière-Swallow & Vikram Haksar, *The Economics and Implications of Data: An Integrated Perspective*, International Monetary Fund Policy Paper No. 19/16 (Sept. 23, 2019), https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596, at 5 (arguing "that international coordination is needed to achieve the minimum data policy principles that are compatible with productive cross-border data economies").

93 Cave, *supra* note 85.

# 4
# Why Isn’t Competition the Easy Fix?

The antidote seemingly is more competition. Just as competition erodes monopoly pricing, so too it can curb the data-opoly’s surveillance and extraction of data. While often true, such as when Facebook initially offered better privacy protections to compete against Myspace and deter inroads from Google+,[1] it is not always true. Increasing competition will not always improve our privacy in many digital markets. Why? Behavioral advertising. When market participants depend on behavioral advertising for their revenues, their incentives are not aligned with our privacy interests, and increasing the level of competition will not cure the problem. As Roger McNamee observed, “The competition for attention across the media and technology spectrum rewards the worst social behavior.”[2]

As we will see, many advertisers, app developers, and website publishers cannot opt out of this toxic competition. Like nuclear weapons, it would be better if no one engages in behavioral advertising. But once a publisher or advertiser turns to behavioral advertising, rivals must follow or pay a competitive price. Thus, even without data-opolies, the competition would still be toxic.

We will next see why Google and Facebook primarily benefit from the status quo. As Ariel Ezrachi and I discuss in our 2020 book, *Competition Overdose*, Google and Facebook designed a competitive process for online advertising that helps them maintain their dominance and where they ultimately profit. We called these creators the “Gamemakers” after the characters who go by that name in *The Hunger Games* book and film trilogy. There is seemingly much competition, but the game is devised so that the Gamemaker always wins.

We are left with a market failure where one traditional policy response—competition—will not necessarily work. Instead, policymakers must develop new tools to tackle the myriad risks posed by these data-opolies.

## A. Why Many Publishers Find It Hard to Opt Out of Behavioral Advertising

Consider the once-mighty mapping company, TomTom, whose quarterly

revenues plummeted in 2008.[3] What prompted the decline? Its CEO attributed three factors: the economic crisis in 2008, smartphones becoming popular, and Google offering navigation for free on Android-powered phones.[4]

As advertisers know, "free" captivates us.[5] It is hard for an app or website publisher to charge a fee when many rivals do not.[6] Think of it, unless the website or app is offering something unique and desirable (such as a movie available only on Netflix), we will likely opt for the free option. Free helps us hedge our bets. If we do not like the app, news story, or website, we move on. Other than our time, we seemingly have not invested in the "free" option. If we like the free offering, then we saved some money.

Knowing that free attracts us, most websites and app developers (whom we'll call *publishers*) offer their service for free but still have to monetize content.[7] They can offer a free trial period, a free basic version with premium upgrades, or added-on paid services. Many rely on advertising revenues. Nevertheless, even in markets not dominated by data-opolies, many publishers compete by finding ingenious ways to capture our attention and personal data.[8]

To compete for advertising revenue, most publishers must engage in behavioral advertising rather than contextual ads (which are targeted based on the app's or website's content, such as sports or woodworking). If publishers do not, they are at a significant competitive disadvantage.

To see why suppose an individual (whom we will call John Doe 123) is interested in buying a luxury SUV. While John Doe 123 is online, luxury SUV manufacturers (like Audi, BMW, Toyota's Lexus, and Mercedes) will want to target him and will pay a higher amount (say $100) for the advertising space than other categories of advertisers. Suppose John Doe 123 is about to visit a woodworking website. Knowing that the visitor is indeed John Doe 123, the woodworking website can use that information to entice the SUV manufacturers to bid for the publisher's ad space. But suppose the woodworking website does not know that the person is John Doe 123 and his interest in buying an SUV. In that case, the luxury SUV manufacturers will unlikely bid for the ad space (or if they do, they will offer substantially less).[9] That makes sense as most people who visit woodworking websites are unlikely to purchase a new car (much less a luxury SUV) in the next few weeks.

Not surprisingly, in the current online display market, when the website or exchange cannot identify the person about to visit the website, the price that advertisers are willing to pay "can fall by about 50 percent."[10] Some advertisers

simply will not bid for the impression.[11] As the competition authorities have found from their market studies, the publishers are only "rewarded by advertisers for having extensive and up-to-date knowledge of their consumers' characteristics, preferences and behavior," which is derived from surveillance data.[12] As the FTC noted,

> YouTube offered channel owners the option to disable behavioral advertising and instead use contextual ads, a less precise method of anticipating ads to which a viewer might respond. But YouTube cautioned channel owners that turning off behavioral ads "may significantly reduce [the] channel's revenue." The unspoken concern was that it also would reduce how much money YouTube would make.[13]

Thus, to maximize advertising revenue, publishers must engage in behavioral advertising if their rivals also engage in behavioral advertising. If they do not, they pay a hefty price. The U.K. competition authority estimated that U.K. publishers "earned around 70% less revenue when they were unable to sell personalised advertising but competed with others who could."[14]

But to sell behavioral ads (such as the luxury SUV ad targeted at John Doe 123) rather than contextual ads (which are targeted based on the content of the publisher's woodworking website or profile of the typical visitors), the publishers need lots of personal data and metadata, which is the data about the data and "describes where the user was when he or she posted, what they were doing, with whom they were doing it, alternatives they considered, and more."[15] Indeed the more interactive data collected on John Doe 123 through greater surveillance, predictions, and observations, the better one can predict his interests, weaknesses, and aspirations, and manipulate his emotions and, ultimately, his behavior. Suppose that John Doe 123 might be interested in refinancing his home mortgage to purchase the luxury SUV and take a two-week vacation. With this data, other advertisers will likely bid for the opportunity to target John Doe 123. If we understand why John Doe 123 wants an SUV and his aspirations for the vacation, that opens possibilities for other advertisers to target him. Once we know why some ads were more effective than others in getting John Doe to behave in the desired way, we can better predict which ads will likely have the intended effect. That increases the bidding. Behavioral advertising has evolved beyond predicting what John Doe 123 wants (e.g., a new SUV) to manipulating his behavior. In using emotional marketing to trigger his desires, whether to buy the SUV, endorse it to friends, or create a community

around the brand, even more advertisers are competing to induce John Doe 123 with their pitch. Emotional marketing is a game-changer for advertising, as the Facebook investor and advisor McNamee noted, since Google and Facebook help advertisers "to exploit the emotions of users in ways that increase the likelihood that they purchase a specific model of car or vote in a certain way."[16]

Advertising generally skews incentives, as the founders of Google recognized.

Back in 1998, when their search engine was not dependent on advertising revenues, Google's founders Sergey Brin and Lawrence Page predicted that "advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers."[17] They laid out how advertising can distort a search engine's incentives and warned of the "insidiousness" of the resulting search bias. Given these risks, the young entrepreneurs believed "that it is crucial to have a competitive search engine that is transparent and in the academic realm."

Behavioral advertising skews incentives even more. As WhatsApp's founders, quoting the movie *Fight Club*, explained:

> "*Advertising has us chasing cars and clothes, working jobs we hate so we can buy shit we don't need.*"
>
> . . .
>
> *Advertising isn't just the disruption of aesthetics, the insults to your intelligence and the interruption of your train of thought. At every company that sells ads, a significant portion of their engineering team spends their day tuning data mining, writing better code to collect all your personal data, upgrading the servers that hold all the data and making sure it's all being logged and collated and sliced and packaged and shipped out.*[18]

Fundamentally, in a behavioral advertising business model, data is collected about us, but not necessarily for us. We are not the customer but the target. FTC Commissioner Chopra noted how Facebook's behavioral advertising business model is the root cause of its widespread and systemic privacy problems:

> Facebook flagrantly violated the FTC's 2012 order by deceiving its users and allowing pay-for-play data harvesting by developers. The company's behavioral advertising business, which monetizes user behavior through mass surveillance, contributed to these violations. Cambridge Analytica's tactics of profiling and targeting users were a small-scale reflection of Facebook's own practices.
>
> Here, Facebook's behavioral advertising business model is both the company's profit engine and arguably the root cause of its widespread and systemic problems. Behavioral advertising generates profits by turning users into products, their activity into assets, their communities into targets, and social media platforms into weapons of mass manipulation. We need to recognize the dangerous threat that this business model can pose to our democracy and economy.[19]

To gather data to manipulate us and target us with behavioral ads, apps and websites must attract us and sustain our attention.[20]

Consequently, the ethical publisher faces a Hobson's choice—(i) opt out of behavioral advertising and watch its ad revenues plummet—on average by 70%, which can effectively kill its business; (ii) change to a freemium subscription model (which puts it at a significant competitive disadvantage to the free apps and websites); or (iii) stick with behavioral advertising revenues, until enough dedicated followers are willing to pay for its app or service. Most cannot afford to opt out of this toxic competition. They must continue finding ways to profile us, surveil us, and manipulate our behavior. To attract and drive up the bidding for their advertising space, they effectively sell us (and our ability to be manipulated).

## B. "Competing with One Arm Behind Your Back"—Why Many Advertisers Find It Hard to Opt Out of Behavioral Advertising

Advertisers are likewise ensnared in this toxic competition. Behavioral advertising is generally perceived to produce better results than traditional contextual advertising. After all, if the luxury SUV manufacturer only targets visitors of car-related websites and apps, it will lose the ability to influence the behavior of millions of other likely purchasers when they visit other websites. It might also be relatively cheaper to target a *Wall Street Journal* reader interested in buying a luxury SUV when they visit the woodworking website than when reading the newspaper.

For example, among the data Google provides the company Mondelez International Inc., which sells cookies under the brands Oreo, Chips Ahoy!, and

Tate's Bake Shop, is how people tend to search for healthy foods in the morning and "for more indulgent treats as the day wears on."[21] Working with Target and Google, the company in 2021 was calculating how likely someone would buy its cookies after seeing ads on YouTube. The snacking company gets a 25% better return on digital ads than TV ads and gets a 40% higher return with Google and Facebook behavioral ads than the average digital ad.[22] Likewise, activewear company Vuori relies on behavioral advertising to increase sales. While the company could identify the age, demo and behavior of its customers, Vuori's CEO concluded that Facebook's algorithm "is much more powerful in terms of identifying people who demonstrate certain shopping behaviors."[23]

What ensues, as one market participant told Congress, is toxic competition among advertisers:

> Basecamp saw this first-hand when we experimented with targeted advertising back in 2017. We ended up spending tens of thousands of dollars with Facebook, primarily on targeted ads using the audience look-alike matching feature. These ads performed better than any other type of internet advertisement we tried at the time. Facebook's targeting capability is crushingly effectively, and therefore truly terrifying.
>
> At Basecamp, we ultimately ended up swearing off the use of targeted advertisement based on the exploitation of personal data. Facebook's record of protecting people's privacy, and gathering their consent in the exploitation of their data for advertisement purposes, is atrocious, and we decided that we wanted no part of it.
>
> But choosing to opt out of targeted advertisement on the internet is like competing with one arm behind your back. It is very clear why most companies feel compelled to do this kind of advertisement, even if it's a violation of their ethics. If their competitors are doing it, they're at a significant disadvantage if they don't. And the same is true for us. We have undoubtedly given up growth to competitors because we've refrained from pursuing targeted ads.[24]

Behavioral advertising is not limited to simply providing us with relevant ads of things we want. Data-opolies and marketers collect this massive amount of data precisely to better predict and manipulate our behavior—to target us or, in the case of Facebook, our teenage children when they feel "worthless," "insecure," "defeated," "anxious," "silly," "useless," "stupid," "overwhelmed," "stressed," and "a failure."[25] As the privacy scholar Paul M. Schwartz observed, "The more that is known about a person, the easier it is to control him."[26] When *The New York Times*, for example, reviewed hundreds of Facebook's patent applications, their review revealed how

> the company has considered tracking almost every aspect of its users' lives: where you are, who you spend time with, whether you're in a romantic relationship, which brands and politicians you're talking about. The company has even attempted to patent a method for predicting when your friends will die.[27]

Facebook would not invest in this surveillance technology unless it helped advertisers induce us to buy things we otherwise would not have purchased at the highest price that we are willing to pay.[28]

Thus, advertisers recognize that most of us do not want this intrusive surveillance.[29] To realize better value from their campaigns and outcompete rivals, however, advertisers are encouraged to rely on emotion analytics and facial coding, where algorithms process our facial expression and voice, to manipulate our behavior: "the more people feel, the more they spend."[30] Even if the ethical advertiser finds this surveillance and manipulation morally repugnant, many cannot afford to opt out, and a race to the bottom ensues.

## C. Why More Competition Cannot Fix the Problems Caused by Behavioral Advertising

The disturbing realization is that this toxic competition would exist even without the data-opolies. Millions of free websites and apps compete to attract millions of advertisers to target billions of users every minute of every day with behavioral ads. To succeed in this competition, websites and apps need detailed, up-to-date data about us, which in turn increases the demand to track us online and offline. As the legal scholar Frank Pasquale observed, "In an era where Big Data is the key to maximizing profit, *every* business has an incentive to be nosy."[31]

While publishers can track our behavior while we are on their websites and apps, they also need to track us for the rest of the day. So publishers invite "third-party trackers" on their websites and apps who follow us online. As the browser Mozilla states,

> Third-party trackers are bad.
>
> Third-party trackers are placed by a website you haven't even visited. They come from separate entities—sometimes vast ad networks—you've never heard of and almost certainly didn't agree to share your information with. These third parties are able to place trackers on sites across the web, thereby collecting tons of data about you and sharing it with whomever they want. Yah, it's kind of creepy.[32]

So, who precisely is tracking us? Two scholars from Princeton University sought to find out. They examined the extent of online tracking on the top one million websites and found over 81,000 third-party trackers.[33] Not every website had trackers. On the one hand, websites that were less dependent on advertising revenues (such as governmental, nonprofit, and university websites) were far less likely to track users.[34] On the other hand, those websites that lacked an external funding source and relied primarily on advertising revenue, like news sites, had the most trackers on their websites.[35]

While the 2016 Princeton study identified many third-party trackers (over 81,000), some track us far more extensively than others. Many companies track us only on a few websites. Of these 81,000 third-party trackers, only 123 were tracking us on more than 10,000 websites. Only four companies—Google, Facebook, Twitter, and AdNexus—had trackers on more than 100,000 websites. And, as we will see later in this chapter, only Google and Facebook tracked us on hundreds of thousands of websites.

One insight from this 2016 study is that the more dependent a website is on advertising revenue, the more likely it will allow others to track you. After all, behavioral advertising turns users into products. Another insight is how robustly competitive this surveillance economy is. While two data-opolies sit on top of the surveillance food chain, 81,000 rivals would be happy to displace them.

With so many companies competing to track us, smartphones now pose significant national security risks.[36] As the National Security Agency warned in 2020, opting out of being tracked is impossible, even for U.S. military and intelligence officers. The NSA tells the military to disable "advertising permissions to the greatest extent possible" and set "privacy settings to limit ad tracking, noting that these restrictions are at the vendor's discretion."[37] But even then, the NSA recognizes that the military, like the rest of us, will be tracked, often without their knowledge, as was the case with TikTok.[38]

Thus, even if Instagram and WhatsApp were spun off from Facebook, behavioral advertising and the toxic competition it propagates would persist. Many of the 81,000 third-party trackers would likely try to expand their surveillance network to better track and manipulate our behavior.

Because behavioral advertising skews the market participants' incentives, we have, as two officials from the International Monetary Fund (IMF) note, a market failure:

> . . . data involves externalities: The collection, sharing, and processing of personal data by one agent imposes costs on others by affecting their privacy. An implication is that a market for data lacking sufficient user control rights—where data collectors do as they please with the data they collect—is likely to lead to excessive data collection and too little privacy.[39]

Without adequate privacy protections, even robustly competitive markets will not function in ways to promote our privacy. As the IMF officials add,

> To the extent that privacy is not internalized in the economic decisions of data collectors and processors, the market will tend toward the collection of excessive personal data and insufficient protection of privacy. For the market for data to internalize this externality, the rights of data subjects must be adequately attributed.[40]

So, privacy laws are needed to correct the fundamental misalignment of incentives caused by behavioral advertising. This is not as easy as one might think. As Alastair Mactaggart, one of the drivers of California's two recent privacy statutes, observed, "If you think about our other fundamental rights as a country, no one is spending millions and millions of dollars trying to undermine the First Amendment or the freedom of religion. But people are actually spending hundreds of millions of dollars trying to undermine privacy because there's so much money in it for corporations."[41] That is especially true when the data-opolies, including Apple through its deal with Google, reap billions of dollars in profits from behavioral advertising each quarter.

### D. Why Data-opolies Have the Incentive to Maintain the Status Quo

If behavioral advertising skews incentives and promotes toxic competition, how can data-opolies make things worse? Google and Facebook have become the "de facto regulators" of online advertising,[42] and we pay the price. As the U.K. competition authority noted, the platforms "both set the rules and are the sole arbiters of whether they abide by them."[43] In their quasi-regulatory capacity, Google and Facebook set "the rules around data sharing not just within their own ecosystems, but for other market participants."[44] Data-opolies can "write one set of rules for others, while they play by another," and impose "their own private quasi regulation that is unaccountable to anyone but themselves."[45]

Besides overseeing and setting the rules for behavioral advertising, Google and Facebook also reap monopoly profits from the status quo. While they claim

to be significant rivals, Google and Facebook in 2018 struck a deal.[46] According to the Texas-led states' antitrust complaint, Facebook "agreed not to compete with Google's online advertising tools in return for special treatment when [Facebook] used them."[47] As a result of the deal, Google, according to an internal presentation, would "avoid competing with" Facebook and would collaborate to "build a moat."[48] The endgame was to "collaborate when necessary to maintain status quo . . ."[49] And the status quo benefits these two data-opolies, as one industry executive testified before Congress:

> Facebook and Google have captured a duopoly on all growth in internet advertisement spending over the last several years. In a report on the growth in internet advertisement from 2016, it was revealed that 99% of all growth that year was captured by just these two companies: Google took 54%, Facebook took 45%, and everyone else was left with the last 1%. This is as clear an example of market failure as they come.[50]

Online behavioral advertising, especially display advertising, requires making predictions on human behavior, which requires personal data.[51] With their significant data advantage, Google and Facebook capture most of the digital advertising revenues, as Figure 4.1 reflects, with Amazon a distant third.[52]

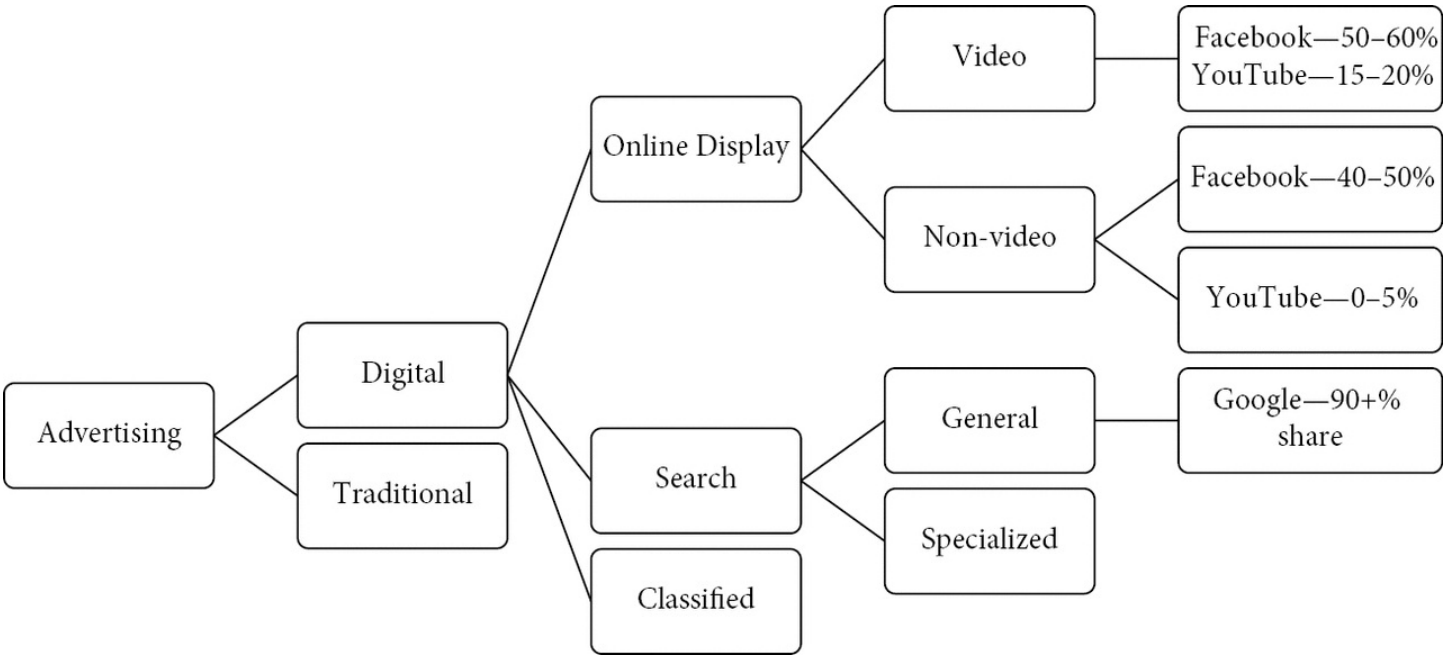


**Figure 4.1** How the antitrust authorities, when assessing market power, delineate different online advertising markets

*Source:* CMA Final Report

The more data the data-opolies accumulate by surveilling us, and the more time the data-opolies get us to spend engaging their services, the more money they make through their advertising businesses.[53] As the U.K. competition authority found, by

> expanding the breadth and variety of online services provided, Google and Facebook are able to gather increasing amounts of the two critical inputs to the digital advertising market: consumer attention and data. This in turn results in greater advertising revenues, enabling them to invest at a greater rate than their rivals, which creates a feedback loop that further cements their powerful position.[54]

By 2018, Google and Facebook extracted 58% of the $111 billion in revenues from the digital ad market—which was more than all of their online competitors combined.[55] In some countries, like the United Kingdom and Australia, Google and Facebook capture about 80% of the billions spent on digital advertising.[56]

To break this down, Google dominates the general search advertising market, controlling over 90% of revenues in the United States, EU member states, and many other counties.[57] Advertisers in the United States "pay about $40 billion annually to place ads on Google's search engine results."[58] That's about $109,589,041 per day. In four days, Google collects more advertising revenue in the United States alone from its search engine than what *The New York Times* collected in advertising revenue for an entire year ($392.4 million in 2020).

Thus, Google benefits from the status quo as it "faces little competitive constraint, either from suppliers of general search advertising or from suppliers of specific search advertising."[59] Google can increase the demand for paid advertising by decreasing the quality of its organic search results.[60] For example, search on your phone for some popular topics, like car insurance. You might have to scroll down a couple pages of search results before seeing any organic (non-paid) search results. Google knows that most of us click the results on the first page of search results. So, it front-loads the number of paid search ads on the first couple pages of results, reduces the number of organic search results on the first two pages, and blurs the distinction between paid and organic search results. Websites that previously relied on these organic search results for traffic now must compete against each other to get their paid search ads on the first two pages of results to prevent the traffic to their websites from plummeting.[61] Basically, Google profits from degrading quality.

Facebook also benefits from the status quo, as it controls the bulk of online

display advertising generally and social advertising in particular, with over 10 million active advertisers in 2020.[62] Based on the U.K. competition authority's calculations in 2020, Facebook controls between 45 and 55% of the U.K.'s online display market, with an even higher share for online display video advertising (with a 50 and 60% share).[63] Facebook generated $84.17 billion in advertising revenue in 2020, or $230,602,739.73 per day.[64] In just two days, Facebook collected more advertising revenue worldwide than *The New York Times* collected in 2020.

Together Google and Facebook generated more advertising revenues in 34 days in 2019 than all the newspapers across the United States collectively made in 2018.[65] Neither data-opoly invests in journalism or content generally but relies on others (including the newspapers and us) for the content. So how have Google and Facebook, which derive most of their revenues from advertising,[66] dominated the online advertising market? By the personal data they collect[67] and in sustaining our attention.[68] Personal data gives Google and Facebook insights on attracting us and keeping us within their ecosystem longer, whether reading stories on Facebook or watching YouTube videos. "Over a third of U.K. internet users' total time online is spent on sites owned by Google and Facebook," which enables them to gather substantially more data than their rivals.[69] With their commanding data- and attention-advantage, both data-opolies, to a significant extent, can set the terms to advertisers and publishers.[70]

## E. Navigating the Ad Tech Stack

Besides reaping monopoly profits from behavioral advertising on their own platforms, Google, and to a lesser extent Facebook, also orchestrate the toxic competition for behavioral display ads on millions of other websites and apps.

To compete for behavioral advertising revenue, websites and apps need attention and personal data, both of which Google and Facebook have. But Google and Facebook do not sell our data. They do not need to. Instead, they sell prediction services to publishers and advertisers.[71]

To see why, let us return to our woodworking publisher example. To generate revenues for its "free" content, the website must sell its ad space. Like millions of other publishers, the woodworking website will rely on programmatic advertising, which brings together advertisers and publishers via online auctions.[72] It is an auction for each particular person about to open an app or visit

a webpage, as the Texas-led states allege in their antitrust complaint:

> One might think that a website with three pages and three different ad slots per page would have a total of nine unique ad units to sell. But because online ads are targeted at individual users, the same site with 1,000,000 readers actually has 9,000,000 different ad units to sell: each of the website's impressions targeted to each unique reader.[73]

The publishers use sell-side software to sell these impressions on ad exchanges. Likewise, advertisers typically use buying software to purchase these impressions on these advertising exchanges. Although the auction process differs for small and large publishers and advertisers,[74] Figure 4.2 summarizes the key intermediaries on the buy- and sell-side.

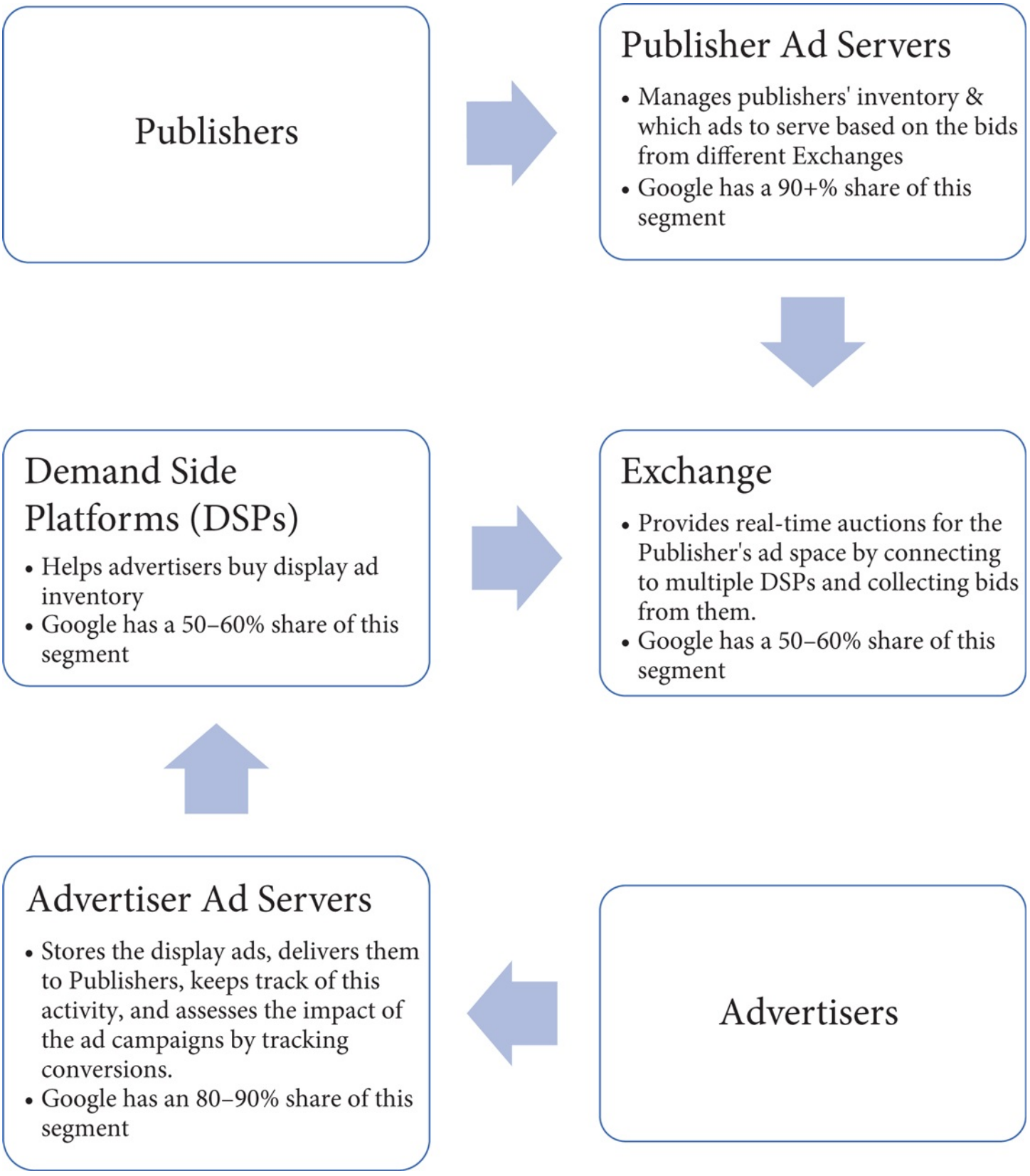


**Figure 4.2** Key intermediaries for online display advertising

*Source:* CMA Final Report

The woodworking website likely relies on a publisher ad server to manage its

ad inventory and determine if the advertising space has been already committed (such as a direct deal with the advertiser). More than likely, it has not. So, the publisher ad server identifies who is about to visit the website (John Doe 123) and electronically sends a request to one or more exchanges (which have historically been called Supply Side Platforms (SSPs)) of the opportunity to target him with a display ad.[75]

One or more exchanges will orchestrate the real-time auction for advertisers wishing to target John Doe 123 on the woodworking website. These exchanges send bid requests to multiple demand side platforms (DSPs).

The DSPs represent large advertisers, like the luxury SUV manufacturers in our example. (Smaller advertisers are routed through ad networks.) The DSPs buy inventory from many publishers for their advertising clients. So the DSPs will evaluate this opportunity for their luxury SUV clients and other clients. Based on their clients' objectives and the data on the user (such as whether John Doe 123, in our example, is of high value), the DSPs will submit bids on the exchange.

Each exchange then ranks the bids from the different DSPs and sends them to the publisher ad server. The publisher ad server compares the bids from the different exchanges and ultimately decides which display ad to serve John Doe 123 on its client's woodworking website. When the webpage opens, John Doe 123 sees the ad (let us say for a BMW SUV).

The advertiser ad server helps BMW by storing its ads and delivering them to the publisher's webpage. It also analyzes the performance of the ad campaign and tracks conversions.[76] So what did John Doe 123 do after seeing the ad for the BMW X models of SUVs? He might have clicked the ad or continued looking for plans to build an Adirondack chair. But John Doe 123 later might visit the BMW website. Or he might read some reviews of the latest BMW SUVs. This requires the ability to track John Doe both on- and offline.

Figure 4.3 summarizes the display ad auction process in the milliseconds between John Doe 123 clicking on the woodworking website and when the website page appears with the display ad.

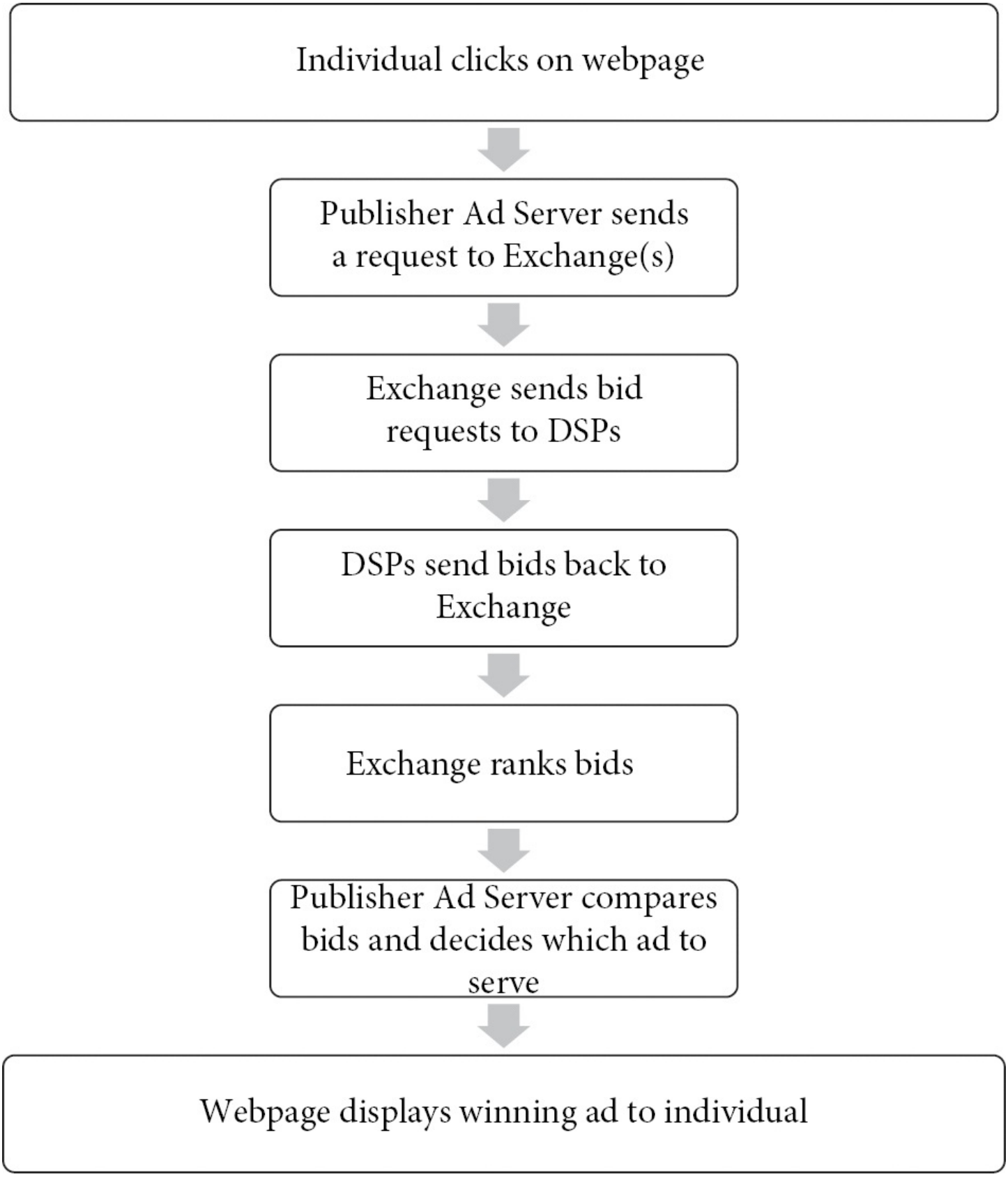


**Figure 4.3** The online display ad auction process

As John Doe 123 clicks on another webpage, it creates another opportunity to influence him with another behavioral ad. This auction process continues 24

hours per day, as we are each tracked and targeted, with our responses monitored to better predict and manipulate our behavior.

Although the markets for these intermediation services might appear robustly competitive, they aren't. Given its data advantage, Google dominates the buy-side and the sell-side of the critical online display ad intermediation services and controls the largest exchange and ad network.[77] As U.S. Senator Richard Blumenthal observed, "in no other markets does the same party represent the seller, the buyer, make the rules, and conduct the auction."[78] Or, as the Texas-led states allege in their 2020 complaint, "In this electronically traded market, Google is pitcher, batter, and umpire, all at the same time."[79]

### 1. Google's Dominance on the Sell-Side

When a publisher wants to sell space on its website or app for display advertising, it must compete against Facebook and Google. But the winner is already ordained. Those with the more extensive surveillance network, who can sustain our attention longer and better manipulate our behavior, wield power and collect the profits. As we saw, the woodworking website to entice advertisers, like BMW, to bid for the impression, needs up-to-date data on that website visitor (John Doe 123 in our example) and his interests. Plus, the woodworking website needs personal data for attribution, namely, what John Doe 123 did after seeing the ad, which also requires up-to-date data that only comes from continual surveillance.

Google, and to a lesser extent Facebook, offer publishers the opportunity to join their advertising network to gain access to potential advertisers and the personal data on each of us.

In exchange for joining Google's or Facebook's ad network, the publisher agrees to extract a lot of personal data about its users and deliver that information to the data-opoly.[80] So the data-opoly installs tracking code and software on millions of websites and apps. These trackers enable the data-opoly to automatically capture highly detailed personal information about each of us (such as when we open the app, click, swipe, view specific pages, and place items into a checkout).[81] Google and Facebook analyze the torrent of data (recall that Facebook gets one billion notifications every day from healthcare apps alone) to maintain detailed, up-to-date profiles about each of us. From its vast surveillance network, the data-opoly can identify who is interested in buying a luxury SUV (like John Doe 123) and who, with enough persuasion, might buy

one. So independent websites and apps help Google and Facebook track us, which increases the data-opolies' data advantage. With more data and opportunities to experiment on us, Google's and Facebook's prediction algorithms improve, and publishers and advertisers become more reliant on the data-opolies' ad intermediary services.

As a result, Google's and Facebook's surveillance networks far surpass the other trackers.[82] Returning to the 2016 tracking study, we see a long tail of the 81,000 trackers found on the one million websites: most third-party trackers operate only on a few websites. Facebook is tracking us on over 30% of the million most popular websites. Google tracks us on 85% of the websites.[83] Only they can perceive what we did after seeing the ad. Even after Europe's new privacy rules, the General Data Protection Regulation, went into effect, Google remains firmly in the lead (with its trackers found on 81% of the European websites) and Facebook second (44% of the EU websites).[84] Likewise, Google is the dominant tracker of apps in the Android ecosystem—it is found on 88% of 959,426 popular apps, with Facebook and Microsoft second, found on 42% of the apps.[85] So, even when a free app does not need to track you to function, like a flashlight app, it likely is.[86]

Many publishers, while complicit in this surveillance, are also victims of it. Their position is "fragile on many levels," the French competition authority noted.[87] The apps and websites lack data; they lack the data-opolies' access to advertisers, and they cannot continually track us. So, in the end, they need to be part of Google's or Facebook's surveillance network and rely on the data-opolies' ad servers.[88]

To consider the plight of publishers, consider newspapers. Data-opolies can starve newspapers many ways, as the Australian Competition and Consumer Commission found.[89] Since many people now get their news online, the local newspapers depend on the data-opolies for traffic to their websites.[90] A change in the data-opoly's algorithm, whether for Facebook's news feed, Google's search engine, or Apple News, can divert traffic away from a news story, even if it is a solid piece of journalism.[91] Moreover, the data-opolies provide us with snippets of the newspapers' stories, which can hurt the newspapers in branding their news and increase the risk of fake news.[92]

Like many publishers, traditional news organizations cannot meaningfully compete against Google and Facebook for behavioral advertising revenue.[93] Instead, these sharecroppers on Google's and Facebook's massive industrial

farms[94] watch the data-opolies siphon their readers and revenue and steer advertisers to wherever the data-opoly profits the most.

Thus, Google and Facebook primarily benefit from this toxic competition where publishers battle to attract us and extract our data, which is funneled to the data-opolies, reinforcing their competitive advantage. Meanwhile, the share of online advertising going to third-party websites and apps is shrinking as Google and Facebook grab more ad revenue.[95] Consider the sweets manufacturer Mondelez. By 2021, it steered between 60% and 70% of its digital ad spending directly to Google and Facebook (up from around 50% in 2017). By 2021, it worked with fewer than 10 online publishers (in contrast to approximately 150 in 2017).[96] As the antitrust scholar Dina Srinivasan noted,

> In 2007, approximately 36% of the advertising revenue that Google booked went to non-Google properties, like The Post and The Register, that also sell their ad space through Google's intermediary tools and exchange. Almost every year since 2004 this split has widened, in Google's favor. By Q1 2020, the share going to non-Google properties had decreased to 15%. The lion's share of Google's $134 billion in advertising revenue went to Google's own.[97]

Thus, millions of publishers watch their revenues shrink as they work harder to please their powerful masters.

## 2. Google's Dominance of the Buy-Side

Let us return to our example and suppose BMW wants to advertise on Google's and Facebook's properties, and perhaps on other websites and apps. To target John Doe 123 with behavioral ads, BMW will likely rely on programmatic advertising on the buy-side.[98]

To bid for the available display ad inventory and connect to the real-time auctions, BMW will likely enlist a Demand Side Platform.[99] More likely than not, BMW and other large advertisers will use Google's ad-buying tools, which have a 50 to 60% market share.

Here, Google can leverage its dominance on the sell-side and over the leading exchange to stifle competition on the buy-side. First, in representing nearly all the publishers, Google funnels the publishers' advertising inventory to its own ad exchange and ad network.[100] But as the Gamemaker, Google can further manipulate the results. It steers the valuable impressions (such as targeting John Doe 123 looking to buy a luxury SUV) to its exchange and funnels the lower-

value impressions (say, Tony Smith, who is not looking to buy much of anything) to publishers' direct deals.[101] Thus to access the higher-value impressions, advertisers must use Google's exchange.[102]

Next, Google can use its control over the leading exchange to favor its buy-side tools with "information and speed advantages when bidding on behalf of advertisers."[103] As a result, Google's anticompetitive strategies "lock in" publishers and advertisers and help the company's ad-buying tools "win more than 80% of auctions on its exchange."[104] This tells advertisers that if they want to improve their odds of winning the rigged auction, they must use Google's ad-buying tools.

But why stop there? Google also leverages its strength from its YouTube video platform, where we are increasingly spending more time, to force many advertisers to use its DSP services. On mobile phones alone, YouTube reaches more 18–34-year-olds in the United States than any TV network.[105] According to one 2020 study, 80% of U.S. children younger than 12 watch videos on YouTube, and among that group, over half use YouTube daily.[106] As we spend a lot of time on YouTube, advertisers need to advertise there. To tighten the screws, Google tells advertisers that if they want to advertise on YouTube, the second most popular outlet for display advertising after Facebook,[107] then the advertiser must also use Google's DSP services. Advertisers typically use only one DSP per ad campaign.[108] Google, by tying its YouTube inventory with its DSP services, squeezes out other DSP providers, thereby helping Google maintain its dominance on the buy-side.[109]

Finally, BMW will likely require the help of an Advertiser Ad Server, which stores the display ads, delivers them to publishers, keeps track of this activity, and assesses the ad campaigns' impact by tracking conversions. Google dominates this market too.[110]

So, Google profits in steering advertisers to its own platforms, like search, Maps, and YouTube. But even when advertisers place ads elsewhere, Google still profits. Regardless of which advertiser wins the bid or which publisher gets the advertisement, Google, as the Gamemaker, collects the data. But it also collects an "ad tech tax." which is the "difference between what advertisers pay and what publishers earn from digital advertising."[111]

*See also* Tex. Google Compl. ¶¶ 242–49 (alleging how withholding "YouTube caused competition on the buy-side to flounder," as "[m]any DSPs stopped growing, many others went out of business, and the market overall has been

closed to entry") & 102 (alleging how Google required (until 2013) small advertisers seeking to purchase Google Search inventory to use its buy-side tools, another factor that helped Google attain a monopoly in the market for ad buying tools for small advertisers).

## 3. Google's Collection of the Ad Tech Tax

Suppose BMW spends $10 million on a particular ad campaign. How much do the websites and apps that publish the ads get? As Figure 4.4 shows, on average between $6.4 and $6.5 million. The rest is the ad tech tax, which Google primarily collects.

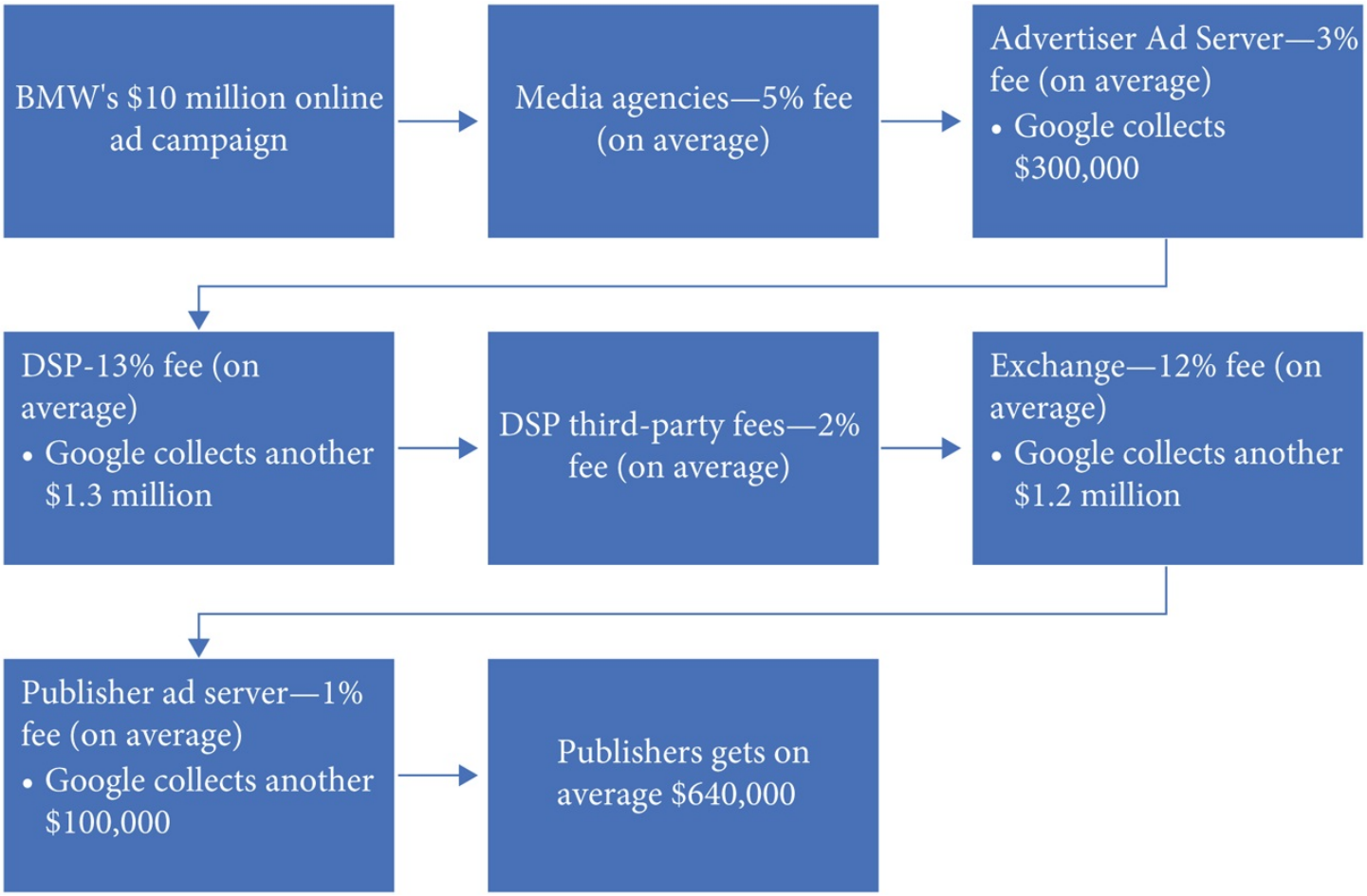


**Figure 4.4** Breaking down the ad tech tax

*Source:* CMA Final Report Figure 2.8

Thus, if BMW spends $10 million on the online ad campaign, the intermediaries on average take 35% according to the UK competition authority.[112] In the United States, Google takes a cut of 22% to 42% of U.S. ad spending that goes through its systems, and Google's ad exchange typically

charges two to four times as much in fees as those charged by rival digital advertising exchanges.[113]

These percentages came from competition authorities in their investigations of the display advertising markets. But no one else really knows how much Google takes, as Google does not tell the publishers and advertisers what it collects along the way for each transaction.[114] We ultimately pay the tax through higher prices (or lower quality) for the advertised goods and services.[115]

## F. Reflections

The online advertising market has at least four fundamental problems.

*First*, Google and Facebook, as the Gamemakers, orchestrate the toxic competition so that they ultimately win. They made the digital advertising market, which is already complex, even more opaque.[116] As a result, advertisers can't determine "whether the services they purchase offer 'value for money.' "[117] The opacity harms the publishers, who cannot "determine whether the ad tech platforms they contract with are the most efficient or not, as comparison between platforms is difficult."[118] The lack of transparency leads to worse outcomes for advertisers and publishers while increasing Google's and Facebook's profits and power as unavoidable trading partners.[119]

*Second*, multiple conflicts of interest exist. Because Google represents most sellers and buyers, controls the leading exchange, and competes against the sellers with its own inventory, Google, in this intentionally opaque advertising ecosystem, can influence which ads are served on its exchange and at which price; and which inventory is bought on behalf of advertisers.[120]

*Third*, since the data-opolies profit from the status quo, they have less incentive to reform it. Google's and Facebook's 2019 revenues ($161.857 billion and $70.697 billion, respectively)[121] exceeded the Gross Domestic Product of over 110 countries.[122] During the 2020 pandemic, Facebook's revenues increased to $85.97 billion,[123] which exceeded the GDP of 125 countries. Google's revenues increased to $182.5 billion,[124] which exceeded the GDP of all but 52 countries. Thus, as the principal regulators and beneficiaries of online advertising, they will continue to direct where many online ads appear, whether on our computers, mobile phones, or connected TVs.

The *fourth* and biggest fundamental problem is that competition will not fix it. Suppose Google had to divest YouTube, Waze, its online ad exchange, and either

its buy- or sell-side ad tools. Suppose Instagram and WhatsApp were spun off as separate companies. Also, suppose the ensuing competition reduced the ad tech tax from 35% to 10%. Would we better off?

In some ways, we would. Newspapers, for example, might recover more ad revenue that could be invested in investigative reporting.

Nevertheless, the underlying competition would remain toxic. The legal scholar Frank Pasquale observed in 2014 how 4,000 data brokers, ranging "from giants like Acxiom, a publicly traded company that helps marketers target consumer segments, to boutiques like Paramount Lists, which has compiled lists of addicts and debtors" were competing to "vacuum up data from just about any source imaginable: consumer health websites, payday lenders, online surveys, warranty registrations, Internet sweepstakes, loyalty-card data from retailers, charities' donor lists, magazine subscription lists, and information from public records."[125]

You might have heard about the father who went to the local Target store, asking why the retailer sent his teenage daughter coupons for prenatal vitamins and maternity clothing. Target, like almost every major retailer, "from grocery chains to investment banks to the U.S. Postal Service, has a 'predictive analytics' department devoted to understanding not just consumers' shopping habits but also their personal habits, so as to more efficiently market to them."[126] The store knew before her father that the teenager was pregnant. Target uses predictive analysis to gain an advantage over other retailers.

But that story seems quaint to the surveillance and manipulation tools used today. If you gamble online, then the gambling app's data-profiling software might be invasively tracking you and profiling your weaknesses to get you to gamble more.[127] Consider one customer who tried to quit. The gambling app Sky Bet, from its surveillance, knew the customer was having financial difficulties. Nonetheless, it emailed the customer, knowing his penchant for playing slots, with "a chance to win more than $40,000 by playing slots." The gambling app's marketing software flagged that he was likely to open this email, and the app's "predictive model even estimated how much he would be worth if he started gambling again: about $1,500."[128] As Ravi Naik, a London lawyer who helped the customer obtain his personal data from the gambling app, observed, "They had taken his addiction and turned it into code."[129]

With or without these data-opolies, it remains a classic race to the bottom. That is why so many apps collect far more data about us, including our

movements, than what's necessary ask for the apps to work.[130] Our geolocation data, like us, are for sale—whether to advertisers, Wall Street banks,[131] or governmental agencies seeking to spy on us.[132] The toxic competition has already advanced from predicting to manipulating behavior. Machine learning is "already at or beyond human-level performance in discerning a person's emotional state on the basis of tone of voice or facial expression."[133] Once an algorithm can predict what stimuli will make you happy or sad, it can manipulate particular emotions for desired results, whether to buy or endorse a product, vote for a specific candidate, or refrain from voting.[134]

In the end, as FTC Commissioner Noah Phillips observed, breaking up these data-opolies will not end the toxic competition: "We could easily end up with two, three or more different entities, each as eager to exploit user data as the next."[135] Thus, the policymaker's handy tool—increasing competition—will not work when the market participants' incentives are misaligned with our privacy interests.

To correct this market failure, we need to realign incentives, where data is collected about us and *for us*. One way is to give us greater control over our personal data, which leads us to the next fundamental issue: Who owns the data, and is that even the right question?

---

1 Complaint, New York v. Facebook, No. 1:20-cv-03589-JEB (D.D.C., Dec. 9, 2020), https://ag.ny.gov/sites/default/files/state_of_new_york_et_al._v._facebook_inc._-_filed_public_complaint_12.11.2020.pdf [https://perma.cc/GYC7-44RX] ¶¶ 73–78; 92–97 [hereinafter States Facebook Compl.].

2 Roger McNamee, Zucked: Waking Up to the Facebook Catastrophe 91 (2019).

3 Charles Arthur, *Navigating Decline: What Happened to TomTom?*, The Guardian (July 21, 2015), https://www.theguardian.com/business/2015/jul/21/navigating-decline-what-happened-to-tomtom-satnav [https://perma.cc/7JHK-LP3H] (noting TomTom's 66% decline in revenues between its last quarter in 2007 and first quarter in 2009).

4 Arthur, *supra* note 3.

5 Allen Finn, *We Analyzed 612 of the Best Google Ads: Here Are 9 Things We Learned*, WordStream (Sept. 26, 2020), https://www.wordstream.com/blog/ws/2017/06/06/best-ads [https://perma.cc/W9BQ-XJEG] (free was the second most popular word in the top performing text ads on Google).

6 For some of the antitrust-related issues relating to free markets, *see* John M. Newman, *Antitrust in Zero-Price Markets: Applications*, 94 Wash. U.L. Rev. 49 (2016); Michal S. Gal & Daniel L. Rubinfeld, *The Hidden Costs of Free Goods: Implications for Antitrust*

*Enforcement*, 80 Antitrust L.J. 521 (2016); John M. Newman, *Antitrust in Zero-Price Markets: Foundations*, 164 U. Pa. L. Rev. 149 (2015).

7 *See, e.g.*, *Distribution of Free and Paid iOS Apps in the Apple App Store as of January 2021*, Statista (Feb. 4, 2021), https://www.statista.com/statistics/1020996/distribution-of-free-and-paid-ios-apps/ [https://perma.cc/H5JA-E62W] (92.7% of apps in the Apple App Store were free as of January 2021); *Distribution of Free and Paid Android Apps in the Google Play Store as of January 2021*, Statista (Feb. 4, 2021), https://www.statista.com/statistics/266211/distribution-of-free-and-paid-android-apps/ [https://perma.cc/GRQ7-J4WN] (96.7% of apps in Google Play Store were free as of January 2021).

8 UK Competition & Markets Authority, Online Platforms and Digital Advertising Market Study: Market Study Final Report (July 1, 2020), https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digit [https://perma.cc/DA5V-RHA5] [hereinafter CMA Final Report] at ¶¶ 59 & 60 (noting that the two critical inputs to the digital advertising market are consumer attention and data); N.Y. State Dept. of Financial Services, Report on Investigation of Facebook Inc. Data Privacy Concerns (Feb. 18, 2021), https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf at 17–18 [hereinafter NY State Facebook Report].

9 Dina Srinivasan, *Why Google Dominates Advertising Markets*, 24 Stan. Tech. L. Rev. 55, 94 (2020).

10 Complaint, Texas v. Google, No. 4:20-cv-957 (E.D. Tex. Dec. 16, 2020), https://www.texasattorneygeneral.gov/sites/default/files/images/admin/2020/Press/20201216% [https://perma.cc/LTF3-K8XS] [hereinafter Tex. Google Compl.] ¶ 126:

> Publishers, and the exchanges that sell inventory on their behalf, need to know the identity of users associated with publishers' impressions in order to sell those impressions for competitive prices. User IDs permit publishers and their exchanges to understand the value of inventory, cap the number of times that users see the same ad, and effectively target and track online advertising campaigns. When exchanges cannot identify users in auctions (e.g., through cookies), the prices of impressions on exchanges can fall by about 50 percent, according to one Google study.

11 Srinivasan, *supra* note 9.

12 CMA Final Report at ¶ 2.11.

13 Leslie Fair, *$170 Million FTC-NY YouTube Settlement Offers COPPA Compliance Tips for Platforms and Providers*, FTC Business Blog (Sept. 4, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/09/170-million-ftc-ny-youtube-settlement-offers-coppa [https://perma.cc/H9PB-69PQ].

14 CMA Final Report at ¶ 44.

15 McNamee, *supra* note 2, at 68; *see also* NY State Facebook Report at 5 (noting how

"Facebook collects information from its users through metadata embedded in the content a user provides, what a user sees through features such as Facebook or Instagram's Camera, and information shared with other users through personal messages").

16 McNamee, *supra* note 2, at 69.

17 Sergey Brin & Lawrence Page, *The Anatomy of a Large-Scale Hypertextual Web Search Engine*, Stan. Infolab Pub. Serv., http://ilpubs.stanford.edu:8090/361/ (last visited Mar. 3, 2021) [https://perma.cc/ZMF4-4XRB].

18 Majority Staff of H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial and Administrative Law, Report and Recommendations: Investigation of Competition in Digital Markets (2020), https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429 [https://perma.cc/29LN-L4BL] [hereinafter House Report] at 156 (quoting *Why We Don't Sell Ads*, WhatsApp (June 18, 2012), https://blog.whatsapp.com/why-we-don-t-sell-ads).

19 Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* Commission File No. 1823109 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_st24-19.pdf.

20 House Report at 135.

21 Keach Hagey & Suzanne Vranica, *How Tech's Triopoly Won the Advertising Game*, Wall St. J. B8 (Mar. 20, 2021).

22 *Id.*

23 *Id.*

24 *Hearing on Online Platforms and Market Power Part 5: Competitors in the Digital Economy Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. 70 (Jan. 17, 2020) (Statement of David Heinemeier Hansson, CTO & Cofounder, Basecamp), https://www.govinfo.gov/content/pkg/CHRG-116hhrg40788/pdf/CHRG-116hhrg40788.pdf [hereinafter Hansson Congressional Statement].

25 Michael Reilly, *Is Facebook Targeting Ads at Sad Teens?*, MIT Tech. Rev. (May 1, 2017), https://www.technologyreview.com/s/604307/ [https://perma.cc/9DMS-GB4A]; McNamee, *supra* note 2 at 69; Sam Levin, *Facebook Told Advertisers It Can Identify Teens Feeling "Insecure" and "Worthless,"* The Guardian (May 1, 2017), https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens [https://perma.cc/7HBD-78C5].

26 Paul Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 Am. J. Compar. L. 675 (1989), https://doi.org/10.2307/840221.

27 Sahil Chinoy, *What 7 Creepy Patents Reveal about Facebook*, N.Y. Times (June 21, 2018), https://nyti.ms/2MGqm7T [https://perma.cc/98ZY-9A2P].

28 For elaboration on behavioral discrimination, *see* Ariel Ezrachi & Maurice E. Stucke, Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy (2016).

29 CMA Final Report at ¶ 4.68.

30 Shoshana Zuboff, The Age of Surveillance Capitalism 284 (2019) (quoting https://blog.realeyesit.com/play-your-audience-emotions-to-stay-on-top-of-the-game); *see also* Sophie Kleber, *Three Ways AI Is Getting More Emotional*, *in* Artificial Intelligence: The Insights You Need From Harvard Business Review 142 (Thomas H. Davenport et al., eds. 2019); Ariel Ezrachi & Maurice E. Stucke, How Big-Tech Barons Smash Innovation—and How to Strike Back (2022).

31 Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information 81 (2015).

32 A tracker "is a script on websites designed to derive data points about your preferences and who you are as you interact with their site." *No-Judgment Digital Definitions: What Is a Web Tracker?*, Firefox Frontier (Oct. 22, 2019), https://blog.mozilla.org/firefox/what-is-a-web-tracker/ [https://perma.cc/N6Q7-JMG2].

33 Steven Engelhardt & Arvind Narayanan, *Online Tracking: A 1-Million-Site Measurement and Analysis*, https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_mea (last visited Mar. 3, 2021) [https://perma.cc/S7FK-U6AB].

34 *Id.* at ¶ 5.4

35 *Id.*

36 *Limiting Location Data Exposure*, U.S. National Security Agency (Aug. 2020), https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_D [https://perma.cc/2JRF-5N44].

37 *Id.*

38 *Id.* (warning that apps, "even when installed using the approved app store, may collect, aggregate, and transmit information that exposes a user's location. Many apps request permission for location and other resources that are not needed for the function of the app."); Kevin Poulsen & Robert McMillan, *TikTok Tracked User Data Using Tactic Banned by Google*, Wall St. J. (Aug. 11, 2020), https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738.

39 Yan Carrière-Swallow & Vikram Haksar, *The Economics and Implications of Data: An Integrated Perspective*, International Monetary Fund Policy Paper No. 19/16 (Sept. 2019), https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596, at 5.

40 *Id*. at 14.

41 Natasha Singer, *The Week in Tech: Why Californians Have Better Privacy Protections*, N.Y. Times (Sept. 27, 2019), https://www.nytimes.com/2019/09/27/technology/the-week-in-tech-why-californians-have-better-privacy-protections.html [https://perma.cc/6KUT-4VNM].

42 *EU: Vestager Considers Toughening "Burden of Proof" for Big Tech*, Competition Pol'y Int'l (Oct. 30, 2019), https://www.competitionpolicyinternational.com/eu-vestager-considers-toughening-burden-of-proof-for-big-tech/ [https://perma.cc/CZ35-AZHR].

43 CMA Final Report at ¶ 52.

44 CMA Final Report at ¶ 47.

45 Majority Staff of H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial and Administrative Law, Report and Recommendations: Investigation of Competition in Digital Markets (2020) at 7, https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429 [https://perma.cc/29LN-L4BL] [hereinafter House Report].

46 Ryan Tracy & John D. McKinnon, *Google, Facebook Agreed to Team Up Against Possible Antitrust Action, Draft Lawsuit Says*, Wall St. J. (Dec. 22, 2020), https://www.wsj.com/articles/google-facebook-agreed-to-team-up-against-possible-antitrust-action-draft-lawsuit-says-11608612219.

47 *Id.* While the complaint was heavily redacted, details were reported by the press. Facebook agreed to spend at least $500 million annually in Google-run ad auctions, and would "win a fixed percent of those auctions." *Id*. Given the agreement's antitrust risks, Google used "Jedi Blue" from the *Star Wars* movies as a code name for its deal.

48 *Id.*

49 *Id.*

50 Hansson Congressional Statement.

51 *See, e.g.*, Zuboff, *supra* note 30, at 95 (citing Microsoft research that accurately estimating the click-through rate of ads has a "vital impact" on search advertising revenue, and that increasing the accuracy rate by 0.1% would yield "hundreds of millions of dollars in additional earnings").

52 Hagey & Vranica, *supra* note 21; House Report at 171 (noting that "Facebook's advantages in terms of access to data and its reach contribute to its ability to earn higher revenue per user than other firms in the social networking market" and "Facebook reported an average revenue per user (ARPU) of $7.05 worldwide and $36.49 in the United States and Canada in July 2020"); Autorité de la Concurrence, Opinion no. 18-A-03 of 6 March 2018 on Data Processing in the Online Advertising Sector, https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2019-10/avis18a03_en_.pdf [https://perma.cc/NXW9-LBU9] [hereinafter Autorité Report]; Spencer Soper, *Amazon Increases Ad Market Share at Expense of Google, Facebook*, Bloomberg News (Sept. 19, 2018), https://www.bloomberg.com/news/articles/2018-09-19/amazon-increases-ad-market-share-at-expense-of-google-facebook [https://perma.cc/XPV7-D5M6]; Leonid Bershidsky, *The Digital Ad Market Is Overdue for Antitrust Review*, Bloomberg News (Dec. 5, 2018), https://www.bloomberg.com/opinion/articles/2018-12-05/amazon-google-facebook-are-ripe-for-a-european-antitrust-review [https://perma.cc/BNY8-NK7U]; *see also* Australian Competition and Consumer Commission, Digital Platforms Inquiry—Final Report at 66 (2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report [https://perma.cc/M36S-YQJ4] [hereinafter ACCC Final Report] ("Google and Facebook receive the majority of digital advertising revenue in Australia; and have captured more than 80 per cent of growth in digital advertising in the past three years.").

53 Complaint ¶ 3, New York v. Facebook, No. 1:20-cv-03589-JEB (D.D.C., Dec. 9, 2020), https://ag.ny.gov/sites/default/files/state_of_new_york_et_al._v._facebook_inc._-

_filed_public_complaint_12.11.2020.pdf [https://perma.cc/GYC7-44RX] [hereinafter States Facebook Compl.]; *see also id.* ¶ 44 ("The volume, velocity (freshness), and variety of Facebook's user data give it an unprecedented, virtually 360-degree view of the user and her contacts, interests, preferences, and activities, which allows Facebook to personalize content to its users that other platforms are not able to provide.").

54 CMA Final Report at ¶¶ 59 & 60.

55 Maurice E. Stucke & Ariel Ezrachi, Competition Overdose 210 (2020); *see also* Autorité Report at 6; ACCC Final Report at 122 (estimating that Google and Facebook have captured over 80% of all growth in online advertising in Australia; for a typical AU$100 spent by advertisers on online advertising (excluding classifieds): $47 goes to Google (some of which is for the provision of ad tech services); $24 goes to Facebook, and $29 goes to all other websites and ad tech).

56 CMA Final Report at ¶¶ 16 & 2.63 (estimating that Google and Facebook accrued as revenue around 80% of all expenditure on search and display advertising in the United Kingdom in 2019, including the revenue from advertising on their own platforms, as well as from intermediation services).

57 CMA Final Report at 5; ACCC Final Report at 8. Search advertising is "where advertisers pay online companies to link their company website to a specific search word or phrase so that it appears in relevant search engine results." CMA Final Report at ¶ 5.6.

58 Complaint ¶ 7, United States v. Google, No. 1:20-cv-03010 (D.D.C. Oct. 20, 2020), https://www.justice.gov/opa/press-release/file/1328941/download.

59 ACCC Final Report at 97; *see also* House Report at 196 (noting how "Google's clear dominance in online search also gives it significant control over the search advertising market," how "many firms spend the vast majority of their ad budgets on Google," and that public reports suggest that, "as of 2019, Google had increased the price of search ads by about 5% per year, exceeding the U.S. inflation rate at that time of 1.6%").

60 House Report at 201–03; McNamee, *supra* note 2, at 73–74.

61 House Report at 201–03.

62 Hagey & Vranica, *supra* note 21.

63 CMA Final Report, Figures 5.9 & 5.10. Display advertising is "where advertisers pay online companies to display advertising using a range of advertising content types shown within defined ad units on web pages or mobile apps." CMA Final Report at ¶ 5.6.

64 Facebook Inc. 2020 Form 10-K, at 52, http://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/4dd7fa7f-1a51-4ed9-b9df-7f42cc3321eb.pdf.

65 Elizabeth Grieco, *Fast Facts About the Newspaper Industry's Financial Struggles As McClatchy Files for Bankruptcy*, Pew Res. Center (Feb. 14, 2020), https://www.pewresearch.org/fact-tank/2020/02/14/fast-facts-about-the-newspaper-industrys-financial-struggles/ (noting that newspaper advertising revenue fell 62% from 2008 ($37.8 billion) to 2018 ($14.3 billion)). In 2019, Google collected $134.811 billion in advertising revenues and Facebook generated $69.66 billion in revenues. Alphabet Inc. 2019 Form 10-K, https://www.sec.gov/Archives/edgar/data/1652044/000165204420000008/goog10-

k2019.htm, at 29, https://abc.xyz/investor/static/pdf/20200204_alphabet_10K.pdf?cache=cdd6dbf; Facebook Inc. 2019 Form 10-K, at 44, http://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/45290cc0-656d-4a88-a2f3-147c8de86506.pdf.

66 Alphabet 2019 Form 10-K at 9 (generating over 83% of total revenues in 2019 from the display of ads online); Facebook Inc. 2020 Form 10-K at 52 (98% of its $85.97 billion in 2020 revenues came from advertising).

67 ACCC Final Report at 7 ("The fundamental business model of both Google and Facebook is to attract a large number of users and build rich data sets about their users. The ubiquity of these platforms and their presence in related markets enable them to build particularly valuable data sets. This enables them to offer highly targeted or personalised advertising opportunities to advertisers. . . . the breadth and depth of the ongoing data collection reinforces their market power."); Commission Decision of June 27, 2017 (Case AT. 39740--Google Search (Shopping)) ¶ 320, https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf [https://perma.cc/NH5J-APP4] ("While users do not pay a monetary consideration for the use of general search services, they contribute to the monetisation of the service by providing data with each query.").

68 ACCC Final Report at 44 (noting how Facebook's 17 million Australian monthly users spend an average of 31 minutes a day on Facebook; Australian Instagram users spend an average of 7 minutes a day, and Australian Google users (excluding YouTube) spend an average of 23 minutes a day on these respective platforms); Digital Competition Expert Panel, Unlocking Digital Competition at 25 (2019) (also known as the Furman Report), https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel [https://perma.cc/VK9M-3GV8] [hereinafter Furman Report] at 28–29 (illustrating Google's and Facebook's dominance over their rivals in capturing U.K. consumers' attention).

69 CMA Final Report at 42. In the United States, 69% used Google's services and products daily in 2017, and another 19% used them several times a week. Alexander Kunst, *How Often Do You Use Google Services and Products?*, Statista (Sept. 3, 2019), https://www.statista.com/statistics/702855/google-services-and-products-usage-frequency-in-us/.

70 Furman Report at 45; House Report at 131 (noting that in 2017, "*Business Insider* reported that Google and Facebook accounted for 99% of year-over-year growth in U.S. digital advertising revenue" and that in 2020 "advertisers and publishers alike have few options when deciding how to buy and sell online ad space").

71 Tex. Google Compl. ¶¶ 125–129; House Report at 131 (finding that "Google and Facebook both have a significant lead in the market due to their significant collection of behavioral data online, which can be used in targeted advertising," that Google and Facebook "do not provide access to this unique data in open data exchanges," and that "advertisers' only access to this information is indirect—through engagement with Google and Facebook's ad tech").

72 CMA Final Report at ¶ 2.51 (noting that while "some direct deals for display advertising continue to be made through traditional channels (ie involving human interaction), the use of programmatic technology has increased over time, with the result that almost all display advertising is now sold programmatically"). Programmatic advertising "is an automated big data system that allows organisations (predominantly retailers) to bid for the privilege to publish personalized online advertising in the right place, to the right people, at the right time." Anthony Samuel et al., *Programmatic Advertising: An Exegesis of Consumer Concerns*, 116 Comput. in Hum. Behav. 106657 (2021), https://doi.org/10.1016/j.chb.2020.106657.

73 Tex. Google Compl. ¶ 32.

74 *See* Tex. Google Compl. ¶¶ 42–60. The ad exchanges "are mostly intended for very large online publishers," while "small online publishers like local online newspapers and blogs mostly sell their web display inventory in marketplaces called 'ad networks.' " In controlling the leading ad exchange and ad network, Google "is *the* bottleneck between publishers and advertisers." *Id.* at ¶ 52. Likewise, large advertisers use Demand Side Platforms, while smaller advertisers use "pared-down analogues." *Id.* at ¶ 53. Smaller publishers and advertisers ultimately pay higher fees for Google's services. *Id.* at ¶¶ 58, 60, 85.

75 Google has hampered publishers from submitting to multiple exchanges at the same time. *See, e.g.*, Tex. Compl. ¶¶ 36, 121 (alleging that with "waterfalling and dynamic allocation, Google's ad server delivered a one-two punch to other exchanges. Google used waterfalling to block other exchanges from competing simultaneously for impressions. Then, through dynamic allocation, Google's ad server passed inside information to Google's exchange and permitted Google's exchange to purchase valuable impressions at artificially depressed prices. Publishers were deprived of competitive bids and competing exchanges were left with the low-value impressions passed over by Google's exchange."); CMA Final Report ¶ 5.276 & Appendix M.

76 Tex. Google Compl. ¶ 36.

77 CMA Final Report at ¶ 5.232 & Appendix M; Online Platforms & Digital Advertising: Market Study Interim Report at ¶¶ 5.185–5.186 (2019), https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pd [hereinafter CMA Interim Report]; Tex. Google Compl. ¶¶ 75–80.

78 *Hearing: Stacking the Tech: Has Google Harmed Competition in Online Advertising? Before the Subcomm. on Antitrust, Competition Policy, and Consumer Rights of the S. Comm. on the Judiciary,* 116th Cong. (Sept. 15, 2020), https://www.judiciary.senate.gov/meetings/stacking-the-tech-has-google-harmed-competition-in-online-advertising; Srinivasan, *supra* note 9 (discussing how, in other electronic trading markets, lawmakers do not let a single firm control the sell-side, the buy-side, and the exchange, without managing conflicts of interest).

79 Texas Google Compl. ¶ 4.

80 Google AdMob, *Get Started* (Mar. 2, 2021),

https://developers.google.com/admob/android/quick-start [https://perma.cc/QPA8-5ETJ] ("Integrating the Google Mobile Ads SDK into an app is the first step toward displaying ads and earning revenue."); Susan E. McGregor & Hugo Zylberberg, *Understanding the General Data Protection Regulation: A Primer for Global Publishers*, Tow Center for Digital Journalism, A Tow/Knight Report Columbia, at 32, 34 (Mar. 2018) [hereinafter GDPR Primer].

81 Abbas Razaghpanah et al., *Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem*, *in* Proc. of the Network & Distributed Sys. Security Symposium (San Diego, CA, Feb. 2018), https://eprints.networks.imdea.org/1744/1/trackers.pdf [https://perma.cc/S8QU-BUPB]; Tex. Google Compl. ¶ 84 ("Google's network reaches more user impressions and websites than any other display network, including over 2 million small online publishers globally. Google has immense scale amongst the long tail of small online publishers."); *see also* Autorité Report, *supra* note 52, at 29–31.

82 CMA Final Report at ¶ 45 (finding that "Google tags and Facebook pixels are widely available on advertiser websites and apps," that "multiple studies have found that Google tags are found on over 80% of the most popular websites, and that Facebook has the second highest prevalence of tags, covering between 40–50% of the most popular websites," and that both "dwarf other platforms' very limited coverage").

83 Engelhardt & Narayanan, *supra* note 33, at ¶ 5.1; *see also* Zuboff, *supra* note 30, at 136 and 137 (collecting other tracking studies with similar findings).

84 CMA Final Report, Appendix G: *The Role of Tracking in Digital Advertising* at ¶ 301.

85 *Id.* at ¶ 302.

86 *See* Zuboff, *supra* note 30, at 137; Ezrachi & Stucke, *supra* note 28, at 179–82 (discussing Goldenshores Technologies' flashlight app).

87 As the French competition authority found from its market sector inquiry:

> . . . many stakeholders do not have proprietary sites where they can directly sell advertising space. Their position is fragile on many levels. They cannot offer advertisers access to inventories that are as extensive as those offered by Google and they remain in an uncertain situation with regard to their ability to collect data on third-party sites and applications in order to offer customised advertising. Internet users are more and more doubtful about the use of their data and they increasingly use technological solutions offered by software publishers and device manufacturers (especially Apple) that limit data collection and ad display, which has an immediate effect on the revenue and profitability of publishers and certain intermediaries whose activities are based on data use.

Press Release, Autorité de la Concurrence, Sector-Specific Investigation into Online Advertising (Mar. 6, 2018), https://www.autoritedelaconcurrence.fr/en/press-release/6-march-2018-sector-specific-investigation-online-advertising [https://perma.cc/MP8Y-RHUT].

88 *See, e.g.*, Tex. Google Compl. ¶¶ 41 & 67–69 ("Google's own documents confirm that it has held a consistent position in the publisher ad server market for display inventory for at least a decade."); GDPR Primer at 30 (noting how "it is difficult for publishers to compete

with advertising networks on the market for online advertising because they control only a fraction of both the advertising space and their audience data").

89 *See* chapter 6 of the ACCC Final Report.

90 House Report at 17–18 ("Google and Facebook have an outsized influence over the distribution and monetization of trustworthy sources of news online, undermining the quality and availability of high-quality sources of journalism") & 63.

91 House Report at 63 (several news publishers noting that "the dominance of Google and Facebook allows them to 'pick winners' online by adjusting visibility and traffic" and how "an update to Google's search algorithm in June 2019 decreased a major news publisher's online traffic 'by close to 50%' even as their referrals from other sources—such as their home page and apps—grew during the same period").

92 ACCC Final Report at 21 (noting how powerful platforms "may increase consumers' risk of exposure to less reliable and lower quality news," as the "news and journalism accessed via digital platforms has been de-coupled from the news media business, often limiting a consumer's familiarity with and knowledge of the original source of the story").

93 House Report at 62 & 181.

94 House Report at 63–64 (journalists describing the relationship between publishers and Facebook as being "sharecroppers on Facebook's massive industrial farm").

95 Hagey & Vranica, *supra* note 21; *How Tech's Triopoly Won the Advertising Game*, Wall St. J. at B8 (Mar. 20, 2021).

96 Hagey & Vranica, *supra* note 21.

97 Srinivasan, *supra* note 9, at 6.

98 Alphabet Inc., Q1 2019 Earnings Call Transcript, Apr. 29, 2019, https://abc.xyz/investor/static/pdf/2019_Q1_Earnings_Transcript.pdf?cache=ebdc584 [https://perma.cc/ZA99-GWZX] (Google CEO noting that by 2019 over 70% of its advertisers were already using automated bid strategies in Google Ads).

99 Tex. Google Compl. ¶¶ 91–92.

100 CMA Final Report at ¶¶ 5.232 & 5.250; Tex. Google Compl. ¶¶ 80, 86, 100 & 104–11 ("Immediately after acquiring a publisher ad server and launching its exchange in 2009, Google made it so the small advertisers bidding through Google Ads had to transact in both Google's ad network and Google's ad exchange. Google also made it so that the large publishers wanting to receive bids from the many advertisers who used Google's ad buying tool had to trade in Google's exchange and license Google's ad server.").

101 Tex. Google Compl. ¶ 149.

102 *Id.*

103 *Id.* at ¶ 59.

104 Keach Hagey & Tripp Mickle, *Google Charges Over Twice Its Rivals in Ad Fees, Suit Shows*, Wall St. J. (Oct. 22, 2021).

105 ThinkWithGoogle, https://www.thinkwithgoogle.com/marketing-strategies/video/18-49-year-old-youtube-behavior/ (last visited Mar. 3, 2021) [https://perma.cc/JKZ2-2RC6].

106 Brooke Auxier et al., *Parenting Children in the Age of Screens*, Pew Res. Center (July 28,

2020), https://www.pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens/ [https://perma.cc/QF9J-DS26].

107 CMA Final Report, Figures 5.9 & 5.10 (5–10% of online display ad revenues generally, and 15 and 20% of the online video display advertising in the United Kingdom).

108 CMA Final Report at ¶ 5.219.

109 CMA Final Report at ¶¶ 63 (finding that Google controls a 50–60% share of DSP services in the United Kingdom) & 5.264:

> Google can leverage the importance of YouTube for advertisers to increase its market power in the DSP market by allowing advertisers to buy YouTube inventory programmatically only through DV360. This restriction affects advertisers' choices of DSP for non-Google inventory as well because . . . a single DSP is typically used for a given campaign. As a result, advertisers who want to include YouTube inventory in their campaigns have a strong incentive to use DV360 for the entire campaign. As we have seen above, access to YouTube is one of the main reasons why advertisers choose DV360; several DSPs submitted that exclusive access to YouTube provides a very significant advantage to DV360 and creates a barrier to the growth of competitors.

110 CMA Final Report at ¶ 5.215 (finding Google to have an 80–90% share in the U.K. ad server market).

111 CMA Final Report at ¶ 2.67.

112 CMA Final Report at ¶ 15 (finding that intermediaries (the largest of which is Google) capture at least 35% of the value of advertising bought from newspapers and other content providers in the U.K. online display advertising market; in other words for every dollar that an advertiser spends for an online display ad, the website that publishes the ad only gets about 65 cents); CMA Interim Report at ¶ 6.178(a).

113 Hagey & Mickle, *supra* note 104; CMA Final Report ¶ 5.242 (finding that in transactions where both Google Ads and Ad Manager (AdX) were used, Google's overall take rate was slightly lower, approximately 30% of the advertisers' spend).

114 House Report at 129.

115 CMA Final Report at ¶¶ 2.70–2.71; Tex. Google Compl. ¶¶ 16, 33 (alleging that the "monopoly tax Google imposes on American businesses—advertisers like clothing brands, restaurants, and realtors—is a tax that is ultimately borne by American consumers through higher prices and lower quality on the goods, services, and information those businesses provide").

116 ACCC Final Report at 119; Furman Report at 116; CMA Final Report at ¶ 8.223 (noting, among other things, how "restricting full independent verification of their own inventory, Facebook and Google have engineered a degree of opacity into the buying and selling of their own advertising inventory"); DMA at 24 (noting how "[t]he conditions under which gatekeepers provide online advertising services to business users including both advertisers and publishers are often non-transparent and opaque" and as a result, "the costs of

online advertising are likely to be higher than they would be in a fairer, more transparent and contestable platform environment"); Tex. Google Compl. ¶¶ 218-223.

117 ACCC Final Report at 14.

118 *Id.*

119 ACCC Final Report at 58, 99, 158, 220, 230; *see also* CMA Final Report at ¶¶ 50 (discussing the platforms' "considerable discretion over a wide variety of parameters that affect the prices advertisers pay") & 5.377 (finding that the "lack of transparency—particularly in relation to ad tech fees, auction rules, and data required for verification and attribution—was leading to worse outcomes for advertisers and publishers"); Tex. Google Compl. ¶¶ 218–223.

120 CMA Final Report at ¶ 66 (finding that "Google's strong position at each level of the intermediation value chain creates clear conflicts of interest, as it has the ability and incentive to exploit its position on both sides of a transaction to favour its own sources of supply and demand") & ¶ 67 (hearing from parties "a wide variety of specific concerns regarding Google's self-preferencing behaviour in intermediation"); Tex. Google Compl. ¶¶ 49 & 335; House Report at 207 ("One key factor that market participants and industry experts cite when accounting for why Google is likely to maintain its dominance in digital ads is its conflict of interest. With a sizable share in the ad exchange market, ad intermediary market, and as a leading supplier of ad space, Google simultaneously acts on behalf of publishers and advertisers, while also trading for itself—a set of conflicting interests that market participants say enable Google to favor itself and create significant information asymmetries from which Google benefits.").

121 Alphabet Inc. 2020 Form 10-K at 29, https://abc.xyz/investor/static/pdf/20210203_alphabet_10K.pdf?cache=b44182d [https://perma.cc/HFZ5-EZ9S]; Facebook, Inc. 2020 Form 10-K at 50, http://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/4dd7fa7f-1a51-4ed9-b9df-7f42cc3321eb.pdf [https://perma.cc/P5MY-YCNP].

122 *GDP by Country*, Worldometer https://www.worldometers.info/gdp/gdp-by-country/ (last visited Mar. 3, 2021) [https://perma.cc/P6CH-AKDV].

123 2020 Facebook 10-K, *supra* note 64, at 52.

124 2020 Alphabet 10-K, *supra* note 64, at 29.

125 Frank Pasquale, *The Dark Market for Personal Data*, N.Y. Times (Oct. 16, 2014), https://www.nytimes.com/2014/10/17/opinion/the-dark-market-for-personal-data.html [https://perma.cc/7C36-TGNF].

126 Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/6X8L-NKJX].

127 Adam Satariano, What a Gambling App Knows about You, N.Y. Times (Mar. 24, 2021), https://www.nytimes.com/2021/03/24/technology/gambling-apps-tracking-sky-bet.html.

128 *Id*.

129 *Id.*

130 Zuboff, *supra* note 30, at 242–43.

131 Ryan Dezember, *Your Smartphone's Location Data Is Worth Big Money to Wall Street*, Wall St. J. (Nov. 2, 2018), https://www.wsj.com/articles/your-smartphones-location-data-is-worth-big-money-to-wall-street-1541131260.

132 Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600; Hamed Aleaziz & Caroline Haskins, *DHS Authorities Are Buying Moment-by-Moment Geolocation Cellphone Data to Track People*, Buzzfeed News (Oct. 30, 2020), https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation [https://perma.cc/B9G4-WZ7D].

133 Erik Brynjolfsson & Andrew McAfee, *The Business of Artificial Intelligence*, *in* Artificial Intelligence: The Insights You Need From Harvard Business Review 10, 23 (Thomas H. Davenport et al. eds. 2019).

134 Ezrachi & Stucke, How Big-Tech Barons Smash Innovation, *supra note* 30.

135 Brent Kendall, *FTC Commissioner: Antitrust Enforcement Isn't Answer to Tech Privacy Concerns*, Wall St. J. (Jan. 30, 2020), https://www.wsj.com/articles/ftc-commissioner-antitrust-enforcement-isnt-answer-to-tech-privacy-concerns-11580419657.

# 5
# Who Owns the Data, and Is That Even the Right Question?

During the 2018 U.S. Senate and House hearings on Facebook after the Cambridge Analytica scandal, the discussion was over who owns the data—Facebook or the user.[1] By one count, Facebook's CEO Mark Zuckerberg said, "You are in control of your data" 45 times during the two congressional hearings.[2] This prompted Zuckerberg's exchange with Senator Jon Tester of Montana:

TESTER: Senator Schatz asked a question earlier about—about data and who owns the data. I want to dig into it a little bit more. You said—and I think multiple times during this hearing—that I own the data on Facebook if it's my data.

ZUCKERBERG: Yes.

TESTER: And—and I'm going to tell you that I think that that sounds really good to me. But in practice—let's think about this for a second. You're making about $40 billion bucks a year on the data. I'm not making any money on it. It feels like you own the data. And in fact, I would say that the—the data that was—that was breached through Cambridge Analytic, which impacted—and correct me if these numbers are wrong—some 80 million Americans.

TESTER: My guess is that few, if any, knew that that information was being breached. If I own that data, I know it's being breached. So could—could you give me some sort of idea on how you can really honestly say it's my data when, quite frankly, they may have goods on me. I don't—I don't want them to have any information on me.

ZUCKERBERG: Senator, when I say . . .

TESTER: Because if I own it, I can stop it.

ZUCKERBERG: Yes. So, Senator, when I say it's your data, what we mean is that you have control over how it's used on Facebook. You clearly need to give Facebook a license to use it within our system.[3]

Why is it hard to believe that Facebook users own the data, as Zuckerberg contended? If users owned their data, they would have known that Cambridge

Analytica used their data to influence the U.S. presidential election in Donald Trump's favor.

So, who owns the data?[4]

We will see that the law in the United States and elsewhere as of 2021 is unclear on our ownership interest in our personal data (if that could be disentangled from other persons' possessory interests). But is this even the right question?

We will examine whether property law is the proper legal framework. There has been a long debate in the United States as to whether to frame privacy in terms of market-based solutions (relying on property, contract, or licensing principles) versus viewing privacy as a fundamental, inalienable right. Both approaches have their respective benefits and shortcomings and share of proponents and critics.[5] While this debate continues, data-opolies have shown how they can game the system, regardless of which approach—property-based or fundamental rights—the jurisdiction relies upon.

We will explore multiple shortcomings of a market-based approach to privacy. Despite its nice ring, the "Own Your Own Data Act"[6] and other proposed legislation that clarifies that we own the data will neither protect us from data-opolies nor prevent toxic competition. The fundamental problems, as the Australian Competition and Consumer Commission summarized, remain: "bargaining power imbalances, information asymmetries between digital platforms and consumers, and inherent difficulties for consumers to accurately assess the current and future costs of providing their user data."[7] Even if we own our data, we will likely face a "take it or leave it" offer when signing up to a platform's terms and conditions and lack control over how our data is used.

## A. The Current Legal Void

If you shopped at the upscale department store Neiman Marcus, you might not have considered who owns the data when paying by credit card for your clothing. But that issue arose in a 2015 U.S. appellate decision, *Remijas v. Neiman Marcus Grp., LLC*.[8] Neiman Marcus had a significant data breach, and the plaintiff customers, whose personal information was hacked, sued for, among many things, negligence and invasion of privacy. To bring these claims, the customers had to show their "standing" under Article III of the U.S. Constitution. They had to establish an "injury in fact," which is "an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not

conjectural or hypothetical."[9] The plaintiffs alleged, among other things, that they had a concrete injury in the loss of their private information, which they characterized as an intangible commodity that they owned. The Court of Appeals for the Seventh Circuit rejected this basis for standing, as the plaintiffs assumed that the law recognizes such a property right: "Plaintiffs refer us to no authority that would support such a finding. We thus refrain from supporting standing on such an abstract injury, particularly since the complaint does not suggest that the plaintiffs could sell their personal information for value."[10] Other courts have reached the same conclusion.[11]

Under the current U.S. regime, the entity that collects the personal data now effectively owns, or at least controls, the data. As data-opolies are now tapping into hospital patient data, the reality, as one industry consultant noted, is "[t]he data belongs to whoever has it."[12]

As a result, the first mover can exploit the current legal void by designing its product or service to ensure that it alone can expropriate the data. Suppose, for example, that you buy a new car with cash. You would probably expect to own the entire vehicle, including any data that it generates. In jurisdictions where the law is unclear on who owns the data, car manufacturers can design their cars to ensure that they primarily collect the data. This data is valuable, as smart connected cars "will also allow manufacturers to remotely monitor a vehicle's health, predict what maintenance work and repair work it needs, and to diagnose its problems."[13] Although some countries and states have addressed this issue, other jurisdictions have not.[14] By restricting the flow of data to itself and authorized car dealerships, car manufacturers can lock us in and hamper our ability to use independent car mechanics.

Now consider buying smart appliances and interconnected devices that work with your new digital personal assistant. You may own the smart vacuum cleaner, but not the personal data it collects, like the dimensions of your home and the furniture you have. Nor can you control the myriad of potential uses of that data—from training algorithms to offering behavioral advertising, like encouraging you to buy a coffee table (absent from your living room).[15] Indeed, the constellation of smart appliances will likely feed the data to the data-opoly. According to one 2020 legal decision, you may not even have a reasonable expectation of privacy over what your digital assistant captures, as courts "have characterized the collection and disclosure of such data as 'routine commercial behavior.' "[16]

To see how much control we actually have over data, the Australian Competition and Consumer Commission (ACCC) conducted in 2018 an interesting experiment. The agency was investigating Facebook's and Google's dominance in the digital platform economy and the extent to which these gatekeepers were collecting data on Australians. So an ACCC staff member downloaded her (for the sake of brevity as the ACCC withheld the person's gender) Facebook data.[17] Not surprisingly, Facebook had stored her "active" user activity information, such as the photos and comments she posted on Facebook.[18] But Facebook also possessed other data that the ACCC employee never knowingly gave Facebook, like the names and phone numbers of her friends and contacts from her smartphone, even though those contacts were not her Facebook friends.[19] Even though the ACCC official turned off location tracking in her Facebook account settings, Facebook nonetheless "had a comprehensive record of IP addresses matched to 53 different locations where the user had logged into their Facebook account."[20] The Facebook data "showed that Facebook had also linked over 500 ad interests to the user's profile and matched the user to contact lists provided by 127 advertisers, including frequent flyer programs and private health insurance companies."[21]

Next, an ACCC staff member downloaded the data attached to her Google family accounts. The results were also chilling.[22] The data "included a recording of every question asked to the family's Google Assistant (by various family members including children)," and location data for several different products and services, including every photo stored.[23] Google somehow collected family photos that the ACCC employee never knowingly shared with Google. How did Google get these personal photos from family members' previous devices when the family members never transferred these photos to their new devices or stored them on the cloud? Google responded that these photos likely came into its possession from a backup sync feature "to save photos to Google Cloud." The ACCC employee subsequently checked to see if her family members turned on this backup feature:

> This was difficult as the family had multiple devices where photos were stored and not all photos on those devices featured in the data available in the Google data download. The staff member then checked the data download for information. It did not outline when consent had been granted and photos uploaded into the cloud or from what device.[24]

Competition officials should not get better privacy protections than the rest of us. But one would expect that the data-opolies would provide them more satisfying answers as to how they acquired the data. If the data-opolies can be non-responsive to the agencies that regulate them, why should we expect any better treatment?

To correct the current market failure, policymakers must first rectify the current legal void, where whoever collects the personal data can use it for whatever purpose. The first fundamental legal issue is control, namely the individuals' right to control what data is collected about them, for what purpose, and by whom. As one review of the economic literature on privacy noted,

> If it is true that information is power, then control over personal information can affect the balance of economic power among parties. Thus, privacy can simultaneously be a source of protection from the economic leverage a data holder could otherwise hold over the data subject (if the merchant figures out how little you know about the product you are browsing, he may steer you towards merchandise or prices that serve his interests better than yours); as well as be a tool the data subject may strategically use against the nonholder (if the salesperson cannot estimate your reservation price, you may be able to exploit this information asymmetry to cut a nice bargain).[25]

Adults in the United States, as of mid-2021, do not have a general legal right to tell firms to stop tracking them, not to use their data for behavioral advertising, or even in many states to have their personal information deleted. Nor, as we shall see, do the privacy laws in Europe sufficiently rein in the data-opolies. When it is not in the market participants' economic interest to provide us with greater protection or control over our personal data, our privacy will suffer. By returning to first principles and clarifying the right to access and expropriate the data, the law can mitigate some of the market power problems posed by data-opolies and the toxic competition engendered by behavioral advertising.[26] So, if we want greater control over our personal information,[27] one proposal is to give us an ownership interest in our data.

## B. Proposals to Give Users an Ownership Interest in Their Data

Americans need a comprehensive federal data privacy law. That was the message to Congress by the Business Roundtable, an association of chief executive officers of America's leading companies. Already by 2019 there was "widespread agreement among companies across all sectors of the economy,

policymakers and consumer groups about the need for a comprehensive federal consumer data privacy law that provides strong, consistent protections for American consumers."[28]

While a consensus exists that individuals should have greater control over their data, the debate is whether to rely on *market-based solutions* (such as property, contract, or licensing principles) or framing privacy as an *inalienable fundamental right*.[29]

For example, one bill before the U.S. Congress called the "Own Your Own Data Act" states that "[e]ach individual owns and has an exclusive property right in the data that individual generates on the internet under section 5 of the Federal Trade Commission Act."[30] While that sounds promising, the bill does not allow individuals to stop data-opolies from tracking them, collecting their data, and using the data for behavioral advertising. The bill only allows individuals to learn what data is being collected about them; to port their data; and to receive an intelligible, easy-to-understand privacy statement. But what happens when you get a privacy statement that is "no longer than 150 words, using a measure of 6 characters to a word" that tells you that your data will be used for behavioral advertising? What if the privacy statement bluntly states that data will be collected about you, but not necessarily to benefit you? Despite "owning" your personal data, you still have little control to stop the data-hoarding, surveillance, and manipulation, as we shall next see.

## C. Shortcomings of a Market-Based Approach to Privacy

Market exchanges work well when both buyers and sellers are fully informed, the terms are transparent, and ample competitive alternatives exist.

Consider all the data collected on you, and then ask whether a property interest would change things. Google, for example, collects personal data about you whenever you –

- use Google's services, including its search engine, YouTube, Google Maps, and Google Shopping;
- use Gmail or receive an email from someone using Gmail;
- use a smartphone with an Android operating system;
- use Google's Chrome browser to surf the web;
- use a Google Nest device, like its smoke alarms, indoor and outdoor cameras, thermostats, and doorbells;
- sign up for a service using your Google account;
- use Google's personal digital assistant, Google Home;
- pay for anything using Google Pay digital wallet; or
- visit any of the two million third-party websites that use Google's analytical technology, including its advertising services.[31]

Even if one fastidiously avoids Google's services, Google, using its tracking and analytical technologies on millions of third-party apps and websites, will still ensnare "90 per cent of users worldwide independent of the browser or operating system they use."[32] Using Google as our example, we can see that any market-based solution for privacy will be ineffective for at least six reasons.

## 1. Informational Asymmetries

Markets work poorly when individuals remain largely unaware of what they are giving up in terms of their attention, autonomy, and data, and for what purpose.[33] As the ACCC noted,

> few consumers are fully informed of, fully understand, or effectively control, the scope of data collected and the bargain they are entering into with digital platforms when they sign up for, or use, their services. There is a substantial disconnect between how consumers think their data should be treated and how it is actually treated. Digital platforms collect vast troves of data on consumers from ever-expanding sources and have significant discretion over how this user data is used and disclosed to other businesses and organisations, both now and in the future. Consumers also relinquish considerable control over how their uploaded content is used by digital platforms. For example, an ACCC review of several large digital platforms' terms of service found that each of the terms of service reviewed required a user to grant the digital platform a broad licence to store, display, or use any uploaded content.[34]

Despite the calls by policymakers for easier-to-read, shorter, and clearer privacy statements, many publishers have the incentive to keep us in the dark when they

need our personal data and attention for behavioral advertising. As a result, even if we own the data, most privacy statements will likely remain lengthy, complex, and ambiguous.[35] As the OECD noted, "by keeping privacy policies deliberately vague, service providers make it difficult for consumers to evaluate the real value of their data. The user is given the immediate benefit of the zero-price service but is unaware of the short or long-term costs of divulging information because they do not know how the data will be used and by whom."[36]

Consequently, even if we own the data, the data-opolies and publishers reliant on behavioral advertising will not change their opaque privacy policies. They will not disclose what data they collect and how exactly they will use our data.[37]

## 2. Difficulties in Assessing Data's Value and Privacy Risks

Even if transparency increased, markets work poorly when it is difficult for sellers to assess the value of what they are giving up. Unlike other markets, such as used cars or baseball cards, we cannot readily assess the value of our personal information,[38] especially when its value is attributable in significant part to how quickly the data can be processed and its contribution to data already collected about us.

For example, what is the "value" when you like something on Facebook? While each Like is seemingly benign, as we saw in Chapter 1, what you Like can reveal many intimate details; as one study found, "even knowing a single random Like for a given user can result in nonnegligible prediction accuracy."[39] Each additional Like can increase Facebook's accuracy in predicting your behavior "but with diminishing returns from each additional piece of information."[40] So, the 1,000th Like may be less valuable to Facebook in predicting whether you are addicted to drugs than the first 300 Likes. Even Facebook cannot easily value the Likes, especially when the point of diminishing returns might vary for predicting different intimate details about you (such as your religious views versus a particular personality trait).

Facebook Likes are only one data source. Now consider, as the ACCC found, Google providing "over 60 different online services that provide Google with over 60 different sources of first-party user data that may be combined and associated with a single user account."[41] In assessing the data's value, we must determine not only the value of our geolocation data from Google Maps at that particular moment but its value in context with all the other data Google collects about us from its other services and third parties, like Mastercard.

So, one cannot assess data's value and privacy risks atomistically. Each geolocation datapoint can be less valuable (and intrusive) than data compiled over 45 days or 45 years. U.S. Supreme Court Justice Sonia Sotomayor noted how retrospective records of public movements can reveal "a wealth of detail" about one's "familial, political, professional, religious, and sexual associations," such as "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[42] Now consider linking the geolocation data to one's searches over the past 45 days, one's postings on Facebook, which apps one used and how, and the websites one visited. It would be like appraising each dot of the pointillist painter Georges Seurat's *A Sunday Afternoon on the Island of La Grande Jatte*, rather than valuing the painting as a whole.

In returning to our example, when visiting the woodworking website, John Doe 123 does not know how much his personal information is worth. Nor can he calculate how much advertisers, such as luxury SUV manufacturers, home mortgage companies, or travel agents, are willing to bid to target him. But even that is incomplete. John Doe 123 must assess the value of the experiment itself (which ads he clicks or views, and which ones he does not), the additional insights when added to the numerous prior behavioral experiments on him (e.g., which ads he more likely clicks when vacationing or before work), and how those insights add to the other information and predictions that the data-opolies have already compiled about him (or his digital doppelgänger).

Even with an ownership interest in our data, we often will not know how much our data is reasonably worth, either in isolation or in context with all the other data already collected about us from first- and third-party sources.[43] The likely result is that we will be bilked.

### 3. Risks and Costs When Data Is Shared with Third Parties

Even if we owned our data, what prevents the data from being traded or shared further.[44] Ordinarily, we are unaffected when someone resells our former car or house. But the sale or sharing of our data with others can raise significant privacy risks. One might accept sharing one's data with a health app. But one might have a greater concern if that sensitive data is shared with Facebook or today's equivalent of Cambridge Analytica, which uses the data to manipulate voter behavior. So markets will not work well when the individual cannot easily

factor to whom else the data may be shared, for what purpose, the risks that the sharing might pose, and the benefit to the entity receiving the information.

## 4. Manipulation of Users' Choices

Markets work poorly when "most users cannot accurately ascertain the risks of exposing their privacy."[45] The data-opolies typically tell us of the benefits of sharing our data but are vague about the potential risks. Data-opolies offer us an immediate, tangible, short-term benefit, such as the use of their social network or search engine, while making it far harder for us to understand the potential long-term risks from the privacy degradation.[46]

As a review of the economic literature noted, "privacy trade-offs are . . . inherently intertemporal," which often mix the tangible with the intangible and nearly incommensurable.[47] With ample data, time, and mental energy, rational users with perfect willpower could perhaps weigh the immediate benefit (such as using Google Maps or Waze to assess current traffic conditions and the best route to the desired locale) against the longer-term risks of Google collecting this information, along with all the other data Google has compiled (or inferred) about us. But one's online activity would be limited to a few minutes per day max. The rest of one's day would be spent plowing through the data and attempting to calculate the risk-reward, which might prove elusive.

However, it gets worse.

Behavioral economics posits that we are not perfectly rational profit-maximizers with willpower. This field of economics was initially intended to nudge us in ways that promote our and societal well-being (such as having us opt out of, rather than opt in to, organ donations and 401(k) retirement participation). But the data-opolies have weaponized behavioral economics to design their framework to encourage behavior that primarily benefits them, not us.[48]

Consider "dark patterns," which "are tricks used in websites and apps that make you do things that you didn't mean to."[49] In its 2018 post-GDPR review, the Norwegian Consumer Council investigated how Facebook and Google deliberately manipulated privacy settings to deter us from protecting our privacy.[50] The data-opolies give us the illusion of control while making it harder for us to actually protect our privacy.[51] As the ACCC likewise found, the digital platforms "tend to understate to consumers the extent of their data collection practices while overstating the level of consumer control over their personal user data."[52] Why? When we have the illusion of control, we paradoxically are

likelier to undertake greater risks in sharing our private information.[53] Even when we think we have control, such as when we use a third-party browser and opt for "do-not-track," we, in reality, do not have control.[54]

To begin with, Facebook and Google, the Norwegian Consumer Council found, both have "default settings preselected to the least privacy friendly options."[55] For example, Facebook preselects keeping facial recognition on. You do not have to do anything except click "Accept and continue."[56] As we saw with Apple and will explore further in Chapter 9, most of us stick with the default (thus explaining why Google spends billions of dollars annually to be the default search engine).

But suppose you are among the few to buck the default and have the time and energy to explore what other options exist. To turn off Facebook's facial recognition technology, you would have to navigate the privacy settings (five clicks in total). Why five clicks instead of one? Again to dissuade you from opting out.

But suppose you are determined to turn off the facial recognition technology. To further discourage you from protecting your privacy, Facebook taps into other behavioral biases, including loss aversion.[57] Under loss aversion, consumers hate giving up options and restricting their choices.[58] Facebook will warn you about a significant potential loss—"if you keep face recognition turned off, we won't be able to use this technology if a stranger uses your photo to impersonate you. If someone uses a screen reader, they won't be told when you're in a photo unless you're tagged."[59] That sounds quite frightening, and you do not know how often this might happen. To dissuade you further, Facebook highlights a few positive uses of its facial recognition technology.[60] But Facebook does not tell you of its creepy uses of this technology, including, as the Norwegian Consumer Council found, "for targeted advertising based on emotional states, or to identify users in situations where they would prefer to remain anonymous."[61] So, Facebook and Google will threaten "users with loss of functionality or deletion of the user account if the user does not choose the privacy intrusive option."[62]

As the Norwegian Consumer Council noted, "[t]he combination of privacy intrusive defaults and the use of dark patterns, nudge users of Facebook and Google, and to a lesser degree Windows 10, toward the least privacy friendly options to a degree that we consider unethical."[63]

Even if we owned our data, the data-opolies would likely exploit our weaknesses to get our data and attention. There is simply too much profit from

behavioral advertising for us to stand in their way. So, they will design privacy *out* of the system and nudge us "to make privacy-intrusive selections by appealing to certain psychological or behavioural biases, using design features such as privacy-intrusive defaults or pre-selections."[64] The data-opolies, after all, are in the prediction and manipulation business; why should we expect any different behavior when it comes to extracting our consent?

## 5. Negative Externalities

The fifth problem with a market-based approach to privacy is the negative externality that individuals may impose on others through their privacy selections. Market-based solutions work well when the property interest is (i) capable of precise definition, (ii) capable of exclusive possession or control, and (iii) the owner can establish a legitimate claim to exclusivity.[65]

A good example is real property, where one can clearly define the parcel of land being transferred. In erecting a fence or stone wall, one can exclude others from one's property. But privacy, unlike real property, is not capable of exclusive possession or control, and individuals with low privacy preferences can adversely affect other people's privacy.[66] Protecting one's data and privacy becomes costlier as others reveal more about themselves.[67]

One example of this "networked privacy" is DNA. Suppose a relative offers her genetic information to a genetics website, like GEDmatch or 23andMe. Her decision can implicate her relatives' privacy rights.[68] How did the police identify Joseph James DeAngelo, a former policeman, as the "Golden State Killer," who committed over 50 rapes and 12 murders across California in the 1970s and 1980s?[69] The police used GEDmatch. This "open-sourced" genealogy website linked a distant relative's DNA to the killer's. As one newspaper reported,

> The case sheds light on a little known fact: Even if we've never spit into a test tube, some of our genetic information may be public—and accessible to law enforcement. That's because whenever one of our relatives—even distant, distant kin—submits their DNA to a public site hoping to find far-flung relations, some of our data is shared as well.[70]

As a 2019 *ABA Journal* article noted, the DNA databases "are so robust that 60% of Americans with European ancestry are identifiable from DNA within these databases," and "that percentage is expected to jump to 90% in just a few years."[71] Consequently, even if you never contributed to a DNA database, your

privacy is implicated if one of your blood relatives did.

Another example is video doorbells and surveillance cameras, such as Amazon's Ring products. Amazon uses crime and safety to tout its surveillance products and emphasizes the partnership with many local police stations: "Connecting residents with public safety agencies through the Neighbors App to create safer, more informed communities."[72] But the community bears the privacy costs of the individual's privacy decisions, as one journalist noted:

> There's a crucial, unstated aspect of owning a Ring camera: You aren't just making the decision to surveil your own property and visitors when you buy one. You make a decision on behalf of everyone around you. If someone walks by your house, lives next door, or delivers packages to your home, they will be recorded and surveilled. They don't get a choice. Buying even one Ring camera is a fundamentally communal decision.[73]

Likewise, in social networks, the choices of others can impinge on your privacy and personal data.[74] If your friend posts a group photo on Facebook without identifying you, Facebook can still identify you with its facial recognition technology.[75] Or, if your friends port their data from Facebook to another platform, to what extent are they also porting your data and reputation?

And the list goes on. Suppose you choose an email provider with greater privacy protection. Your privacy is affected when your friends use less privacy-friendly email providers that scan the content for behavioral advertising and other purposes. The next time you are watching TV at a friend's house, the television might be tracking what you are watching. The TV manufacturer sells your viewing history to third parties, who will use it to see if you visited a retailer after seeing its television ad or to target you later on your phone, tablet, computer, and smartwatch.[76] One issue is who must consent. In a case involving VIZIO, the second-largest manufacturer of smart televisions, the FTC assumed the "consumer," likely the person who purchased the television.[77] But televisions, like digital assistants, will sweep in data from children, other household members, relatives, friends, and others in the house. There is no legal mechanism for the smart device to inform them of their being tracked and requiring their consent.

Indeed, when we trade away information on others, a race to the bottom can ensue. Suppose a navigation app offers to purchase geolocation data to reflect traffic conditions. Suppose we are all stuck in traffic on the George Washington

Bridge. Your data reveals information about the rest of us waiting to get into New York City.[78] If I sell my geolocation data first, I would likely get a better price than the 500th commuter seeking to sell her location data.

We can still opt for privacy, but soon we may end up paying a privacy tax. Suppose more drivers agree to allow auto insurance companies to track their driving in exchange for lower premiums (a practice called telematics). As many more people opt for the privacy-intrusive tracking, the insurer can assume that the remaining holdouts are either poor drivers (who have not participated because their insurance premiums would likely increase) and drivers concerned about their privacy. If the insurer cannot accurately and readily distinguish between the two, and if other insurers cannot make this distinction (without tracking the person's driving), the insurer can raise the holdouts' premiums. The same applies to health, life, and homeowner's insurance. Even if each privacy tax is modest, the taxes, when tallied, might prompt more people to sell their data and privacy sooner rather than later.

So, even if you owned your data, the choices of others can devalue your property right and infringe your privacy. Requiring everyone's permission is problematic, as that increases transaction costs and reduces allocative efficiency.[79]

## 6. Lack of Viable Alternatives

Finally, the most important reason why market-based solutions for privacy will be ineffective in markets with data-opolies is the lack of viable alternatives. Policymakers cannot rely on market-based solutions in markets dominated by a few powerful platforms. Even if we own the data, we individually have little bargaining power and cannot negotiate for better privacy protection. We face a "take-it-or-leave-it" offer, whereby we must consent to the data-opolies' terms for accessing our data, or we simply will not get the service.[80]

In the aftermath of the Cambridge Analytica scandal, for example, Facebook users' trust in the platform plummeted—with only 28% believing that the company is committed to privacy, down from a high of 79% in 2017.[81] Despite the public outrage, #DeleteFacebook campaign, and other scandals, Facebook continued to grow. Between March 2018, when the Cambridge Analytica news broke and March 2020, Facebook "added more than 400 million monthly users—more than the entire population of the U.S."[82]

This is not because Facebook users are agnostic about privacy. Quite the

contrary: 74% of surveyed users in 2018 were very or somewhat concerned about Facebook's invasion of their privacy (a 9-percentage point increase from 2011).[83] Even if Facebook users are displeased with the company's privacy violations, they cannot readily switch to alternative social networks unless they could easily port their data, and all of their friends also switched to the same alternative network.[84]

The same applies to Google, which the FTC sanctioned three times between 2011 and 2020. One egregious violation was when Google "baited children using nursery rhymes, cartoons, and other kid-directed content on curated YouTube channels to feed its massively profitable behavioral advertising business."[85] Nonetheless, Google remains the dominant search engine (with over a 90% share worldwide in January 2021), without losing many users to the more privacy-friendly search engine DuckDuckGo (which had in early 2021 only a 0.64% worldwide share).[86]

Google's continued dominance is not because we are unconcerned about our privacy. On the contrary: 65% of those surveyed in 2018 were very or somewhat concerned about Google's invasion of their privacy, an increase of 13 percentage points from 2011.[87] Again network effects blunt our ability to switch. Unless many of us started supporting an alternative privacy-protective search engine and video platform, Google will continue to benefit from the data-driven network effects.[88]

So even if the "Own Your Own Data Act" or similar legislation gives us a property interest in our personal data, we still could not reject the data-opolies' terms. For if we did, we would not have any viable privacy-friendly alternatives, given the network effects and other entry barriers.[89] Indeed, network effects can at times undercut privacy. As more people join a data-opoly's platform, the more attractive the platform is to potential users, the more willing other users are to join the platform (and surrender their personal data), and the lower the data-opoly's cost in acquiring the data.[90] Thus, the big platforms get bigger, and they have to offer less to attract new users' data. While Facebook and Google collect far more data about us than a decade ago, the value of their services has not increased commensurately. (Indeed, in some ways, it has gotten worse with more ads being targeted at us.[91])

## D. Reflections

Providing us an ownership interest in our data might have some benefits. For

example, it might provide some protection in the United States against government surveillance.[92] It might help plaintiffs in federal courts establish standing to sue for a data breach. But the "Own Your Own Data Act" and similar legislation will fail in markets dominated by data-opolies. In clarifying that we own our data (assuming the law could define our property interest and not someone else's), this market-based solution would neither protect us from data-opolies nor prevent toxic competition. The fundamental problems remain, including the imbalance in bargaining power, the data-opolies' "take it or leave it" offers,[93] and the inherent difficulties for us to accurately assess the current and future costs of providing our data.[94]

So, even if you own the data, as Facebook's CEO repeatedly asserted, you still cannot stop the surveillance, dark patterns, and manipulation.[95] Instead of asking who owns the data, policymakers might consider an alternative approach of viewing privacy and one's right in one's data as a fundamental, inalienable right. That too, as we will see next, has its shortcomings. But it remains the better path forward.

---

1 *Transcript of Mark Zuckerberg's Senate Hearing*, Wash. Post (Apr. 10, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/ [https://perma.cc/T3JK-D47X].

2 Tom Wheeler, *The Root of the Matter: Data and Duty*, Harvard Kennedy School, Shorenstein Center on Media, Politics, and Public Policy (Nov. 2018), 8, https://shorensteincenter.org/wp-content/uploads/2018/11/Root-of-the-Matter-Wheeler.pdf [https://perma.cc/8JYK-TQTU].

3 Transcript of Mark Zuckerberg's Senate Hearing, *supra* note 1.

4 Vasudha Thirani & Arvind Gupta, *The Value of Data*, World Economic Forum (Sept. 22, 2017), https://www.weforum.org/agenda/2017/09/the-value-of-data/ [https://perma.cc/4HET-KSWU].

5 *See, e.g.*, Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 Stan. Tech. L. Rev. 1 (2001); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 Stan. L. Rev. 1373 (2000).

6 S. 806, 116th Cong. (1st Sess. 2019), https://www.congress.gov/bill/116th-congress/senate-bill/806/actions.

7 Australian Competition and Consumer Commission, Digital Platforms Inquiry—Final Report at 374 (2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report [https://perma.cc/M36S-YQJ4] [hereinafter ACCC Final Report]; *see also* Alessandro Acquisti, Curtis Taylor, & Liad Wagman, *The Economics of Privacy*, 54 J. Econ. Lit. 442, 444 (2016), https://dx.doi.org/10.1257/jel.54.2.442 (finding one key theme from the economic

literature on privacy "relates to the observation that consumers are rarely (if ever) completely aware about privacy threats and the consequences of sharing and protecting their personal information," so that "market interactions involving personal data often take place in the absence of individuals' fully informed consent").

8 794 F.3d 688 (7th Cir. 2015).

9 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548, 194 L. Ed. 2d 635 (2016), as revised (May 24, 2016) (internal quotation omitted).

10 *Remijas*, 794 F.3d at 695.

11 *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 968 (7th Cir. 2016) (refusing to recognize a property right to personally identifiable data as a basis for standing to sue in a data breach case); Carpenter v. United States, 138 S. Ct. 2206, 2243, 201 L. Ed. 2d 507 (2018) (Thomas, J., dissenting) ("Although § 222 protects the interests of individuals against wrongful uses or disclosures of personal data, the rationale for these legal protections has not historically been grounded on a perception that people have property rights in personal data as such."); Dinerstein v. Google, LLC, No. 1:19-cv-04311, 2020 WL 5296920, at *11 (N.D. Ill. Sept. 4, 2020) (noting that plaintiffs cited no authority that HIPAA or the MPRA creates a property interest in health data); Key v. BMW of N. Am., LLC, No. 1:19-cv-03366-MMC, 2020 WL 137166, at *3 (N.D. Cal. Jan. 13, 2020) (data extracted from plaintiff's vehicle does not constitute property in which she has an ownership interest since under California law, "information is not property unless some law makes it so"); Divane v. Nw. Univ., No. 16-cv-8157, 2018 WL 2388118, at *12 (N.D. Ill. May 25, 2018) ("It does not appear that courts have recognized a property right in such information."); Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 3:16-cv-00014-GPC-BLM, 2016 WL 6523428, at *6 (S.D. Cal. Nov. 3, 2016) (rejecting plaintiff's standing claim based on an alleged property right claim to his personal identifying information, as plaintiff failed to identify any authority to support this proposition).

12 Melanie Evans, *Hospitals Give Tech Giants Access to Detailed Medical Records*, Wall St. J. (Jan. 20, 2020), https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200.

13 Sarah Kessler, *The Connected Car of the Future Could Kill Off the Local Auto Repair Shop*, Quartz (Sept. 5, 2017), https://qz.com/1054261/the-connected-car-of-the-future-could-kill-off-the-local-auto-repair-shop/ [https://perma.cc/85FP-DWRR].

14 *See, e.g.*, Kirsten Korosec, *Massachusetts Voters Pass a Right-to-Repair Measure, Giving Them Unprecedented Access to Their Car Data*, Tech Crunch (Nov. 4, 2020), https://techcrunch.com/2020/11/04/massachusetts-voters-pass-a-right-to-repair-measure-giving-them-unprecedented-access-to-their-car-data/. Wolfgang Kerber, *Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data*, 9 J. Intell. Prop. Info. Tech. & E-Com. L. 310 (2018), https://www.jipitec.eu/issues/jipitec-9-3-2018/4807/ [https://perma.cc/7TN5-83KW]. Under the Driver Privacy Act of 2015, 49 U.S.C. § 30101(a), any data retained by a motor vehicle's *event data recorder* is the property of the car's owner. But the law applies only to that data from "a device or function in a vehicle that records the vehicle's dynamic

time-series data during the time period just prior to a crash event (e.g., vehicle speed vs. time) or during a crash event (e.g., delta–V vs. time), intended for retrieval after the crash event" and excludes "audio and video data." 49 C.F.R. § 563.5.

15 Maggie Astor, *Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared*, N.Y. Times (July 25, 2017), https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html [https://perma.cc/Q4MA-6SKZ].

16 In re Google Assistant Privacy Litig., 457 F. Supp. 3d 797, 830 (N.D. Cal. 2020) (citations omitted) (finding that plaintiffs have not alleged "sufficient information about the conversations that were allegedly intercepted and recorded to establish that they were had under circumstances that would give rise to a reasonable expectation of privacy," a deficiency fatal to their claims for invasion of privacy and intrusion upon seclusion).

17 ACCC Final Report at 381.

18 *Id.*

19 *Id.*

20 *Id.*

21 *Id.*

22 *Id.*

23 *Id.*

24 *Id.*

25 Acquisti et al., *supra* note 7, at 445.

26 Yan Carrière-Swallow & Vikram Haksar, *The Economics and Implications of Data: An Integrated Perspective*, International Monetary Fund Policy Paper No. 19/16 (Sept. 2019), https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596, at 13 ("The relevant economic question of control over data is then more of access than of ownership. An implication is that, before we can have an efficient and responsible market for data, we need to agree on who controls it—who will have access to it, and who won't—so that its benefits can be derived and shared fairly and traded off in a considered manner that appropriately balances costs, security, and privacy.").

27 UK Competition & Markets Authority, Online Platforms and Digital Advertising Market Study: Market Study Final Report at p. 149 (July 1, 2020), https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digit [https://perma.cc/DA5V-RHA5] [hereinafter CMA Final Report]; Kyle Daly, *Poll Reveals Americans' Data Privacy Frustrations*, Axios (Aug. 13, 2020), https://www.axios.com/exclusive-poll-reveals-americans-data-privacy-frustrations-16514f76-ff5e-4df1-929e-6ba259268023.html [https://perma.cc/3KPQ-QV3J] (2020 survey found that "Americans broadly want more control over what happens with their personal information and think that existing tools seem outdated and should be easier to use").

28 Letter to from Business Roundtable to Sen. Mitch McConnell, Majority Leader, U.S. Senate et al. (Sept. 10, 2019), https://s3.amazonaws.com/brt.org/BRT-CEOLetteronPrivacy-

Finalv2.pdf [https://perma.cc/7V79-KCTY].

29 *See, e.g.*, Marc A. Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 Am. J.L. & Med. 586, 610 n. 115 & 612 (2010) (collecting some of the literature in favor and against treating personal data as the individual's property with rights to prevent others from using it without permission).

30 S. 806, 116th Cong. (2019) (https://www.govinfo.gov/content/pkg/BILLS-116s806is/pdf/BILLS-116s806is.pdf).

31 ACCC Final Report at 7 ("The collection of user data by both major digital platforms (and other digital platforms) also extends far beyond the collection of data provided or observed via a user's interaction with the owned and operated apps and services. Data collected from the user's interaction with vast numbers of other websites and apps is combined with the data from the owned and operated platforms, and, in Google's case, with data collected from a user's device, where the device uses the Android mobile operating system."); Autorité de la concurrence, Press Release, Sector-specific investigation into online advertising (March 6, 2018) ("By collecting data not only from their services but also from third-party sites and applications that use their advertising services, Google and Facebook have unrivalled volumes of data, due to the number of users of their services but also the type of data collected: sociodemographic and behavioural.").

32 ACCC Final Report at 69, 87–88.

33 Acquisti et al., *supra* note 7, at 480 ("when interacting with services that offer trade and protection for their data, consumers face similar hurdles as those that arise when dealing with transparency and consent in the presence of traditional privacy policies—including the hurdle of estimating the fair value of their personal information"); Background Note by the Secretariat, Consumer Data Rights and Competition, OECD Doc. DAF/COMP(2020)1 at ¶ 45 (Apr. 29, 2020), https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf [https://perma.cc/SQ48-WEPD] [hereinafter OECD Consumer Data Rights and Competition] (noting that if "consumers do not understand how their data is being collected and used, then they are less likely to be able to drive effective competition in respect of this").

34 ACCC Final Report at 2–3; *see also* Digital Competition Expert Panel, Unlocking Digital Competition at 22 (2019) (also known as the Furman Report), https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel [https://perma.cc/VK9M-3GV8] [hereinafter Furman Report] (finding that many platforms operating in the attention market "provide valued services in exchange for their users' time and attention, while selling access to this time to companies for targeted advertising," but many consumers "are typically not consciously participating in this exchange, or do not appreciate the value of the attention they are providing") & 23 (noting that many consumers "are not aware of the extent or value of their data which they are providing nor do they usually read terms and conditions for online platforms"); CMA Final Report at ¶¶ 4.61–62.

35 ACCC Final Report at 23; Majority Staff of H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial and Administrative Law, Report and Recommendations: Investigation of Competition in Digital Markets

(2020), https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429 [https://perma.cc/29LN-L4BL] [hereinafter House Report] at 53 ("Because persistent data collection online is often concealed, it is more difficult to compare privacy costs across different products and services. Consumers are largely unaware of firms' data collection practices, which are presented in dense and lengthy disclosures.") (footnotes omitted).

36 Background Note by the Secretariat, Big Data: Bringing Competition Policy to the Digital Era at 25, OECD Doc. DAF/COMP(2016)14 (Apr. 26, 2017), https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf [hereinafter OECD Big Data Report].

37 ACCC Final Report at 374.

38 Acquisti et al., *supra* note 7, at 447.

39 Michal Kosinski, David Stillwell, & Thore Graepel, *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 Proc. Nat'l Acad. Sci. 5802 (2013), https://doi.org/10.1073/pnas.1218772110 [https://perma.cc/2LR4-4782].

40 *Id.*

41 ACCC Final Report at 379.

42 United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) (quoting People v. Weaver, 12 N.Y.3d 433, 441–42 (2009)).

43 Acquisti et al., *supra* note 7, at 447 (noting that "much of consumer data that is of value to advertisers is nonstatic information that is dynamically generated as part of the interaction of the individual with other online services, such as search engines or online social networks").

44 *Id.*

45 Norwegian Consumer Council, Deceived by Design 7 (2018), https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design [https://perma.cc/Z8N6-56D8].

46 *Id.*

47 Acquisti et al., *supra* note 7, at 447; *see also* CMA Final Report at ¶ 4.51.

48 Shoshana Zuboff, The Age of Surveillance Capitalism 295, 343 (2019); Roger McNamee, Zucked: Waking Up to the Facebook Catastrophe 96–97 (2019). A key theme relates to the observation that consumers are rarely (if ever) completely aware about privacy threats and the consequences of sharing and protecting their personal information. Hence, market interactions involving personal data often take place in the absence of individuals' fully informed consent. Furthermore, specific heuristics may profoundly influence consumers' privacy decision making.

49 *What Are Dark Patterns?*, https://darkpatterns.org/ (last visited Mar. 10, 2021) [https://perma.cc/7WDJ-ZPXQ].

50 Norwegian Consumer Council, *supra* note 45.

51 *Id.*; *see also* CMA Final Report at ¶ 37 (identifying many examples "of how platforms' choice architecture and use of defaults inhibits consumers' ability to exercise informed choice and nudges consumers into making choices that are in the best interest of the

platforms") & 3.94–3.128 (discussing evidence that default positions have a significant impact on consumer behavior in search); ACCC Final Report at 374; States Facebook Compl. ¶ 237 ("In what came to be an oft-repeated theme, Facebook made great efforts to present its privacy changes as giving users greater control, even as Facebook made more privacy settings public and thus less protective by default, took away options to limit visibility, and changed its privacy policy to allow for more collection and use of user data."); Complaint ¶ 81, Utah v. Google, 3:21-cv-05227 (N.D. Cal. July 7, 2021) (alleging how Google dissuades Android users from directly downloading apps to their phone with needless obstacles and ominous warnings, including warnings that the installation file from reliable sources "can harm your device").

52 ACCC Final Report at 23.

53 Acquisti et al., *supra* note 7, at 480.

54 Just consider Amazon's privacy notice for Whole Foods:

> Note that your browser settings may allow you to automatically transmit a "Do Not Track" signal to websites and online services you visit. There is no consensus among industry participants as to what "Do Not Track" means in this context. Like many websites and online services, Whole Foods currently does not alter its practices when it receives a "Do Not Track" signal from a visitor's browser.

*Privacy Notice*, Whole Foods Market, https://www.wholefoodsmarket.com/site-information/privacy-notice (Dec. 31, 2019) [https://perma.cc/5SGM-7FLM].

55 Norwegian Consumer Council, *supra* note 45, at 15.

56 *Id*. at 17.

57 In contrast to Bernoulli's theory of expected utility, prospect theory predicts that individuals favor risk aversion for gains, favor risk seeking for losses, and most importantly suffer loss aversion, whereby the dissatisfaction in actually losing money from a reference point (say $100) is greater than the satisfaction in winning that sum of money. Daniel Kahneman, *Maps of Bounded Rationality: Psychology for Behavioral Economics*, 93 Am. Econ. Rev. 1449, 1456–57 (2003).

58 In one computer experiment, participants tried to keep options open even when counterproductive. Dan Ariely, Predictably Irrational: The Hidden Forces That Shape Our Decisions 142–48 (2008). In the Door Game, each MIT student could click on three doors on the computer screen to find the room with the biggest payoff (between 1 and 10 cents). Each student was given 100 clicks, and could click one door as many times possible without a penalty. Each time the student sampled another door, that switch cost the student one additional click. Experiment 2, the Disappearing Door Game, was the same as the Door Game except each time a door was left unvisited for 12 clicks, it disappeared forever. To keep options open, participants in Experiment 2 ended up making substantially less money (about 15% less) than participants in Experiment 1. Participants would have made more money by sticking to one door. *Id.* at 147. A similar result occurred when participants were told the exact monetary outcome they could expect from each room.

59 Norwegian Consumer Council, *supra* note 45, at 22.

60 *Id.* at 22 ("The technology is, according to the popup, used for purposes 'such as help protect you from strangers using your photo' and 'tell people with visual impairments who's in a photo or video.' ").

61 Norwegian Consumer Council, *supra* note 45, at 23.

62 *Id.* at 3.

63 *Id.* at 4.

64 ACCC Final Report at 374; *see also* CMA Final Report at ¶ 4.173 (finding that the platforms' choice architectures rather than remediate biases are more likely to exacerbate biases).

65 *See, e.g.*, Kremen v. Cohen, 337 F.3d 1024 (9th Cir. 2003) (using these three factors to determine whether a property right exists in a domain name).

66 *See, e.g.*, Carrière-Swallow & Haksar, *supra* note 26, at 23 n. 3 (noting how "[s]ome data involves multiple data subjects," so when one person "may divulge that they are friends with another or that they both attended a political gathering," that disclosure may have privacy implications for the second person); NAACP v. Alabama *ex rel*. Patterson, 357 U.S. 449, 462 (1958) (noting how the "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs"). Here we see how privacy can foster the freedom of association, where the privacy interest is not individual anonymity per se but allowing people to meet privately. That privacy interest (along with the constitutional rights protected under the First Amendment) could be chilled if one person disclosed who else belonged to the group or attended the meeting.

67 Acquisti et al., *supra* note 7, at 446; Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 Wash. L. Rev. 555 (2020 .

68 Clare Wilson, *Serial Killer Suspect Identified Using DNA Family Tree Website*, New Scientist (Apr. 27, 2018), https://www.newscientist.com/article/2167554-serial-suspect-identified-using-dna-family-tree-website/ [https://perma.cc/MMA3-A6EK]; Amy Dockser Marcus, *When Your Ancestry Test Entangles Others*, Wall St. J. (Feb. 16, 2020) (noting how the "sheer size of consumer DNA databases—estimated at over 25 million people already—means that even people who choose not to get tested can be identified through DNA uploaded into genealogy databases by relatives").

69 Wilson, *supra* note 68.

70 Matthias Gafni & Lisa M. Krieger, *Here's the "Open-Source" Genealogy DNA Website That Helped Crack the Golden State Killer Case*, Mercury News (San Jose) (Apr. 26, 2018), https://www.mercurynews.com/2018/04/26/ancestry-23andme-deny-assisting-law-enforcement-in-east-area-rapist-case/.

71 Jason Tashea, *Blood Ties: Family-Tree Genealogy Sites Arm Law Enforcement with a New Branch of DNA Sleuthing, but the Battle over Privacy Looms*, ABA J. (Nov. 1, 2019), https://www.abajournal.com/magazine/article/family-tree-genealogy-sites-arm-law-enforcement-with-a-new-branch-of-dna-sleuthing-but-the-battle-over-privacy-looms

[https://perma.cc/N9P2-26NJ].

72 *Neighbors Public Safety Service: Working Together for Safer Communities*, Ring https://shop.ring.com/pages/neighbors-public-safety-service (last visited Mar. 5, 2021) [https://perma.cc/C6M2-UFMP].

73 Caroline Haskins, *How Ring Transmits Fear to American Suburbs—Why Do We Surveil Ourselves?*, Vice (Dec. 6, 2019), https://www.vice.com/en/article/ywaa57/how-ring-transmits-fear-to-american-suburbs [https://perma.cc/F3EH-5WUD].

74 Furman Report at 68 (asking "If a friend in my network is using a newsfeed app with poor privacy standards, what happens if they misuse the information in my post?").

75 Complaint ¶ 241, New York v. Facebook, No. 1:20-cv-03589-JEB (D.D.C. Dec. 9, 2020), https://ag.ny.gov/press-release/2020/attorney-general-james-leads-multistate-lawsuit-seeking-end-facebooks-illegal [https://perma.cc/NLY2-MF6A] [hereinafter States Facebook Compl.].

76 Complaint, FTC v. VIZIO, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf. VIZIO televisions, the FTC alleged, continuously tracked what consumers were watching. Over 10 million VIZIO's televisions transmitted information about what the viewer was watching "on a second-by-second basis." Why the intrusive tracking? VIZIO profited from selling the consumers' television viewing history to third parties. One purpose for the viewing data was to analyze advertising effectiveness. With the data from the TV, third parties could analyze a household's behavior across devices, for example, "(a) whether a consumer has visited a particular website following a television advertisement related to that website, or (b) whether a consumer has viewed a particular television program following exposure to an online advertisement for that program." Another purpose for the viewing data was to better target the household members on their other digital devices.

77 Stipulated Order for Injunction and Monetary Judgment, FTC v. VIZIO, Inc., Case No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.p

78 House Report at 45–46.

79 *See, e.g.*, Broad. Music, Inc. v. Columbia Broad. Sys., Inc., 441 U.S. 1, 21–22 (1979) (discussing how a blanket license helps reduce transaction costs that would be otherwise prohibitive in markets with many sellers and buyers).

80 ACCC Final Report at 23 (finding "considerable imbalance in bargaining power between digital platforms and consumers" and how "[m]any digital platforms use standard-form click-wrap agreements with take-it-or-leave-it terms and bundled consents, which limit the ability of consumers to provide well-informed and freely given consent to digital platforms' collection, use and disclosure of their valuable data") & 374.

81 Herb Weisbaum, *Trust in Facebook Has Dropped by 66 Percent Since the Cambridge Analytica Scandal*, NBC News (Apr. 18, 2018), https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011 [https://perma.cc/UN3W-KY9D].

82 Laura Forman, *Facebook's Politics Aren't Aging Well*, Wall St. J. (June 30, 2020), https://www.wsj.com/articles/facebooks-politics-arent-aging-well-11593446127; States Facebook Compl. ¶ 244.

83 Jeffrey M. Jones, *Facebook Users' Privacy Concerns Up Since 2011*, Gallup (Apr. 11, 2018), https://news.gallup.com/poll/232319/facebook-users-privacy-concerns-2011.aspx [https://perma.cc/XA9Y-YH4E].

84 States Facebook Compl. ¶ 242 (citing study Facebook commissioned that found that dissatisfied users have nowhere else to go and Facebook remains the only choice); House Report at 140 (discussing how Facebook's persistently high market share is not contestable due to high barriers to entry that discourage competition, and that these entry barriers include strong network effects, high switching costs for consumers, and data advantages); Chris Hughes, *It's Time to Break Up Facebook*, N.Y. Times (May 9, 2019), https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html [https://perma.cc/4ABN-LN7M].

85 Dissenting Statement of Commissioner Rohit Chopra, *In re Google LLC and YouTube, LLC*, Commission File No. 1723083 (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtu [https://perma.cc/PNM6-LETP].

86 *Statcounter*, Search Engine Market Share Worldwide—February 2021, https://gs.statcounter.com/search-engine-market-share (last visited Mar. 5, 2021) [https://perma.cc/5GTY-9GTR].

87 Jones, *supra* note 83.

88 Maurice E. Stucke & Ariel Ezrachi, *When Competition Fails to Optimize Quality: A Look at Search Engines*, 18 Yale J.L. & Tech. 70 (2016).

89 CMA Final Report at ¶¶ 3.205 & 3.212.

90 Carrière-Swallow & Haksar, *supra* note 26, at 9 (noting that "where demand-side network externalities are such that participation in the network becomes more attractive to marginal users as the number of users (and the data they generate) grows," which "means that scale increases the marginal user's willingness to surrender their data in exchange for access, thus lowering the platform's barter cost of acquiring more data").

91 CMA Final Report at ¶¶ 5.69, 5.84, 5.85 & 8.153 (discussing the increase in ad load on Google's search engine and Facebook).

92 In Carpenter v. United States, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018), the issue was whether the government conducted a search under the Fourth Amendment of the U.S. Constitution when it accessed historical cell phone records that provided a comprehensive chronicle of the user's past movements. A majority of Justices held yes, and noted that property rights (contra the views of three dissenting Justices) were not the sole measure of Fourth Amendment violations. But Justices Thomas, Alito, and Gorsuch in their dissenting opinions were amendable to a property-based approach. As Justice Gorsuch asked, what kind of legal interest is sufficient to make something yours? Positive law, he noted, may help provide the Court detailed guidance on evolving technologies without resort to judicial

intuition. *See also* United States v. Jones, 565 U.S. 400 (2012) (applying a common law property-based analysis that relied on the fact that police committed a physical trespass in installing the GPS device to vehicle).

93 CMA Final Report at ¶ 13.

94 ACCC Final Report at 374; *see also* Acquisti et al., *supra* note 7, at 444 (finding one key theme from the economic literature on privacy "relates to the observation that consumers are rarely (if ever) completely aware about privacy threats and the consequences of sharing and protecting their personal information. Hence, market interactions involving personal data often take place in the absence of individuals' fully informed consent."); Julie E. Cohen, *Privacy, Ideology, and Technology: A Response to Jeffery Rosen*, 89 Geo. L.J. 2029, 2044 (2001) (noting how the "call for greater informational privacy is, fundamentally, a critique of the political economy of information markets").

95 CMA Final Report at ¶ 13.

# 6
# The Promise and Shortcomings of Treating Privacy as a Fundamental Inalienable Right

Scandals, at times, can bring reform. Consider Watergate during the Nixon administration. As the U.S. Department of Justice observed,

> In 1974, Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies that had been exposed during the Watergate scandal. It was also concerned with potential abuses presented by the government's increasing use of computers to store and retrieve personal data by means of a universal identifier—such as an individual's social security number.[1]

In enacting the Privacy Act of 1974, the U.S. Congress found over forty years ago that "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information."[2] So, Congress declared that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States," and sought to provide individuals greater control over information about them in the federal government records.[3] The United Nations and many jurisdictions now view privacy as a fundamental human right.[4]

In viewing privacy as a fundamental right, policymakers can give individuals greater control over their data and privacy. But deeming privacy as a fundamental right does not automatically provide individuals greater control over their data. Nor does it lead to a uniform approach to deter data-hoarding and curb the toxic competition engendered by behavioral advertising.

To see why, we will consider the California Consumer Privacy Act of 2018 (CCPA) and Europe's General Data Protection Regulation (GDPR). Both statutes have been hailed as privacy highpoints. Both treat privacy as a fundamental, inalienable right;[5] both seek to give individuals greater control over their data.[6] But both statutes failed to deter the data-hoarding and toxic competition. Indeed, data-opolies are more powerful in Europe in 2021 than before the GDPR went

into effect in 2018. But, as we will see, there is hope. Californians in 2020 voted to strengthen their privacy law,[7] and Europe is considering additional privacy measures to curb data-opolies.

## A. Privacy as a Fundamental Right

California's Constitution opens with the proclamation that "[a]*ll* people," not just Californians, have inalienable rights, including "pursuing and obtaining . . . privacy."[8] The European Union Charter of Fundamental Rights protects both the right to respect one's "private and family life, home and communications" and personal data.[9]

In viewing privacy as a fundamental right, both legal regimes seek to provide individuals greater control over their data.[10] Indeed, as the European Data Protection Board observed, "one of the main purposes of the GDPR is to provide data subjects with control over information relating to them."[11] And many Europeans, one year after the GDPR went into effect, felt that they had some control over their data.[12]

But despite sharing these objectives, the jurisdictions took different approaches: California initially took a "hoard-but-regulate" philosophy, while Europe takes a "data minimization" philosophy.

## B. CCPA's "Hoard-but-Regulate" Philosophy

California provided its residents greater control over their data than in most other U.S. states, giving Californians the right to the following:

- know what personal information was being collected about them;
- know whether their personal information was sold or disclosed and to whom;
- say no to the sale of their personal information;
- access their personal information;
- equal service and price, if they exercised their privacy rights; and
- delete some of the data.[13]

The CCPA also required firms to take reasonable steps to safeguard Californians' personal data (such as encrypting the data).[14]

Some data-opolies lobbied against the statute, even though the privacy law

did not hinder their ability to collect and use personal data for behavioral advertising.[15] As we saw, personal data represents a crucial source of the data-opolies' power. In terms of data flow, the central juncture is the initial capture of personal data, or as Shoshana Zuboff describes, the capture of behavioral surplus.[16] So, as Californians spend more time within Google's and Facebook's ecosystems, both data-opolies could continue to collect *first-party* personal data to profile them, target them with behavioral ads, and manipulate their behavior.

The CCPA did give Californians greater control, should the data-opoly sell their personal data to third parties, which happens less frequently. But, as we've seen, Google and Facebook also collect personal data from third parties, such as publishers within their advertising network. Under the CCPA, Californians could prevent these third parties from "selling" personal data to the data-opolies without their permission. But even this was tested. Facebook, for example, claimed that the personal data shared with advertisers and publishers did not count as a "sale" under the California statute, even though as the privacy scholar Chris Hoofnagle noted, the Facebook pixel and the transfer of data with third parties were at the core of the CCPA.[17] This included not only the information Facebook collected from the consumer, either actively or passively but also information observing the consumer's behavior.

One fundamental problem with the CCPA was its focus on the "sale" of data, which is not a significant issue when data-opolies hoard their first-party data and sell predictions and manipulations instead. Data-opolies do not need to sell our data. They sell something far more valuable—predictions on our behavior, whether it is which ads we will more likely click, which apps we will probably use, what shows we will likely watch, what products we will likely buy, or which message will help convince us to vote for one candidate or another. Once companies hoard enough data and attention to become unavoidable trading partners for advertisers and publishers, then they serve as attention brokers, offering "to very precisely target the right audiences and the right states of mind."[18]

Indeed, the CCPA's "hoard-but-regulate" approach to privacy can increase the data-opolies' power. The data-opolies could pressure websites and app developers to pressure their users to share the data with the data-opolies. But even without this consent, the data-opolies will continue to collect a lot of first-party personal data while we are within their vast ecosystem of services and products.

Suppose many individuals tell publishers not to sell or transfer their data to third parties. In that case, the apps and websites cannot pool their data to profile users. Nor can they sell personal data to intermediaries. Each publisher's profile of users will be far less complete than the data-opolies' profiles. They will be unable to assess the ads' impact on behavior (the long tail of attribution). Publishers will be more dependent on Google and Facebook, which will continue to harvest a significant variety of first-party data.

Finally, the punishment mechanisms under the CCPA's "hoard-but-regulate" approach were ineffectual. Californians can only ask companies to delete data collected *from* them, but not data collected *about* them.[19] Even if a few Californians ask Google, Apple, Facebook, and Amazon to delete their data, the data-opolies' algorithms had the opportunity to incorporate that data to better predict those persons' behavior. The data-opoly could continue making inferences about their behavior. And the individuals are still left with few viable competitive alternatives, given the network effects and other entry barriers. The data-opoly resumes collecting their data until the individuals remember to again request that their data be deleted, and actually did so.

### 1. Lessons from the CCPA

Even when privacy is viewed as a fundamental right, the law will not necessarily deter data-hoarding and provide individuals greater control over their data. One response is that the California Consumer Privacy Act was hastily drafted. But more fundamentally, the statute's "hoard-but-regulate" approach imposed few, if any, restraints on the data-opolies' surveillance, collection of personal data, and use of that data to manipulate behavior.

A "hoard-but-regulate" approach might work in markets without data-opolies and where privacy competition is already robust. In these markets, the firms' and our incentives are aligned. Companies will not overreach in collecting more data than necessary. If they do, they stand the risk that we will discover their data-hoarding using the statute's access provision. We can punish these egregious offenders by transferring our personal data to a rival that protects our privacy and deleting the data we provided to the offending company. Thus, the "hoard-but-regulate" approach presupposes robust privacy competition. It will not work in markets where the participants, dependent on behavioral advertising revenues, scramble to find better ways to attract us, collect our data, and manipulate our behavior. It is especially ineffectual when data-opolies orchestrate and intensify

this toxic competition for their benefit.

Consequently, missing from California's original privacy framework were data minimization principles, which we will see next in the GDPR. While data minimization principles can help curb the toxic competition and data-opolies, they too have shortcomings.

## C. The Promise and Failure of the GDPR's Data Minimization Principles

Before the advent of data-opolies and digital platform economy, many countries were concerned about protecting privacy and data protection as fundamental human rights while allowing data to flow across borders to promote economic and social development.[20] In 1980, the OECD member countries developed guidelines to help harmonize their national privacy legislation.[21] To reconcile these fundamental but competing values of promoting privacy and economic and social development (a topic we will explore in Chapter 7), the OECD turned to Fair Information Practices,[22] which served as the framework for many privacy statutes. Two Fair Information Practices seek to limit the collection and use of personal data: the *Collection Limitation Principle* limits the types of information that an organization can collect and how the information is collected. The *Use Limitation Principle* limits how an organization can use the information internally.[23]

These two data minimization principles would appear to sap the data-opolies' power. The Collection Limitation Principle seemingly should give us greater control to prevent data-opolies and the millions of websites and apps from collecting data about us. They could only collect the data with our knowledge and voluntary consent. Even if we consented, the Use Limitation Principle would limit how they use our personal data. We, for example, could limit Google's use of our data to improving its search results, but not for behavioral advertising. These data minimization principles seemingly address their data-hoarding and use of AI to manipulate our behavior. To test this hypothesis, let us examine Europe's General Data Protection Regulation, which incorporates both data minimization principles.

### 1. The Promise of the GDPR

Unlike the California Consumer Privacy Act, companies under the GDPR cannot collect whatever data they want. Europe's privacy law requires firms to

"process[] as little data as possible in order to achieve the [lawful] purpose."[24] When designing their products, services, and applications, companies must incorporate as the default these data minimization principles. Personal data must be:

(a) "processed lawfully, fairly and in a transparent manner in relation to the data subject" (*lawfulness, fairness and transparency*);
(b) "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (*purpose limitation*);
(c) "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (*data minimization*); and
(d) "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" (*storage limitation*).[25]

So, a company must have a specific lawful purpose for collecting personal data. Even when it has a lawful purpose, the company can only collect the minimum amount of personal data that is necessary for that lawful purpose, and not any more. Moreover, the data can be used only for the specific lawful purpose(s) and not for any other purpose. And after the data is no longer required for that purpose, the data must be deleted or anonymized.

Thus, GDPR's data minimization principles depend on whether there is a specific, explicit, and legitimate purpose for collecting and processing that data. The privacy law provides six lawful bases to collect and use personal data:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[26]

For our purposes, the two primary lawful bases for data-opolies to collect and process our data are (i) when we *consent* to the processing of our data "for one or more specific purposes" or (ii) when processing the data is *necessary*. The concepts of *consent*, *choice*, and *necessity* are related. Consent to be valid under the GDPR must be freely given, specific, informed, and unambiguous.[27] Consent is not freely given when the individual has "no genuine or free choice or is unable to refuse or withdraw consent without detriment."[28] Nor is the consent freely given when a company conditions its service on our providing more personal data than what is necessary to perform the contract.[29] The GDPR also allows individuals to withdraw consent easily.[30]

Consequently, on paper, the GDPR's data minimization principles appear well-suited in deterring data-hoarding, sapping the data-opolies' market power, and curbing behavioral advertising. A data-opoly cannot rely on *consent* as a lawful basis to collect personal data. Given the imbalance in bargaining power between the individual and data-opoly, and the absence of viable competitive alternatives, consent cannot be said to be freely given.[31] Nor could a data-opoly justify collecting and using the personal data for behavioral advertising as this purpose is not objectively *necessary* to perform the contract or provide the service. So, Facebook and Google logically would no longer have a lawful basis to collect, hoard, and use personal data for their extensive behavioral advertising apparatus. If the GDPR went into effect in mid-2018, Google and Facebook should no longer collect and process more personal data than what the statute

allows. With the data siphon turned off for behavioral advertising, Google and Facebook, in theory, should no longer enjoy a substantial data (and competitive) advantage over other advertising outlets in Europe; their market power (at least for advertising) should have diminished.

This has not happened. Google and Facebook are as powerful in Europe post-GDPR as they were before 2018. Indeed, the larger platforms' market shares increased under the GDPR, and some believe that the GDPR has led to greater concentration in online advertising in Europe.[32] In late 2020, European policymakers recognized that dominant platforms were still "comprehensively tracking and profiling end users."[33] The U.K. competition agency predicted in 2020 that the likelihood of an entrant displacing either Google or Facebook in the foreseeable future was "low."[34] On both sides of the Atlantic, data-opolies continue to violate individuals' privacy.[35]

## 2. The Failure of the GDPR in Deterring Facebook

The German competition authority's case against Facebook indicts not only the recidivist privacy offender but the GDPR. As in many other countries, Facebook dominates the German social network market, with a 95% share of daily active users.[36] As the Bundeskartellamt stated, the GDPR should have protected Europeans, as its purpose

> is to counter asymmetries of power between organisations and individuals and ensure an appropriate balancing of interests between data controllers and data subjects. In order to protect the fundamental right to informational self-determination, data protection law provides the individual with the right to decide freely and without coercion on the processing of his or her personal data.[37]

Nonetheless, despite the GDPR's intentions, Facebook continued to track users and nonusers even when they were not logged onto the social network. As Chapter 1 notes, whenever someone visits the many websites with a Facebook "like" button or that uses "Facebook Analytics" services, Facebook collects their data to profile that person further. Facebook did not have any legal justification for surveilling millions of Europeans across millions of websites; it violated the GDPR, including its data minimization principles.[38] Even if users were aware of this surveillance, their consent was not freely given, the Bundeskartellamt found, because of the lack of viable competitive options.[39] Nor was the surveillance and data collection objectively necessary for Facebook to provide its social

networking services to users.[40]

Interestingly, the competition authority sought as its remedy what the GDPR failed to do: namely, protect Germans from Facebook's involuntary and secretive surveillance and provide them with greater control over their data.[41] Under the Bundeskartellamt's proposed remedy, Facebook users must consent to the surveillance. If a user declines, Facebook cannot withhold access to its social network. It would have to stop tracking the person across the internet, and it could not merge the user's data from its Facebook, Instagram, and WhatsApp platforms.[42]

Facebook disagreed. Its data collection is not exploitative since the company faces "fierce competition," it complies with the GDPR, and its using personal data across its services "helps to make them better and protect people's safety."[43] Facebook prevailed on appeal before the Düsseldorf Higher Regional Court, which found that the allegations of Facebook's exploitative data processing did not harm Facebook users, Facebook's current or potential competitors, or competition.[44]

The competition authority appealed, and Germany's Federal Supreme Court reversed, ruling in the Bundeskartellamt's favor, but on a different legal basis, namely that Facebook did not give users any choice and options.[45] So, in Germany, "there are neither serious doubts about Facebook's dominant position on the German market for social networks nor about Facebook abusing this dominant position by leaving its users no choice but to accept the processing of their 'off Facebook' data."[46]

Notably, Germany's *competition* authority, not Europe's privacy agencies, challenged Facebook's data collection practices. Facebook, indeed, argued that the EU data protection regulators, not the competition officials, should "determine whether companies are living up to their responsibilities" under the GDPR.[47] This was odd when Ireland's Data Protection Commission at the time was investigating Facebook for multiple privacy violations.[48] The privacy agency was also rumored to bring a significant action against Facebook by 2019.[49] Why would Facebook argue that Ireland's privacy agency should review its behavior, not Germany's competition agency? And why hasn't Ireland's Data Protection Commission weighed in as of 2021? We will explore these issues in the next subpart.

But the Bundeskartellamt's case against Facebook is not a triumph for competition law either. While the antitrust litigation continues, Facebook

continues to amalgamate the personal data it collects across its three platforms. Moreover, even under the proposed remedy, Facebook can freely extract data from users while they are on Facebook and Instagram for behavioral advertising—a purpose which the competition agency assumed was necessary for Facebook to provide its free services. The legal scholar Rupprecht Podszun summarized the unsatisfactory status: "the Bonn-based competition watchdog started its investigations in 2016, we are in our fourth year with this case and a final decision is still a long way off."[50]

No competition case has been brought against Google for its exploitative data collection practices, even though Google tracks us more widely across the internet for behavioral advertising purposes. The European Commission observed the inherent challenges in prosecuting the data-opolies' exploitative data collection practices under competition law.[51]

Neither competition nor privacy law in the United States, European Union, or elsewhere have deterred the data-opolies' privacy violations. Even after European policymakers enacted a comprehensive privacy statute that incorporates data minimization principles, data-opolies could still game the system. Since the CCPA and GDPR have failed to deter the surveillance economy, European policymakers are now exploring new privacy and competition provisions, such as the "Digital Markets Act." But before assessing whether these policies will succeed, we must first understand why the GDPR failed.

## 3. Why the GDPR's Data Minimization Principles Failed to Rein in the Data-opolies

One explanation is a lack of resources for the privacy agencies that enforce the GDPR. As *The New York Times* reported in 2020, Europe's privacy rules "have been a victim of a lack of enforcement, poor funding, limited staff resources and stalling tactics by the tech companies, according to budget and staffing figures and interviews with government officials."[52] For example, Luxembourg's privacy authority, which is responsible for regulating Amazon, "had a budget of roughly €5.7 million" in 2019, which was roughly the equivalent of Amazon's sales over 10 minutes.[53] The resource-constrained Irish Data Protection Commission had, as of June 2020, 2 open inquiries involving Apple, 2 involving Google, and 11 open inquiries involving Facebook, Instagram, and WhatsApp.[54] A lead lawyer's salary at the privacy agency in 2020 was only €60,000-€70,000, a fraction of

what their counterparts defending these data-opolies earn.[55]

But even if Ireland's Data Protection Commission has more resources, can it rein in the data-opolies? Unlikely. Consider my conversation with a senior official from Google. After a conference on the digital economy, the Google official graciously offered to drive me to the San Francisco airport. To find the quickest route, he turned to Google Maps, which prompted the following discussion.

When users share their geolocation data, he noted, Google can quickly report the local traffic conditions and provide the fastest route. Under my privacy-centric world, he observed, this benefit would be lost.

Not necessarily, I replied. Users could opt to share their geolocation data with Google to improve Google Maps, but choose not to have their data used for behavioral advertising.

The Google official disagreed. It has many employees (over 114,000 in 2019[56]). How would Google pay their salaries, fund their research, and provide Google Maps without advertising revenue?

I raise this anecdote to show the differing viewpoints over whether the collection and use of personal data are *necessary* to provide the service.

Under the GDPR, Google must have a lawful basis for collecting and processing the data. Besides users' consent, the other likely legal basis that Google would rely upon is necessity. Google can collect our geolocation data when it "is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."[57] So when we use Google Maps or Waze, our geolocation data is necessary for Google to provide local traffic conditions, in assessing from our car speed which roads are congested and which ones are not. As more users share their location data across many roads, we can better avoid traffic, a classic example of network effects.

But our geolocation data can also help Google improve its other services, like providing more relevant search results. So, while taking a road trip, one can search for "best coffee places nearby" and get relevant responses based on one's current location. Location data can also help in less obvious ways. Microsoft, for example, conducted consumer research that suggested that "Google has an advantage in local restaurant queries 'from Android phone location tracking, allowing it to track popular times and prompt users to submit reviews.' "[58] This can improve other Google services, such as providing users with more recent

reviews of local restaurants.

Finally, our geolocation data can help Google sell location-based advertisements. Google earned an estimated $2.95 billion in revenue in 2019 from just Google Maps.[59] To maximize ad revenues, Google uses our geolocation data "to personalise advertisements for other users; to infer demographic information; to measure the performance of advertisements; to promote, offer to supply or supply advertising services to third parties; and/or to produce anonymized, aggregated statistics (such as store visit conversions statistics) and share those statistics with advertisers."[60] Even when we are using Google's search engine, we will receive ads based on our location whether or not we have chosen to see personalized advertising.[61]

So, is Google's collecting our geolocation data necessary for the provision of its services, and if so, for which purpose? Is our location data required to determine traffic conditions; provide more relevant search results; improve Google's other products and searches (such as restaurant reviews); and improve behavioral advertising, enabling Google to offer many services for "free"? From Google's perspective, the geolocation data is reasonably necessary for all these purposes.

Others would disagree as the privacy interests in our location are significant. The U.S. Supreme Court observed that the geolocation data collected over just four months could provide "an all-encompassing record of the holder's whereabouts" and open

> an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations. These location records hold for many Americans the "privacies of life."[62]

Who then should determine if and when the data collection is necessary for the performance of a contract? Currently, under the GDPR, whoever collects the data, which is Google in our example. And as competition officials have noted,[63] the data-opolies' incentives are not necessarily aligned with our privacy interests.

The irony is that as the data-opolies leverage their power into other segments (such as personal digital assistants, cars, virtual reality, and wearables), they are more likely to find a reason why collecting this personal data is necessary to provide some of their many other services. Recall that Google collects first-party data from over 60 different sources. Google can potentially justify using our geolocation data for multiple purposes, many of which we may not have thought

of as necessary.

One problem then with the GDPR is that the data minimization principles are not self-executing. There are no real checks on the data-opolies' discretion as to whether the collection and use of personal data are necessary. We cannot check whether the data-opolies are abusing their discretion. For one thing, given the opaqueness of the data collection, we do not know what personal data is being collected while being surveilled on- and offline and how exactly the information is being used. The European Data Protection Board (EDPB), which helps ensure that Europe's data protection rules are consistently applied throughout the European Union, warned, "Tracking of user behaviour for the purposes of such advertising is often carried out in ways the user may not be aware of, and it may not be immediately obvious from the nature of the service provided, which makes it almost impossible in practice for the data subject to exercise any control over the use of their data."[64] If we cannot easily detect if and when the collection and use of personal data are unnecessary to perform the contract or provide that service, we cannot control how the data is used.

The data-opolies' privacy policies are of no help. They remain "long, complex, vague, and difficult to navigate."[65] Not surprisingly, few people read them. As the U.K. competition authority found from a 28-day review, "the average visit to the Google privacy page was just 47 seconds, with 85% of visits lasting less than 10 seconds."[66] Why should we spend time reading the privacy policies when we cannot change them?

Even under the GDPR, data-opolies continue to provide their services on take-it-or-leave-it terms and use dark patterns and default settings to nudge us to the privacy-intrusive options.[67] Google, for example, allows users to turn off behavioral advertising (but still collects data about them and uses their location data to serve ads even if the user opted against personalized advertising).[68] Facebook users automatically have their personal data used for behavioral advertising.[69]

Even with sufficient resources, Europe's privacy agencies would have difficulty monitoring and assessing when the company's collection and use of data were necessary to provide particular services. The conclusion does not follow a priori from objective, transparent metrics. Instead, like the rest of us, the privacy agency, absent an extensive investigation, would not know what personal data the firm was collecting and how it was using the data internally.

In returning to our anecdote, suppose a European privacy authority was in our

car en route to the San Francisco airport. Suppose the privacy official agreed with me that under Article 6(1)(b) of the GDPR, Google could collect and process the data for traffic conditions, but not for behavioral advertising as that purpose was not necessary for Google's performance of the contract.

Like the old arcade game, Whack-a-Mole, even if the agency refutes one justification, the data-opoly could offer another lawful basis. So, when the U.K. competition agency asked Facebook about its clickwrap agreements, Facebook pivoted from consent as a justification to other unspecified legal bases under the GDPR. Facebook told the regulator "that, unlike its Terms of Service, as its Data Policy is a privacy notice and relies on a number of legal bases under the GDPR to process consumer data, and as the privacy policy is also not a contract, Facebook is not required to obtain consent from consumers to this policy, either on creation of an account or following any changes to the policy once they had created an account."[70]

Of the GDPR's six different lawful bases for collecting and processing personal data, in the context of commercial purposes, the three most common bases are *consent* under Article 6(1)(a), *contract* under Article 6(1)(b), and *legitimate interests of the data controller* under Article 6(1)(f).[71] Suppose the privacy official in our car trip goes further and states that in the context of behavioral advertising, consent is the only valid legal basis under the GDPR. That is the general view of EU privacy officials.[72] That is seemingly good news for enforcers, as six potential justifications under the GDPR are narrowed to one, namely, whether we consented to the processing of our data for one or more specific purposes.

The problem is that we typically do consent. As we saw in Chapter 5, that consent can be manipulated through the use of default settings and dark patterns. The data-opoly's "privacy check-up" gives us the illusion of control while making it harder for us to protect our privacy.

To prove that consent was not freely given, the privacy agency would have to show that the user "has no genuine or free choice or is unable to refuse or withdraw consent without detriment."[73] This, in turn, would require the privacy agency to prove a significant imbalance in negotiating power between the platform and individual. This inquiry can take competition agencies that specialize in these determinations years to undertake.[74] One complaint about antitrust enforcement is that it "can often be slow, cumbersome, and unpredictable."[75] It is unlikely that privacy officials could ascertain the

platform's dominance any quicker. As the OECD noted, "the fact that so few consumers engage with and understand privacy notices, whether from a dominant business or otherwise, is a key challenge for any case trying to prove that a dominant business' data collection practices are excessive."[76]

Finally, even if the privacy agency determines that the data-opoly had no legal basis for collecting and using our data, its fines and other remedies will unlikely deter the data-opolies and the toxic competition. As Europe's top antitrust enforcer observed, privacy enforcement:

> no matter how robust, may not capture all the complexities that the accumulation of "big data" sets by digital platforms can give rise to in markets for digital services. It is precisely the ability of large digital platforms to accumulate and exploit these big data sets about consumer behaviours and transactions which may lead to competition problems.[77]

## D. California Strikes Back

Besides voting for the next U.S. president, Californians in 2020 elected whether to transform their state's privacy law. In voting yes for Proposition 24, they would enact the California Privacy Rights Act of 2020,[78] driven by Alastair Mactaggart, who also spearheaded the CCPA two years earlier. The amendments would strengthen privacy, he and other proponents argued, by adding the following benefits:

> Purpose limitation: only use info for stated purpose.
> Storage limitation: only keep info as long as business has said it will.
> Data Minimization: don't collect more info than necessary.
> Sensitive Personal Info: right to stop its use (includes: race, precise geolocation, religion, union membership, genetics, biometrics, sexual orientation, contents of communications).
> Right to see "all" personal info, not just last 12 months'.
> Precise geolocation—no tracking within ~250 acres.
> Profiling—right to object to automated decision-making, and to learn meaningful information about the logic involved.
> Right to opt out of cross-context behavioral advertising fixes major CCPA weakness.
> Data protection agency with guaranteed funding.[79]

Opponents of Proposition 24 argued that the new law would diminish privacy in

allowing " 'pay for privacy' schemes, mak[ing] workers wait years to learn what confidential information employers collect on them, and mak[ing] it harder to stop tech giants from selling [their] information."[80]

So how did Californians vote on the 53-page bill? Fifty-six percent voted in favor.[81] Much will depend on the regulations to effectuate the California Privacy Rights Act of 2020, how the statute will be interpreted, and its enforcement. But on paper, California's new privacy law seeks to correct many shortcomings of the 2018 law's "hoard-but-regulate" approach.

Unlike the CCPA, but like the GDPR, the new privacy law incorporates data minimization principles to give users greater control.[82] Californians can still opt out of their personal data being sold to (and, under the 2020 statute, "shared" with) third parties.[83] But the law also gives Californians the right to limit the use and disclosure of their "sensitive personal information."[84] Californians can, at any time, direct a business that collects their sensitive personal information "to limit its use . . . to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services."[85] This language suffers the same infirmities as the GDPR in leaving its execution to the data-opoly's discretion. But it appears that the 2020 law allows Californians to opt out of having their sensitive personal data used for behavioral advertising.[86] We shall examine the benefits and shortcomings of the CPRA and other remedies considered by policymakers in Chapter 9. But California's 2020 law represents another step in the right direction.

The definition excludes sensitive personal information that is "publicly available," as defined under the statute. Moreover, the State Attorney General can update and add new categories of personal and sensitive personal information through regulations. CPRA § 1798.185(a)(1).

## E. Reflections

As we saw, easy labels do not supply ready answers. Giving us an ownership interest in our data will not work. Nor does declaring privacy a fundamental right. While the GDPR's data minimization principles appear promising, the concepts of *necessity* and *consent* are not self-executing constraints on the data-opolies' discretion. One can tell data-opolies to collect and use only that personal data necessary to provide the service. Enforcing it is a lot harder. As long as the discretion remains with the powerful platforms, whose dominance and profits depend on surveillance and hoarding of personal data, they will game the system.

Rather than leave the interpretation and execution of the data minimization principles primarily to the data-opolies, policymakers instead are seeking to effectuate these principles through default provisions (such as enabling individuals to opt into (or out of) behavioral advertising). That is good news. But is it still good news if these policies minimize the collection and use of data to a trickle? To answer that question, we must consider the interplay between competition and privacy, and our third overarching question, *What are the policy implications if data is non-rivalrous*?

---

1 United States Department of Justice, Overview of the Privacy Act of 1974: Policy Objectives (Feb. 24, 2021), https://www.justice.gov/opcl/policy-objectives [https://perma.cc/QCF9-QNML].

2 Privacy Act of 1974, Pub. L. No. 93–579, § 2(a), 88 Stat. 1896, 1896.

3 *Id.* Despite this congressional statement, the U.S. Supreme Court has steadfastly avoided finding any constitutionally protected right to informational privacy. Instead, the Court assumed, without deciding, that the Constitution protects an informational privacy right, and held that the government's actions would not violate such a right (if it existed). *See, e.g.*, Nat'l Aeronautics & Space Admin. v. Nelson, 562 U.S. 134, 138 (2011); Whalen v. Roe, 429 U.S. 589, 603 (1977). Justice Scalia, in his concurring opinion, which Justice Thomas joined, disclaimed any constitutionally protected right to informational privacy. *Nelson*, 562 U.S. at 161.

4 *See, e.g.*, Article 12 of the 1948 Universal Declaration of Human Rights, https://www.un.org/en/universal-declaration-human-rights/ ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."); Oliver Diggelmann & Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, 14 Hum. Rts. L. Rev. 441 (2014), https://doi.org/10.1093/hrlr/ngu014; *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*, Global Internet Liberty Campaign http://gilc.org/privacy/survey/intro.html (last visited Mar. 8, 2021) [https://perma.cc/3Z3Y-SHXL].

5 *See* California Consumer Privacy Act of 2018, ch. 55 § 2(h), 2018 Cal. Stat. 1807, 1809 [hereinafter CCPA]; European Data Prot. Bd., *Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects* ¶ 51 (Apr. 9, 2018), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf [https://perma.cc/D9VZ-JW7P] [hereinafter EDPB Guidelines].

6 Sec. 2(h) of the CCPA (legislature noting that "[p]eople desire privacy and more control

over their information" and how "California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information").

7 California Privacy Rights Act of 2020, https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf [hereinafter CPRA]; Stacey Gray et al., *California's Prop 24, the "California Privacy Rights Act," Passed. What's Next?*, Future of Privacy Forum (Dec. 17, 2020), https://fpf.org/blog/californias-prop-24-the-california-privacy-rights-act-passed-whats-next/ [https://perma.cc/V365-FWPG].

8 Cal. Const. art. I, § 1.

9 Charter of Fundamental Rights of the European Union: 2010 (O.J.) (C83) 389, art. 7 (respect for private and family life) & 8 (protection of personal data), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN.

10 Sec. 2(a) of the CCPA (noting that fundamental to this right of privacy "is the ability of individuals to control the use, including the sale, of their personal information"); *see also* Iris van Ooijen & Helena U. Vrabec, *Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective*, 42 J. Consum. Pol'y 91 (2019), https://doi.org/10.1007/s10603-018-9399-7.

11 EDPB Guidelines ¶ 51.

12 Eur. Comm'n, Special Eurobarometer 487a, Summary: The General Data Protection Regulation (Mar. 2019), https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/Docume [https://perma.cc/86QG-XLCS] (finding that 65% of respondents surveyed who provided personal information online felt they have at least some control over this information: 14% felt they had complete control and 51% felt they had partial control).

13 Sec. 2(i) of the CCPA.

14 Sec. 1798.150(a)(1) of the CCPA.

15 Kartikay Mehrotra et al., *Google and Other Tech Firms Seek to Weaken Landmark California Data-Privacy Law*, LA Times (Sept. 4, 2019), https://www.latimes.com/business/story/2019-09-04/google-and-other-tech-companies-attempt-to-water-down-privacy-law.

16 Shoshana Zuboff, The Age of Surveillance Capitalism 74–97, 338–40 (2019).

17 Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, Wall St. J. (Dec. 12, 2019), https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345.

18 Tim Wu, *Blind Spot: The Attention Economy and the Law*, 82 Antitrust L.J. 771, 789 (2019).

19 CCPA § 1798.105(a) (providing consumers "the right to request that a business delete any personal information about the consumer which the business has collected from the consumer").

20 OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980),

http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborde

21 *Id.*

22 For a good summary of the history, benefits and shortcomings of the Fair Information Practices, *see* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 Md. L. Rev. 952 (2017).

23 OECD Privacy Principles, Annex to the Recommendation of the Council of 23rd September 1980: Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, http://oecdprivacy.org/#principles (last visited Mar 8, 2021) [https://perma.cc/BHE5-HPGN].

24 EDPB Guidelines ¶ 15; Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC [hereinafter GDPR] art. 5, https://gdpr-info.eu/.

25 GDPR art. 5; *see also* GDPR art. 25(2) ("The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.").

26 GDPR art. 6(1).

27 GDPR art. 7(4).

28 GDPR Recital 42.

29 GDPR art. 7(4) ("When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.").

30 GDPR art. 7(3).

31 EDPB Guidelines ¶ 51 (noting that "personal data cannot be considered as a tradeable commodity. Data subjects can agree to processing of their data, but cannot trade away their fundamental rights.").

32 Background Note by the Secretariat, Consumer Data Rights and Competition, OECD Doc. DAF/COMP(2020)1 (Apr. 29, 2020) ¶ 168, https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf [https://perma.cc/SQ48-WEPD] [hereinafter OECD Consumer Data Rights and Competition]; Zuboff, *supra* note 16, at 485–87.

33 European Commission, Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), at 1 (Dec. 15, 2020), https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf [https://perma.cc/G87S-Q88U] [hereinafter Digital Markets Act].

34 UK Competition & Markets Authority, Online Platforms and Digital Advertising Market Study: Market Study Final Report (July 1, 2020) ¶ 6.6, https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digit [https://perma.cc/DA5V-RHA5] [hereinafter CMA Final Report].

35 *See, e.g.*, Digital Competition Expert Panel, Unlocking Digital Competition at 43 (2019) (also known as the Furman Report), https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel [https://perma.cc/VK9M-3GV8] [hereinafter Furman Report] ("The German competition authority's recent decision to impose restrictions on Facebook's collection and combination of user data without explicit consent is evidence that privacy issues remain with GDPR in place.").

36 Bundeskartellamt, Case Summary: Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing (Feb. 15, 2019), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufs 22-16.pdf?__blob=publicationFile&v=4 [https://perma.cc/Y69N-ZGPG] [hereinafter Bundeskartellamt Facebook].

37 *Id.*

38 Bundeskartellamt, Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources: Background Information on the Bundeskartellamt's Facebook Proceeding (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02 __blob=publicationFile&v=6.

39 Bundeskartellamt Facebook at 10 (finding that given "Facebook's dominant position in the market, users consent to Facebook's terms and conditions for the sole purpose of concluding the contract . . . cannot be assessed as their free consent within the meaning of the GDPR").

40 Bundeskartellamt Facebook at 10 ("Processing data from third-party sources to the extent determined by Facebook in its terms and conditions is neither required for offering the social network as such nor for monetising the network through personalised advertising, as a personalised network could also be based to a large extent on the user data processed in the context of operating the social network.").

41 Note by Germany, Consumer Data Rights & Competition, OECD Doc. DAF/COMP/WD(2020)32 (June 12, 2020) at ¶ 20, https://one.oecd.org/document/DAF/COMP/WD(2020)32/en/pdf ("The Bundeskartellamt found that using and actually implementing Facebook's data policy, which allows Facebook to collect user and device-related data from sources outside of Facebook's social network and to merge it with data collected on the Facebook network, constitutes an abuse of a dominant position on the social network market in the form of exploitative business terms pursuant to Section 19(1) German Competition Act (Gesetz gegen Wettbewerbsbeschränkungen, GWB). Taking into account the assessments under data protection law pursuant to the GDPR, the Bundeskartellamt came to the conclusion that Facebook's business terms are inappropriate terms to the detriment of both private users and competitors.").

42 Bundeskartellamt, Press Release, Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources, Feb. 7, 2019, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02 __blob=publicationFile&v=2 [https://perma.cc/6Y7C-TE4F] (head of the German competition agency stating "Voluntary consent means that the use of Facebook's services

must not be subject to the users' consent to their data being collected and combined in this way. If users do not consent, Facebook may not exclude them from its services and must refrain from collecting and merging data from different sources").

43 Yvonne Cunnane & Nikhil Shanbhag, *Why We Disagree with the Bundeskartellamt*, Facebook (Feb. 7, 2019), https://about.fb.com/news/2019/02/bundeskartellamt-order/ [https://perma.cc/QGR8-DXAT].

44 Oberlandesgericht Düsseldorf [Higher Regional Court of Düsseldorf] Aug. 26, 2019, VI-Kart 1/19 (V), https://www.justiz.nrw.de/nrwe/olgs/duesseldorf/j2019/Kart_1_19_V_Beschluss_20190826.h [https://perma.cc/ZK4N-N62R], *translated in* https://www.d-kart.de/wp-content/uploads/2019/08/OLG-Düsseldorf-Facebook-2019-English.pdf [https://perma.cc/SZ2W-FFLW].

45 Rupprecht Podszun, *Facebook @ BGH*, D'Kart Antitrust Blog (June 23, 2020), https://www.d-kart.de/en/blog/2020/06/23/facebook-bgh/ [https://perma.cc/G2KD-UY22].

46 Bundeskartellamt 2019 Annual Report at 37, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Jahresbericht/Jahresbericht_20 __blob=publicationFile&v=3 [https://perma.cc/EP22-JBDN].

47 Cunnane & Shanbhag, *supra* note 43.

48 *See, e.g.*, Press Release, Data Protection Commission, Data Protection Commission Opens Statutory Inquiry into Facebook (Apr. 25, 2019), https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-facebook-0 [https://perma.cc/C4TB-ZRYQ] (investigating whether Facebook was storing "hundreds of millions of user passwords, relating to users of Facebook, Facebook Lite and Instagram, . . . in plain text format in its internal servers").

49 Sam Schechner, *EU Nears Decisions in Facebook Privacy Cases*, Wall St. J. (Aug. 13, 2019), https://www.wsj.com/articles/eu-nears-decisions-in-facebook-privacy-cases-11565602202.

50 Podszun, *supra* note 45.

51 Note by the European Union, Consumer Data Rights & Competition, OECD Doc. DAF/COMP/WD(2020)40 (June 12, 2020) at ¶ 41, https://one.oecd.org/document/DAF/COMP/WD(2020)40/en/pdf [https://perma.cc/Y66C-2UEV] (noting that "[r]egardless of the final outcome of the German Facebook case, it is apparent that exploitative theories of harm are challenging in relation to defining what constitutes an excessive or unfair level of data collection or use from a consumer's point of view, as well as in establishing the necessary link between such data practices and abusive conduct in the sense of competition enforcement").

52 Adam Satariano, *Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates*, N.Y. Times (Apr. 28, 2020), https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html [https://perma.cc/MAR6-AXTX.

53 *Id.*

54 Data Protection Commission (Ireland), *DPC Ireland 2018–2020: Regulatory Activity*

*Under GDPR* (June 2020), https://www.dataprotection.ie/sites/default/files/uploads/2020-06/DPC%20Ireland%202018-2020%20Regulatory%20Activity%20Under.pdf [https://perma.cc/37DK-VU3A].

55 Karlin Lillington, *Data Protection Offices Need Proper Resources Now More Than Ever*, Irish Times (Dublin) (Apr. 30, 2020), https://www.irishtimes.com/business/technology/data-protection-offices-need-proper-resources-now-more-than-ever-1.4241106 [https://perma.cc/YR57-MQVN].

56 Rob Copeland, *Google Parent's Ad Sales Rise, But So Do Costs*, Wall St. J. (Oct. 28, 2019), https://www.wsj.com/articles/google-parent-alphabets-ad-sales-hit-record-but-costs-pile-up-11572295328.

57 GDPR art. 6(1)(b).

58 CMA Final Report at ¶ 3.90.

59 Majority Staff of H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial and Administrative Law, Report and Recommendations: Investigation of Competition in Digital Markets 108 (2020), https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429 [https://perma.cc/29LN-L4BL].

60 Press Release, Australian Competition and Consumer Commission, Google Allegedly Misled Consumers on Collection and Use of Location Data (Oct. 29, 2019), https://www.accc.gov.au/media-release/google-allegedly-misled-consumers-on-collection-and-use-of-location-data [https://perma.cc/585R-VK2N].

61 CMA Final Report at ¶ 4.127.

62 Carpenter v. United States, 138 S. Ct. 2206, 2217, 201 L. Ed. 2d 507 (2018) (internal citations omitted).

63 *See, e.g.*, ACCC Final Report at 7 ("Policymakers should consider the extent to which important decisions about the dissemination of information, the collection of personal data and business' interaction with consumers online, should be left to the discretion of certain large digital platforms, given their substantial market power, pervasiveness and inherent profit motive (including their need for very strong profit growth).").

64 EDPB Guidelines ¶ 4.

65 ACCC Final Report at 401.

66 CMA Final Report at ¶ 39.

67 EDPD Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0 (Adopted on Oct. 20, 2020), at 19, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_ (noting that dark patterns are contrary to the spirit of the GDPR's Article 25).

68 CMA Final Report at ¶¶ 4.127–28.

69 CMA Final Report at ¶ 4.130.

70 CMA Final Report at ¶ 4.157 n. 308.

71 OECD Note by the EU, *supra* note 51, at ¶ 17.

72 *Id.* at ¶ 18.

73 GDPR Art. 6, Recital 42 (Burden of Proof and Requirements for Consent),

https://gdpr-info.eu/recitals/no-42/.

74 CMA Final Report at ¶ 7.33 (noting how antitrust cases "typically take over a year, and sometimes several years, to reach a decision," such as the European Commission's Android case, which took more than five years to bring; Shopping case, which took more than seven years; and AdSense which took nine years, and which does not include the appeal processes, which all three cases as of October 2021 are still being reviewed).

75 Furman Report at 6; *see also* European Commission, Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), at 15 (Dec. 15, 2020), https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf [https://perma.cc/G87S-Q88U] (noting how antitrust "enforcement occurs ex post and requires an extensive investigation of often very complex facts on a case by case basis").

76 OECD Consumer Data Rights and Competition, *supra* note 32, at ¶ 105.

77 *Hearing on Online Platforms and Market Power Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. (July 30, 2020) (Statement of Margrethe Vestager Executive Vice-President, European Commission at 2), http://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-20200729-SD007.pdf.

78 California Proposition 24, *Consumer Personal Information Law and Agency Initiative (2020)*, BallotPedia (last visited Mar. 8, 2021), https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_an [https://perma.cc/4BG4-HVRW].

79 Yes on Prop 24, *How Prop 24 Adds More Privacy Rights Compared to the CCPA*, YouTube (Sept. 23, 2020), https://www.youtube.com/watch?v=UTAa3EtQwhg [https://perma.cc/5KLA-N53Q].

80 Proposition 24: *Amends Consumer Privacy Law*, CaliforniaChoices.org (last visited Mar. 8, 2019), https://www.californiachoices.org/proposition-24 [https://perma.cc/F9J3-H86R].

81 Consumer Personal Information Law and Agency Initiative (2020), *supra* note 78.

82 *See* CPRA §§ 1798.100(a)(2), (a)(3), & (c).

83 CPRA § 1798.120.

84 Section 1798.140(ae) of the CPRA defines "sensitive personal information" as

(l) personal information that reveals
  (A) a consumer's social security, driver's license, state identification card, or passport number;
  (B) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
  (C) a consumer's precise geolocation;
  (D) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
  (E) the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication;
  (F) a consumer's genetic data; and

(2) (A) the processing of biometric information for the purpose of uniquely identifying a consumer; (B) personal information collected and analyzed concerning a consumer's health; or (C) personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

85 CPRA § 1798.121(a).

86 As we'll see in Chapter 9, there is ambiguity whether the opt-out precludes behavioral advertising.

# 7
# What Are the Policy Implications if Data Is Non-rivalrous?

Let us consider the looming, and largely unexplored, clash between privacy and competition. Suppose a country's privacy law successfully implements these "data minimization" policies. The privacy law effectively limits the flow of personal data in the first instance (from the consumer to the initial collector) to a trickle.

Suppose the country's competition policies, on the other hand, seek to "democratize" personal data—by circulating and redistributing the data (with sufficient privacy safeguards) to maximize its overall value. To improve data analytics from training the algorithms with new sources of data, glean more insights from machine learning, foster data-driven innovations, and promote competition, we often need a lot of personal data. So the country's competition policies focus on "data openness" by increasing data portability, improving interoperability, and requiring data-opolies to share some of the personal data with rivals.

As we will see, push too hard on the privacy lever, then the amount of data collected is reduced. With less data to democratize, competition, innovation, and data philanthropy can suffer. But push too hard on the competition lever, policymakers can ultimately promote a surveillance economy where we are the commodity. With each lever being pulled in opposite directions, something has to give. That can be both privacy and competition.

## A. How Personal Data Is Like TV Shows and Air, and Unlike Candy Bars

When economists say goods and services are non-rivalrous, what they mean is that many people can use (or enjoy) them without significantly reducing the goods' and services' value. So, we can both enjoy watching the same television show without reducing its value for someone else. Likewise, economists say personal data, at times, is non-rivalrous—many people can use the data to glean insights without reducing the data's value for others.[1] Consider how many people at this moment are using the United States' publicly available datasets at data.gov. The data's value does not diminish when thousands of researchers are

simultaneously mining the 192,180 datasets for insights.

In contrast, only one person can consume a *rivalrous* good. If you eat your child's last Halloween candy bar, then others cannot eat it.

Now consider all the personal data that wearables, like Apple Watch and Fitbit, collect, including "the number of steps you take, your distance traveled, calories burned, weight, heart rate, sleep stages, active minutes, and location."[2] That data benefits not only Apple and Fitbit and those using the wearables. That health data, some scientists say, can revolutionize biomedical research.[3] Google points to these potential benefits for acquiring Fitbit, as the data can help its algorithms learn to "detect lung cancer, eye disease and kidney injuries."[4]

The myriad potential benefits from personal data include personalized medicine and "helping cure rare or chronic diseases."[5] Geolocation data from our smartphones, besides assessing traffic conditions, can help health officials determine the extent to which residents are self-quarantining during the coronavirus pandemic.[6] Data from smart thermometers can help health officials track the spread of the coronavirus.[7] The COVID-19 pandemic has reinforced the importance of sharing data, which President Joe Biden promoted in his initial executive orders.[8]

Beyond healthcare, imagine how different academic departments of a research university could glean insights from the personal data that Facebook collects.[9] We can share our insights and underlying datasets with other researchers, nonprofit organizations, think tanks, and government agencies. Thus, Europe's proposed Data Governance Act seeks "to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU," including sharing data on altruistic grounds.[10]

While many businesses, nonprofits, and governments can benefit from mining personal data, two significant barriers are the time and cost of collecting and preparing the data.[11] But once the data is collected, cleaned, organized, and formatted, the data can be shared with multiple groups, who can derive value from it. You might have shared an Excel spreadsheet with colleagues that saved them much time, effort, and money. Without it, they might not have invested the effort to collect the data for their project; nonetheless, your spreadsheet, in lowering these initial costs, helped them uncover additional insights for their research. So, the incremental value need not be great for each use, but as your spreadsheet circulates within the research community, the value adds up.

As a result, when personal data are non-rivalrous, some economists posit that

the welfare-optimal solution is to price the data at zero so that it could be used as much as possible to maximize its potential value.[12] As long the potential benefit exceeds the cost in transferring the data and organizing the datasets for the new intended use, it seemingly makes sense to make the data available. Indeed, before COVID-19, we saw the emergence of "data philanthropy," where nonprofits unlock the power of private data for the public good. Firms would turn over personal data, with some safeguards, to a public-serving analyst. The university or nonprofit research organization would use the data "to yield new insights; improve public policies, programs, and services; or otherwise serve the public good."[13] Facebook, for example, has offered to make data available to social science researchers, who could mine the data for additional insights in their respective fields.[14]

Everyone seemingly benefits. The potential for data-driven innovation increases as well, as two IMF officials note:

> Data analysis can also be used in innovation, as new insights extracted from data can lead to the development of new products or services. More recently, the proliferation of big data and the development of machine learning algorithms have enabled data analysis to address increasingly complex problems. Data has thus come to represent a necessary input into the development and production of a wide range of new products. For instance, cars equipped with sensors may record the actions of drivers as they navigate city streets, building up a massive data set of human decisions in the face of various situations. Patterns in this data can then be analyzed using machine learning algorithms to predict and mimic human decision-making in complex road environments, which may then enable the production of a safe self-driving car.[15]

Data is collected about us but primarily shared with others to benefit us.

## B. The Unhappy Status Quo

In considering the non-rivalrous nature of data, we see how the status quo harms competition and innovation.

As one of the pioneers of Artificial Intelligence observed, "today's technology is driven by algorithms," and in "machine learning, whoever has the most data wins."[16] Deep learning algorithms currently require lots of data, which only a few firms possess. A data-divide can lead to an AI divide where access to large datasets and computing power is needed to train algorithms. This can lead to an innovation divide. As one 2020 research paper found: "AI is increasingly being

shaped by a few actors, and these actors are mostly affiliated with either large technology firms or elite universities."[17] The "haves" are the data-opolies, with their large datasets, and the top-ranked universities with whom they collaborate; the "have nots" are the remaining universities and everyone else. The authors examined 171,394 papers from 57 leading computer science academic venues. What they found was a pecking order: Large technology firms "are publishing more in deep learning areas than both elite and non-elite universities." And elite universities and large technology firms "are increasingly contributing more to AI research relative to other computer science areas," while mid-tier and non-elite universities are publishing relatively fewer papers.[18] This divide is not due to industriousness. Instead, it is attributable, in part, to whether the university has access to the large tech firms' voluminous datasets and computing power.[19] Without "democratizing" these datasets by providing a "national research cloud," the authors warn that our innovations and research will be shaped by a handful of powerful tech firms and the elite universities they happen to support.[20]

Current market forces encourage data-hoarding, "as incumbents protect their data advantage over potential competitors by limiting access to it."[21] This data-hoarding prevents access to the essential raw ingredients needed for deep-learning research. It would be as if biochemists had the lab equipment, but not the basic organic materials and chemicals required for their research, which a few companies control. As long as large datasets are a crucial input, this AI divide will not self-correct.

When data-opolies hoard non-rivalrous data, society loses out in several significant ways. First, the data-opolies gain an unfair competitive advantage. As one review of the economic literature noted, the data-opolies can use data's non-rivalrous nature to give themselves an additional competitive advantage by leveraging the data internally across their many products and services, thereby increasing entry barriers.[22] When Google uses our geolocation data to improve its other products and services, like providing more relevant search results and prompting users for reviews of local restaurants, data-poorer rivals, like Yelp and TripAdvisor, are at an even greater competitive disadvantage.

Second, our privacy and autonomy are further threatened when the data-opolies steer the path of innovation toward their interests, not ours (such as research on artificial neural networks that can better predict and manipulate our behavior). As we saw with Facebook, data-opolies can share the personal data selectively with third parties, but only when it significantly benefits them (and

not necessarily consumers or society). In parceling out who can access their data and for what purpose, a few powerful platforms can shape the direction of deep learning (a field of artificial intelligence, where computers can learn by experience with large datasets and acquire skills without human involvement[23]). The data-opolies may not support research and innovation in areas that could threaten their business model or dominance. This includes Timnit Gebru, the co-lead of Google's ethical AI team. Google reportedly forced her out when a research paper she co-authored conflicted with its business interests.[24]

Third is the loss of potential helpful innovations that could have been derived from access to these voluminous datasets. Google, for example, is using AI to improve breast cancer detection.[25] But imagine the additional insights if other researchers had access to Google's large datasets to train algorithms for different innovative medical uses. So we lose out on these potential innovations and insights.

Finally, in increasing the AI divide, data-hoarding can make digital markets even more concentrated and less contestable. Data-opolies, in influencing or undertaking the research and innovation, can more easily colonize future ecosystems where deep-learning will likely play a key role, such as digital assistants, driverless vehicles, chatbots and service bots for customer service, neurotechnologies (including brain-computer interfaces where algorithms can decipher the "subtle patterns in brain activity" to identify words that a person was trying to say or their thoughts[26]), and health (from disease and tumor diagnoses to personalized medicines explicitly created for an individual's genome).

## C. Policies to Promote the Flow of Data

If data-hoarding is a barrier to competition and innovation in many digital platform markets, then data openness looks like a good solution. Democratizing the data counters the private incentives of powerful firms "to hoard data, potentially stifling competition and reducing the social benefits that could flow from wider access."[27] Rivals, like the search engines DuckDuckGo and Bing, need access to personal data to overcome entry barriers and the data-driven network effects. Competitors can make use of this data, given its non-rivalrous nature, and competition and innovation would flourish.

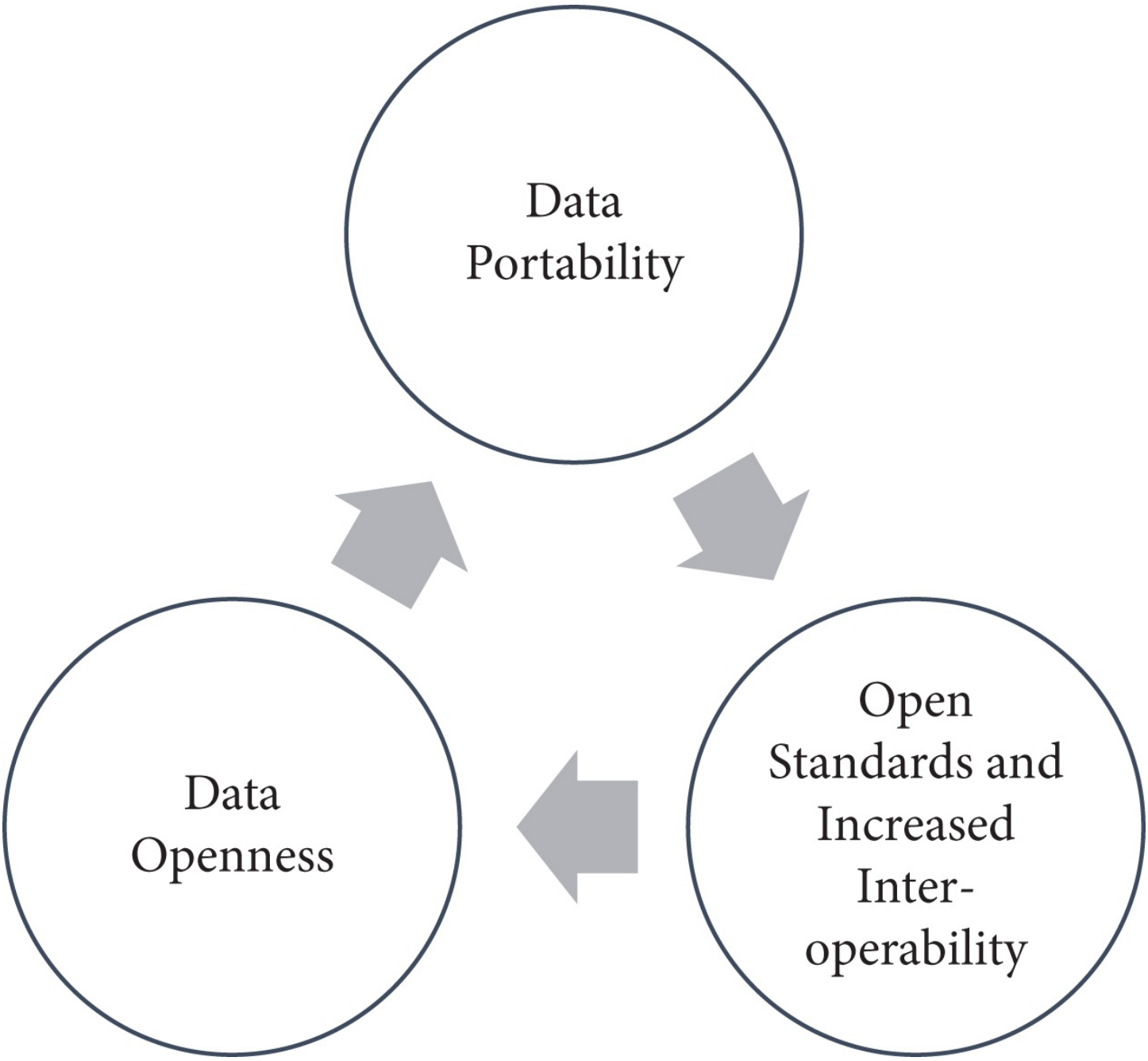


**Figure 7.1** Policies to promote the flow of personal data

Accordingly, to stimulate competition and innovation, competition officials seek to promote the flow of personal data. Figure 7.1 reflects three key policy mechanisms.

## 1. Data Portability

Data portability policies enable individuals to readily port their data across digital services, a feature that both the GDPR[28] and CPRA[29] incorporate, albeit incompletely.[30] Just as one can port one's banking data to another financial

institution in some countries,[31] so too individuals can port their data—whether their music lists, social network posts, or photos—to other platforms.

The hope is that stronger data portability provisions will lower our switching costs and provide us greater freedom. Data-opolies will be less able to lock us in and hoard our data. Other firms, with this data, can offer personalized services. Markets can become more contestable. Innovation could flourish as other firms unlock the value in our data.[32]

For example, bipartisan legislation has been proposed to allow users on large platforms to more easily port their data.[33] Likewise, Europe's Digital Markets Act proposes additional obligations on powerful gatekeepers to improve data portability for individuals and other businesses (with the individual's consent).[34]

Some, however, question whether data portability will reduce the data-opolies' power. After all, the Data Transfer Project, which Google, Apple, Facebook, Microsoft, and Twitter launched in 2018, seeks to improve data portability among platforms.[35] Why would data-opolies promote data portability, which in theory could erode their market power? And why hasn't data portability reduced their power, especially in light of Google's and Facebook's multiple privacy scandals?

Several reasons. First, data portability does not significantly diminish a platform's market power entrenched by network effects.[36] Suppose you learn that you can port your Facebook data today. Would you? And where to? As we saw in Chapter 2, Facebook knows that users will not port their data to a rival social network unless the users' friends also migrate to the same social network. In this "chicken-and-egg" problem, a rival social network will not emerge unless it will be assured that many people will switch to it, which is unlikely. So, Facebook allows you to port your data. But when there is no competing social network where you and your friends can switch, Facebook knows that you will not switch.[37]

Second, data portability is less important when the value of data and accompanying network effects depend on the *velocity* in processing the data.[38] Navigation apps, for example, need your current location to assess traffic conditions. Porting last week's or last year's geolocation data will not help smaller navigation apps. The same goes for search data. Porting older search query data will not necessarily help the smaller search engine tackle current uncommon (tail) inquiries. Thus, there is little incentive for users to port their data to (or use) DuckDuckGo, when the search results, based in part on the

network effects, are inferior to Google's search results. Consequently, users will remain with the dominant search engine, and websites will continue to focus on optimizing their websites for Google, not the smaller search engines. Data portability will not change this.[39]

Third, data portability is reactive. Suppose you can port your financial data to a particular lender. Also suppose you have an array of loans (investment properties, home mortgage, and car loans) and checking and savings accounts. Search costs, however, remain high. Prospective financial institutions, without personal data, will not know which individuals to target with competitive rates. And you have less incentive to switch unless you get more attractive interest rates and terms. But surveying numerous financial institutions is time consuming (and can potentially hurt your credit rating).[40] So, even with data portability, you are stuck: you do not know which lenders, based on your credit history and personal data, would offer a better rate. And financial institutions without your credit history and personal data cannot quickly identify you with an attractive offer.

Fourth, data portability can be cumbersome, complex, and time-consuming.[41] Although the GDPR requires that personal data be provided in a " 'structured, commonly used and machine-readable format' there is no explicit requirement for parties to develop technical standards to facilitate the transmission of personal data across suppliers."[42]

Finally, data portability depends on defining "what constitutes the personal data to which a user has exclusive rights."[43] The data portability provision may allow us to port only the data that we provided to the platform, not the data inferred about us, nor the data acquired from third parties about us, which may be far more critical to spurring competition.[44]

Consequently, policymakers seek to promote data portability, such as enabling the data transfer with a click of the button.[45] But many understand the need for additional measures to reduce switching costs and lock-in.[46]

## 2. Open Standards and Increased Interoperability

Why aren't we locked in our email accounts as much as our texting accounts? Basically, through open standards and increased interoperability, we can email others, whether they have an Apple, Google, Yahoo, AOL, or Microsoft account. We can use different browsers to surf the web (although many browsers rely on Google's open-source Chromium project). And we can telephone others whether

they are—or are not—within the same mobile network. The same cannot be said for mobile messaging apps, where Facebook controls the two largest networks, WhatsApp and Messenger.[47] A WhatsApp user cannot text an Apple Messages user. So, in limiting interoperability, Facebook and Apple can use network effects offensively, knowing that as more people text primarily with their apps, others will join Facebook's texting platforms or buy Apple products, increasing their dominance.[48]

Accordingly, the government can impose measures to increase interoperability, which increases the odds that other firms can access individuals and their data.[49]

Facebook, for example, would likely oppose efforts to increase interoperability between its social networks and other platforms and services. But to boost competition, the U.K. competition authority proposed making it easier for the billions of Facebook users to

- identify and make contact with friends or other potential contacts from other social platforms,
- post photos and updates across several platforms simultaneously,
- view posts from friends on other social platforms, or consolidate and view updates across social platforms,
- allow consumers to search for content across their aggregated services in real-time, and
- engage with content by commenting or "liking" it.[50]

The greater the interoperability, the less dependent we are on Facebook's platform. We can connect and communicate with others on multiple social networks, including Facebook, without having to be on Facebook.[51] Suppose greater interoperability helps level the competitive playing field. In that case, rivals might also have the incentive to help mitigate privacy risks by devising technologies that provide individuals greater control over their data. So, the competition and privacy concerns are lessened when "the decision to post content across platforms is user-initiated, freely given and informed."[52]

Another proposal is to enable each person to store the data they create and then have a personal API, which manages the information and provides permission to compatible apps to access or link to the data.[53]

Finally, policies are being proposed to prevent data-opolies from favoring their services and hindering the interoperability of rival services on its operating

system.[54]

But policymakers recognize that interoperability alone will not fully restore competition without meaningful choices and competition in the market today.[55] More is needed to deter data-hoarding.

## 3. Data Openness

A third measure is data openness. If personal data is necessary to compete and innovate, then distributing privately held data to universities, other nonprofits, government agencies, and market participants can spur new insights and innovation, close the AI divide, and increase competition and innovation.[56] The aim is to promote "access to non-personal or anonymised data, [which] will tackle the key barrier to entry in a digital market, while protecting privacy."[57]

One way to spur competition and innovation is to impose a legal duty on data-opolies to share data with rivals.[58] With immediate access to personal data, competitors can scale up. Google's persistently high market share in general search, as we saw in Chapter 1, is derived in part from the data-driven network effects. The more people "google," the more opportunities the leading search algorithm can learn what responses for uncommon "tail" queries are relevant, and the better the search results become. If rivals Bing and DuckDuckGo had real-time access to Google's ranking, query, click and view data, their search results could become more relevant (especially for the "tail" queries). More people might use the privacy-centric DuckDuckGo, and the ensuing competition would force Google to improve its privacy practices.

Thus, the European Commission and U.K. may require Google to provide rival search engines with click and query data that would help them improve their search algorithms and "overcome Google's scale advantages."[59] The EU is also considering requiring platforms "to share data with smaller rivals, especially when it comes to consumer behavior regarding the products sold by those competitors."[60]

Putting aside, for now, the privacy issues, data sharing can also skew incentives. Non-dominant firms do not have any antitrust duty to deal. Even monopolies generally do not have a duty to deal under the competition law.[61] One concern is that a general obligation to deal would incentivize rivals to free ride off the monopolies' efforts, and thereby chill the incentives to innovate.[62] Thus, policymakers propose imposing a duty to deal only when necessary (i.e., other less burdensome measures could not spur competition) and proportionate to

achieve its aims (to not chill the original data collector's incentives to compete and innovate).[63]

Consequently, to maximize the overall value derived from data's non-rivalrous nature, competition policymakers will be more predisposed to the collection of personal data and focus instead on "democratizing" the data—i.e., circulate and redistribute the data (with sufficient privacy safeguards). This assumption underlies many of the data mobility policy proposals to date, whether providing consumers greater freedom to share their data (through stronger data portability provisions) or improving other market participants' access to the personal data (by policies that promote multi-homing and interoperability and require data-opolies to provide rivals access to the personal data).

## D. The Privacy and Competition Levers

Imagine policymakers have two levers: one for privacy, another for competition. The privacy lever, through data minimization policies, tightens the flow of personal data. The competition lever democratizes the data through data openness principles.

Each lever can play an important role. The privacy lever would reduce the volume and variety of personal data that the data-opolies collect to a fraction. Basically, the minimum needed to provide the instant service. With no personal data for behavioral advertising, Google and Facebook would be less dominant. Without the velocity of personal data fueling their nowcasting radar, the data-opolies would find it harder to identify nascent competitive threats. With far less surplus data to train their algorithms, data-opolies would have less leverage to muscle into other markets that rely on deep learning. In providing us with greater control over our data, the privacy lever would diminish a vital source of the data-opolies' power. With their power pared, a data-opoly would find it harder to exclude rivals. Entry, competition, and innovation would increase.

But the competition official might argue that its lever would promote our welfare even more. To compete and innovate, companies need access to personal data. So, the competition lever, subject to some privacy safeguards, would widen the flow of personal data across the economy. With more non- and for-profit organizations extracting value from the data, the AI divide would narrow. Data-driven innovations and insights would increase. Smaller, data-poorer firms could effectively compete and differentiate themselves by offering greater privacy protections and privacy-centered innovations.

Consider the ensuing debate between the privacy and competition officials, each pulling their respective levers.

The competition official shouts, “Allow the data-opolies to collect the data. We can then re-circulate the data to the non-profits, businesses, and government with the competition lever. They will mine the data, and we’ll benefit.”

Seeing no response, the competition official next points to the unintended harm from the privacy law’s “data minimization” policies:

> You’re limiting the flow of personal data from the users. As a result, others now have to expend more time, money, and resources to access this data.
>
> Universities, for example, cannot easily tap into Facebook’s vast database since your data minimization policies are curtailing Facebook’s ability to collect or store this data.
>
> So when you’re restricting the platforms’ data collection, the reservoir of personal data for data-philanthropy is also shrinking.
>
> Universities and other research organizations now have to incur the costs to collect, clean, and organize that data.
>
> As these costs increase, less personal data will be collected overall.
>
> That’s destroying value—just consider all the potential value that could be unlocked from the data, and all the potential data-driven innovations.

The privacy official would likely respond, “How do you define value and value for whom?”

## E. How Do We Define Value, and Value for Whom?

Let us assume that data sharing can increase the value for the recipients. Critical here is asking how do we define value and value for whom. Suppose one’s geolocation data is non-rivalrous. Its value does not diminish if used for multiple, non-competing purposes:

- Apple could use geolocation data to track the user's lost iPhone.
- The navigation app could use the iPhone's location for traffic conditions.
- The health department could use the geolocation data for contact tracing (to assess whether the user came into contact with someone with COVID-19).
- The police could use the data for surveillance.
- The behavioral advertiser could use the geolocation data to profile the individual, influence her consumption, and assess the advertisement's success.
- The stalker could use the geolocation data to terrorize the user.

Although each could derive value from the geolocation data, the individual and society would not necessarily benefit from all of these uses. Take surveillance. In a 2019 survey, over 70% of Americans were not convinced that they benefited from this level of tracking and data collection.[64]

Over 80% of Americans in a 2019 survey and over half of Europeans are concerned about the amount of data collected for behavioral advertising.[65] Even if the government, behavioral advertisers, and stalkers derive value from our geolocation data, the welfare-optimizing solution is not necessarily to share the data with them and anyone else who derives value from the data.

Nor is the welfare-optimizing solution to encourage competition for one's data. As one survey of the economic literature noted, "exploiting the commercial value of data can often entail a reduction in private utility, and sometimes even in social welfare overall. Thus, consumers have good reasons to be concerned about unauthorized commercial application of their private information."[66]

## F. The Privacy Costs in Mining Data

Now suppose we anonymize a large dataset of Facebook users. Here we can democratize the data in allowing others to mine it for insights. But what happens to our privacy? Specifically, what are the risks of someone being able to re-identify the anonymized data to specific Facebook users? One might think that if the data is anonymized, we get all of the upsides (using the data to glean insights) with none of the privacy downsides. But that is wrong. One norm among computer scientists is that the privacy risk increases (however small) with the repeated mining of anonymized data for different purposes.[67] This is true with or without any privacy-preserving techniques, like differential privacy tools.

We shall examine the benefits of differential privacy tools in Chapter 11. For now, one benefit is the ability to measure the increase in privacy risk even when anonymized data is reused for another purpose.[68]

To illustrate, suppose a college has access to a large Facebook dataset for research purposes. To protect privacy, the university uses differential privacy tools to add "noise" to the anonymized data to make it more difficult to identify any specific Facebook user. Suppose five university departments want to analyze the dataset. The political science department, for example, would use the dataset to explore the extent to which online social networks influence voter turnout and political participation.

Knowing that mining even large anonymized datasets increases the risk of re-identifying individual Facebook users with their data, the university can use differential privacy tools to set the overall privacy loss parameter ε at 1. (We will learn more about that parameter in Chapter 11, but, for now, assume that the number represents the maximum level of acceptable privacy risk in re-identifying the Facebook users with the anonymized data.[69]) The privacy loss parameter ε for each of the department's studies is the following:

- psychology (0.8),
- marketing (0.7),
- political science (0.3),
- sociology (0.2), and
- neuroscience (0.1).

Great, one might say, as the privacy loss parameter for each study falls below the university's threshold of 1. But that assumes that only one department does its research. We know that the more the data is used by different departments for different purposes, the risk of re-identifying Facebook users with their data increases. So the beauty of the differential privacy tools is the ability to quantify that increase in privacy risk. As one study posited, one would add the privacy loss parameter ε for each of the department's studies: psychology (0.8) + sociology (0.2) + neuroscience (0.1) + marketing (0.7) + political science (0.3), which leads to overall privacy loss parameter ε of 2.1, twice the level of privacy risk that the university deems acceptable.[70]

If faculty meetings can be contentious, imagine how the university would decide which departments get to use the Facebook data. The sociology, neuroscience, and computer science departments might band together to get the

data, leaving other researchers to consume the remaining privacy loss parameter ε of 0.4. Recognizing this, the psychology department might rush for the Facebook data first, leaving the sociology and neuroscience departments to fight it out as to who gets to use the data for their research.

Here everyone agrees that the Facebook data is non-rivalrous in so far that each department can derive value for its research from the dataset. But it is not costless to our privacy even when the dataset is anonymized. As we will explore in Chapter 11, the risk of re-identification remains. Once this privacy risk is considered, the optimal result is not to provide each university department with the data, as the privacy risk will be too great. Ideally, the omniscient university could undertake a cost/benefit analysis and parcel out the Facebook data to those research projects that maximize overall value while keeping the overall privacy loss parameter ε at or below 1.

But in the real world, that would not happen. Instead, with multiple universities mining the Facebook data, we can have a classic market failure, similar to coal power plants' pollution. The universities (like the coal power plants) get many of the benefits from the cheap data (fuel) but do internalize the privacy (pollution) costs. Instead, Facebook users bear the privacy costs from the universities' researching activities. Since the universities do not internalize these costs, they have little incentive to incur the time, effort, and expense to collectively agree on an overall privacy loss parameter and on which research projects would get the Facebook data (a contentious, subjective undertaking). Instead, each university would mine the Facebook data, even if its research value is low, and not care about the negative externality on Facebook users' privacy.

The differential privacy tools are not the problem.[71] Instead, these tools simply quantify what was formerly hidden: Repeatedly mining anonymized data has privacy costs. Those costs can quickly add up as more entities mine the data, and we ultimately pay that cost with our privacy.

## G. Reflections

The fact that personal data is non-rivalrous does not necessarily point to the optimal policy outcome. It does not suggest that data should be priced at zero. Indeed, "free" granular personal datasets can make us worse off.

Avoiding the competition and privacy levers is not the answer, as the digital economy will not self-correct. The status quo, while benefiting the data-opolies, promotes neither competition, innovation, nor privacy. Under the current legal

environment, data-opolies violate our privacy, hoard our personal data, and selectively provide third parties access when it advances their business interests. Under their quasi-regulatory regime, the data-opolies will continue to set the rules around surveillance and data sharing not just within their ecosystems but for other market participants. The data will continue to fuel their nowcasting radar to identify and squelch nascent competitive threats. The data-opolies will continue to infringe our privacy as they colonize new markets, where they will promote toxic (rather than healthy) competition and will make it harder for anyone that threatens their power.

To change the status quo, policymakers must adjust the privacy lever to minimize data collection and processing while adjusting the competition lever to foster greater data mobility.

But the fact that data is non-rivalrous does not suggest that privacy and competition are inherently at odds. Privacy can be a critical non-price component of competition. Competition along this parameter can deliver greater privacy protection (and better privacy technologies). Likewise, privacy policies can promote healthy competition.

But at times, privacy and competition will be at odds.[72] As one 2019 IMF report recognized, "The collection of personal data has always involved a trade-off between respecting the individual's desire for privacy—including from government—and reaping the commercial and social benefits that can be derived from its collection and dissemination."[73] When the data minimization and data democratization levers are in tension, who should decide these trade-offs, and how? Policymakers have not directly addressed these issues. Instead, they address the privacy-competition conflict indirectly, in promoting one lever over another. But when directly confronted with a privacy-competition conflict, four traps, as we will see next, await them.

---

1 *What Are Non-rivalrous Goods?*, Corporate Finance Institute (last visited Mar. 9, 2021), https://corporatefinanceinstitute.com/resources/knowledge/economics/non-rivalrous-goods/ [https://perma.cc/DMX7-9V67]; Majority Staff of H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial and Administrative Law, Report and Recommendations: Investigation of Competition in Digital Markets (2020) at 43, https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429 [https://perma.cc/29LN-L4BL] [hereinafter House Report].

2 *Fitbit Privacy Policy: Information We Collect*, Fitbit (Oct. 8, 2020), https://www.fitbit.com/us/legal/privacy-policy#info-we-collect [https://perma.cc/LX8Y-

4KWE].

3 Stephen P. Wright et al., *How Consumer Physical Activity Monitors Could Transform Human Physiology Research*, 312 Am. J. Physiology: Regulatory, Integrative & Compar. Physiology R358 (2017), https://pubmed.ncbi.nlm.nih.gov/28052867/ [https://perma.cc/KG43-W9QR].

4 Rob Copeland et al., *Inside Google's Quest for Millions of Medical Records*, Wall St. J. (Jan. 11, 2020), https://www.wsj.com/articles/paging-dr-google-how-the-tech-giant-is-laying-claim-to-health-data-11578719700.

5 European Commission, *Regulation on Data Governance—Questions and Answers* (Nov. 25, 2020), https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2103.

6 Cathrin Schaer, *Coronavirus: They Want to Use Your Location Data to Fight Pandemic. That's a Big Privacy Issue*, ZDNet (Mar. 19, 2020), https://www.zdnet.com/article/coronavirus-they-want-to-use-your-location-data-to-fight-pandemic-thats-a-big-privacy-issue/ [https://perma.cc/UG4G-YNM3].

7 Donald G. McNeil, *Can Smart Thermometers Track the Spread of the Coronavirus?*, N.Y. Times (Mar. 18, 2020), https://www.nytimes.com/2020/03/18/health/coronavirus-fever-thermometers.html [https://perma.cc/3QW4-8BBU].

8 Exec. Order No. 13,994, 86 Fed. Reg. 7189 (Jan. 26, 2021), https://www.govinfo.gov/content/pkg/FR-2021-01-26/pdf/2021-01849.pdf (requiring the "Director of OMB, in consultation with the Director of OSTP, the United States Chief Technology Officer, and the COVID-19 Response Coordinator, shall promptly review the Federal Government's existing approaches to open data, and shall issue supplemental guidance, as appropriate and consistent with applicable law, concerning how to de-identify COVID-19-related data; how to make data open to the public in human- and machine-readable formats as rapidly as possible; and any other topic the Director of OMB concludes would appropriately advance the policy of this order. Any guidance shall include appropriate protections for the information described in section 5 of this order.").

9 Jeff Horwitz, *Facebook Delivers Long-Awaited Trove of Data to Outside Researchers*, Wall St. J. (Feb. 13, 2020, https://www.wsj.com/articles/facebook-delivers-long-awaited-trove-of-data-to-outside-researchers-11581602403 (discussing delays in Facebook's Social Science One project, which allows "a select group of academics to study internal data about how content gets shared on its platform, which could lead to a better understanding of patterns in fake news").

10 EU Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)* (Nov. 25, 2020), COM(2020) 767 final, 2020/0340(COD), https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act.

11 Gil Press, *Cleaning Big Data: Most Time-Consuming, Least Enjoyable Data Science Task, Survey Says*, Forbes (Mar. 23, 2016), https://www.forbes.com/sites/gilpress/2016/03/23/data-preparation-most-time-consuming-least-enjoyable-data-science-task-survey-says [https://perma.cc/5CNQ-PBEU] (finding that the surveyed data scientists spent 60% of their time on cleaning and organizing data, and

19% of their time collecting data sets "meaning data scientists spend around 80% of their time on preparing and managing data for analysis" and 76% of the surveyed data scientists "view data preparation as the least enjoyable part of their work").

12 Yan Carrière-Swallow & Vikram Haksar, *The Economics and Implications of Data: An Integrated Perspective*, International Monetary Fund Policy Paper No. 19/16 (Sept. 2019), https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596, at 5 ("Like a new idea, society will benefit most from data when it is widely shared, because more users will be able to use it to increase efficiency and innovate."), 13 (noting how data is non rivalrous as "one agent's use of data does not diminish the ability of others to use it, even simultaneously") & 14 ("An important implication of the nonrivalry of data is that, from a social perspective, it is desirable for data to be widely shared.").

13 Brice McKeever et al., *Data Philanthropy: Unlocking the Power of Private Data for Public Good*, Urban Institute (July 2018), https://www.urban.org/sites/default/files/publication/98810/data_philanthropy_unlocking_the [https://perma.cc/FY25-YMSJ].

14 *Announcing the Social Media and Democracy Research Grants*, Social Science Research Council, https://www.ssrc.org/pages/announcing-the-social-media-and-democracy-research-grants/ (last visited Mar. 9, 2021) [https://perma.cc/79MP-DMBU] (noting how Facebook will make data available to independent social science researchers for the first time).

15 Carrière-Swallow & Haksar, *supra* note 12, at 10.

16 Terrence J. Sejnowski, The Deep Learning Revolution 166 & 195 (2018).

17 Nur Ahmed & Muntasir Wahed, *The De-democratization of AI: Deep Learning and the Compute Divide in Artificial Intelligence Research* (Rev. Oct. 22, 2020), https://arxiv.org/pdf/2010.15581.pdf [https://perma.cc/7NCW-YPU6].

18 *Id.* at 4.

19 *Id.*

20 *Id.* at 4–6; see also Ariel Ezrachi & Maurice E. Stucke, How Big-Tech Barons Smash Innovation—and How to Strike Back (2022).

21 Carrière-Swallow & Haksar, *supra* note 12, at 14.

22 Carrière-Swallow & Haksar, *supra* note 12, at 22:

> . . . where data appears as one of the factors of production, nonrivalry of data gives rise to increasing returns to scale when data is combined with other inputs. The intuition is that each unit of data can be used by all units of other inputs simultaneously. A larger stock of complementary labor or capital allows each unit of data to be better exploited, raising the average product of data. An implication is that access to the same nonrival data results in larger firms with more complementary inputs being more productive than those with fewer inputs. This will tend to increase average firm size in the economy and can potentially stifle competition by representing a barrier to entry for smaller, data-poor firms.

23 Bernard Marr, *What Is Deep Learning AI? A Simple Guide with 8 Practical Examples*, Forbes (Oct. 1, 2018), https://www.forbes.com/sites/bernardmarr/2018/10/01/what-is-deep-learning-ai-a-simple-guide-with-8-practical-examples/ [https://perma.cc/NPR3-VSRD].

24 Karen Hao, *We Read the Paper That Forced Timnit Gebru Out of Google. Here's What It Says*, MIT Tech. Rev. (Dec. 4, 2020), https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru/.

25 Martin Stumpe, *Applying Deep Learning to Metastatic Breast Cancer Detection*, Google AI Blog (Oct. 12, 2018), https://ai.googleblog.com/2018/10/applying-deep-learning-to-metastatic.html [https://perma.cc/78AK-PKP4].

26 Robin Marks, *"Neuroprosthesis" Restores Words to Man with Paralysis - Technology Could Lead to More Natural Communication for People Who Have Suffered Speech Loss*, University of California San Francisco (July 14, 2021), https://www.ucsf.edu/news/2021/07/420946/neuroprosthesis-restores-words-man-paralysis?utm_source=ucsf_fb&utm_medium=fb&utm_campaign=2021_neuroprosthesisresults; Tech@Facebook, *Imagining a New Interface: Hands-free Communication Without Saying a Word* (March 30, 2020), https://tech.fb.com/imagining-a-new-interface-hands-free-communication-without-saying-a-word/.

27 Carrière-Swallow & Haksar, *supra* note 12, at 1.

28 Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC [hereinafter GDPR] art. 20, https://gdpr-info.eu/ (providing that "[t]he data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided").

29 California Privacy Rights Act of 2020 § 1798.110(c)(5), https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf [hereinafter CPRA].

30 *See* Digital Competition Expert Panel, Unlocking Digital Competition at 25 (2019) (also known as the Furman Report), ¶ 2.59, https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel [https://perma.cc/VK9M-3GV8] [hereinafter Furman Report] (identifying some of the limitations of the GDPR's data portability right).

31 *Open Banking Around the World: Towards a Cross-Industry Data Sharing Ecosystem*, Deloitte (Nov. 29, 2018), https://blogs.deloitte.co.uk/financialservices/2018/11/open-banking-around-the-world-towards-a-cross-industry-data-sharing-ecosystem.html [https://perma.cc/9S2Q-ELDM].

32 Discussion paper on Data Portability, Personal Data Protection Commission in

Collaboration with Competition and Consumer Commission of Singapore (Feb. 25, 2019), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf?la=en.

33 ACCESS Act of 2019, S. 2658, 116th Cong., https://www.govinfo.gov/content/pkg/BILLS-116s2658is/pdf/BILLS-116s2658is.pdf; The Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2021, H.R. 3849, 117th Cong. § 3 (requiring platforms that fall within the definition of a "covered platform" to maintain "a set of transparent, third-party-accessible interfaces (including application programming interfaces) to enable the secure transfer of data to a user, or with the affirmative consent of a user, to a business user at the direction of a user, in a structured, commonly used, and machine-readable format that complies with the standards issued under [the Act]"); *see also* Ylan Mui, *A Bipartisan Group of Senators Wants to Help You Leave Facebook*, CNBC (Oct. 22, 2019), https://www.cnbc.com/2019/10/22/bipartisan-group-of-senators-introduce-data-portability-bill.html [https://perma.cc/3CTF-J7M4].

34 European Commission, Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), at 27 (Dec. 15, 2020), https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf [https://perma.cc/G87S-Q88U] [hereinafter Digital Markets Act]:

> To ensure that gatekeepers do not undermine the contestability of core platform services as well as the innovation potential of the dynamic digital sector by restricting the ability of business users to effectively port their data, business users and end users should be granted effective and immediate access to the data they provided or generated in the context of their use of the relevant core platform services of the gatekeeper, in a structured, commonly used and machine-readable format.
>
> This should apply also to any other data at different levels of aggregation that may be necessary to effectively enable such portability. It should also be ensured that business users and end users can port that data in real time effectively, such as for example through high quality application programming interfaces. Facilitating switching or multi-homing should lead, in turn, to an increased choice for business users and end users and an incentive for gatekeepers and business users to innovate.

35 *About Us*, Data Transfer Project, https://datatransferproject.dev/ (last visited Mar. 9, 2021) [https://perma.cc/6XH9-JZ2G].

36 House Report at 387 (noting that data portability alone "would not fully address concerns related to network effects since consumers would still need to recreate their networks on a new platform and would not be able to communicate with their network on the incumbent platform").

37 Australian Competition and Consumer Commission, Digital Platforms Inquiry—Final Report at 116 (2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report

[https://perma.cc/M36S-YQJ4] [hereinafter ACCC Final Report]; House Report at 145–46 (discussing how in contrast to its public statements, Facebook employees internally "recognize that high switching costs insulate Facebook from competition"; outlining why Facebook has not done enough to facilitate data portability for its consumers, so that, "while Facebook publicly claims to support data portability, its users seldom leave Facebook due to the challenges of migrating their data").

38 Background Note by the Secretariat, Consumer Data Rights and Competition, OECD Doc. DAF/COMP(2020)1 (Apr. 29, 2020), https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf at ¶ 173 [https://perma.cc/SQ48-WEPD] [hereinafter OECD Consumer Data Rights and Competition] (data portability "may not facilitate multi-homing or the provision of complementary services that rely on continuous, potentially real-time, transfers of consumer data"); Jacques Crémer, Yves-Alexandre de Montjoye, & Heike Schweitzer, Special Advisers' Report: Digital Policy for the Digital Era (2019), https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf [https://perma.cc/NV44-U3R2].

39 ACCC Final Report at 116.

40 Frederic Huynh, The Skinny on FICO® Scores and Inquiries, FICO/blog (May 21, 2012), https://www.fico.com/blogs/skinny-ficor-scores-and-inquiries (explaining that multiple credit inquiries by consumers seeking new credit accounts can account up to 10 percent of their FICO credit score).

41 Furman Report at 65 (noting that data portability provisions often rely "on a consumer to manually request and download their data, convert it into a format required by the business they want to move it to and to upload it again").

42 Furman Report at 68.

43 Bhaskar Chakravorti, *Why It's So Hard for Users to Control Their Data*, Harv. Bus. Rev. (Jan. 30, 2020), https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data [https://perma.cc/MT22-LN46].

44 OECD Consumer Data Rights and Competition, *supra* note 37, at ¶ 176 ("it appears to be generally accepted that data portability should not extend to inferred data"); Note by the European Union, Consumer Data Rights & Competition, OECD Doc. DAF/COMP/WD(2020)40 (June 12, 2020) at ¶ 23, https://one.oecd.org/document/DAF/COMP/WD(2020)40/en/pdf [https://perma.cc/Y66C-2UEV] (noting that the data portability right under the GDPR applies only to personal data provided by the data subject, and "'observed data' provided by the data subject by virtue of the use of the service or device" but not inferred or derived data "such as the results of algorithmic analysis or other assessments performed on the data provided"); Furman Report at 69.

45 Furman Report at 65.

46 ACCC Final Report at 115 (finding with respect to Google and Facebook that "it is not clear that enhanced data portability would generate new entry or facilitate switching").

47 H. Tankovska, *Most Popular Mobile Messaging Apps Worldwide as of January 2021,*

*Based on Number of Monthly Active Users*, Statista (Feb. 10, 2021), https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ [https://perma.cc/E4SJ-DQF4].

48 House Report at 142 (discussing how network effects and tipping points "are particularly strong in messaging apps," since "WhatsApp and other regional messaging apps have bimodal distribution of reach in countries—an all-or-nothing reach at above 90% or below 10%—messaging tends toward consolidation and market tipping"; as a result, most countries "have a single messaging app or protocol because they cannot support multiple messaging apps").

49 *See, e.g.*, House Report at 386 (discussing how an interoperability requirement "would allow competing social networking platforms to interconnect with dominant firms to ensure that users can communicate across services," "breaks the power of network effects by allowing new entrants to take advantage of existing network effects at the level of the market, not the level of the company," and "would also lower switching costs for users by ensuring that they do not lose access to their network as a result of switching") (internal footnotes and quotations omitted); ACCESS Act of 2021 § 4(a) (requiring covered platforms to "maintain a set of transparent, third-party-accessible interfaces (including application programming interfaces) to facilitate and maintain interoperability with a business user that complies with the standards issued under [the Act]").

50 UK Competition & Markets Authority, Online Platforms and Digital Advertising Market Study: Market Study Final Report (July 1, 2020), at ¶¶ 3.217 & 8.56, https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digit [https://perma.cc/DA5V-RHA5] [hereinafter CMA Final Report].

51 CMA Final Report ¶ 92; OECD Consumer Data Rights and Competition, Note from the UK, OECD Doc. DAF/COMP/WD(2020)51 (June 2, 2020) at ¶ 19, https://one.oecd.org/document/DAF/COMP/WD(2020)51/en/pdf [https://perma.cc/76KL-DF6G] (noting that the United Kingdom is considering as a response to Facebook's powerful position in social media, inter alia, whether Facebook "should be required to interoperate specific features with existing competitors (such as the ability to post content across several platforms simultaneously); whether there should be limits on Facebook's ability to impose restrictions on competitors' use of the interoperable features and whether aspects of past API access should be restored to facilitate competition; whether any rules requiring greater interoperability should apply to Facebook alone or also to other social media platforms"); Furman Report at 67.

52 CMA Final Report at ¶ 8.63.

53 CMA, UK Competition & Markets Authority, Online Platforms & Digital Advertising: Market Study Interim Report (2019), Appendix L at ¶ 42, https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pd [hereinafter CMA Interim Report] (discussing Solid PODS (personal online data stores), whose "framework is aimed at avoiding lock-in to any online service, and improving privacy for the users and creating an ecosystem in which developers can create apps without needing

to harvest massive amounts of data").

54 *See, e.g.*, Digital Markets Act Art. 6(f) (requiring gatekeepers to "allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services"); American Choice and Innovation Online Act, H.R. 3816, 117th Congress, 1st Session; American Innovation and Choice Online Act, S. 2992, 117th Congress, 1st Session; Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2021, H.R. 3849, 117th Congress, 1st Session.

55 House Report at 386.

56 Furman Report at 74.

57 *Id.* at 6.

58 CMA Final Report at ¶ 90.

59 CMA Final Report at ¶ 85; Digital Markets Act Art. 6(j) (requiring gatekeepers to "provide to any third party providers of online search engines, upon their request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data").

60 Valentina Pop, *Big Tech to Face More Requirements in Europe on Data Sharing, AI*, Wall St. J. (Feb. 19, 2020), https://www.wsj.com/articles/big-tech-to-faces-more-restrictions-in-europe-on-data-ai-11582111937.

61 As the Supreme Court noted over 100 years ago, "[i]n the absence of any purpose to create or maintain a monopoly, the [Sherman] act does not restrict the long recognized right of trader or manufacturer engaged in an entirely private business, freely to exercise his own independent discretion as to parties with whom he will deal . . ." United States v. Colgate & Co., 250 U.S. 300, 307 (1919). The Court limited the scope of when a monopoly has an antitrust duty to deal in Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398, 409 (2004) and later noted that "there are rare instances in which a dominant firm may incur antitrust liability for purely unilateral conduct" and "limited circumstances in which a firm's unilateral refusal to deal with its rivals can give rise to antitrust liability." Pac. Bell Tel. Co. v. Linkline Commc'ns, Inc., 555 U.S. 438, 448 (2009). Of course, different justices, reading the older case law, could clarify and broaden the duty to deal. But one district court in dismissing the FTC's and states' monopolization claims against Facebook did the opposite in declaring unilateral refusals to deal essentially "per se lawful" and "presumptively legal." New York v. Facebook, Inc., No. CV 20-3589 (JEB), 2021 WL 2643724, at *10 (D.D.C. June 28, 2021) (internal citations omitted); Fed. Trade Comm'n v. Facebook, Inc., No. CV 20-3590 (JEB), 2021 WL 2643627, at *15 (D.D.C. June 28, 2021). In Europe, the duty to deal is arguably broader. Eur. Comm'n, Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings, 2009 O.J. (C 45) ¶¶ 75–90, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009XC0224(01)&from=EN.

Nonetheless, "[w]hen setting its enforcement priorities, the Commission starts from the position that, generally speaking, any under-taking, whether dominant or not, should have the right to choose its trading partners and to dispose freely of its property." *Id.* at ¶ 75.

62 Berkey Photo, Inc. v. Eastman Kodak Co., 603 F.2d 263, 285 (2d Cir. 1979).

63 Furman Report at 75.

64 Brooke Auxier et al., *Americans Concerned, Feel Lack of Control over Personal Data Collected by Both Companies and the Government*, Pew Res. Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/ [https://perma.cc/3PPH-TTHU] (approximately "three-quarters of adults say they benefit very little or none from the data that companies (72%) or the government (76%) collect about them. On the other hand, about three-in-ten Americans (28%) say they get a great deal or some personal benefit from companies' collecting data, and 23% say the same about the government's efforts"); *see also* Alessandro Acquisti, Curtis Taylor, & Liad Wagman, *The Economics of Privacy*, 54 J. Econ. Lit. 442, 476 (2016), https://dx.doi.org/10.1257/jel.54.2.442.

65 Auxier et al., *supra* note 65; European Union Note, *supra* note 45, at ¶ 11; Special Eurobarometer survey no. 447 on "Online platforms," June 2016, p. 52, https://ec.europa.eu/information_society/newsroom/image/document/2016-24/ebs_447_en_16136.pdf ("clear majority of Internet and online platforms users feel uncomfortable with the fact that the different types of online platforms use information about their online activity and personal data to tailor advertisements or content to what interests them"—55% were uncomfortable with search engines using information about their online activity and personal data to create tailored advertisements or content; 56% were uncomfortable with the fact that online marketplaces use information about their online activity and personal data; and 58% were uncomfortable with online social networks using information on their online activity and personal data to tailor advertisements or content).

66 Acquisti et al., *supra* note 65, at 476 (collecting earlier studies).

67 Alexandra Wood et al., *Differential Privacy: A Primer for a Non-Technical Audience*, 21 Vand. J. Ent. & Tech. L. 209, 244 & 251 (2018).

68 Harvard University Privacy Tools Project, Differential Privacy, Privacy as a Quantifiable Measure, https://privacytools.seas.harvard.edu/differential-privacy (last assessed Mar. 18, 2021):

> A crucial feature of differential privacy is that it defines privacy not as a binary notion of "was the data of individual exposed or not," but rather a matter of accumulative risk. That is, every time a person's data is processed her risk of being exposed increases. To this end, the definition of differential privacy is equipped with parameters ("epsilon and delta") that quantify the "privacy loss"—the additional risk to an individual that results from her data being used. Regardless of any auxiliary knowledge used in a re-identification attack, the risk to one's privacy caused by a differentially private algorithm will forever be bounded by this privacy loss.

69 Emily Einhorn, *Brain Data and Differential Privacy*, Columbia U. NeuroRights Initiative (July 15, 2020), https://nri.ntc.columbia.edu/news/brain-data-and-differential-privacy (noting that a privacy loss parameter "is a variable within the [Differential Privacy] mathematical formula that determines how much privacy can be compromised for any single individual when an analysis is performed on a dataset. A privacy loss parameter of zero means that full privacy of each individual within the data set is fully guaranteed. However, perfect privacy always comes with a trade off. The greater the privacy guarantee in the DP equation, the more noise that is used and consequently, the less accurate the outcome is of any analysis using that data. A privacy parameter of zero is seldom used because it requires so much noise that it renders the data nearly useless.")

70 Wood et al., *supra* note 68, at 252 (noting that the composition theorems developed for differential privacy state that "the composition of two differentially private analyses results in a privacy loss that is bounded by the sum of the privacy losses of each of the analyses").

71 Wood et al., *supra* note 68, at 251 (noting that it "a fundamental law of information that privacy risk grows with the repeated use of data, and hence this risk applies to any disclosure limitation technique," and that "traditional SDL techniques—such as suppression, aggregation, and generalization—often reduce accuracy and are vulnerable to loss in privacy due to composition").

72 CMA Interim Report Appendix L at ¶¶ 74–85.

73 Carrière-Swallow & Haksar, *supra* note 12, at 3.

# 8
# Avoiding Four Traps When Competition and Privacy Conflict

While both are important, neither privacy nor competition are absolute rights.[1] Each must be balanced against other important societal interests and fundamental rights. So, when should competition trump personal privacy? When should privacy trump competition? In deciding this, policymakers can fall into at least four traps:

1. When in doubt, opt for competition;
2. When in doubt, opt for privacy;
3. Confusing what is measurable with what is important; and
4. Celebrating what looks like an impressive privacy improvement when they should instead be wary.

## A. First Trap: When in Doubt, Opt for Competition

The first trap is to overly rely on the competition lever. Although there is no fundamental right to competition, the U.S. Supreme Court did call the competition laws "the Magna Carta of free enterprise" and as "important to the preservation of economic freedom and our free-enterprise system as the Bill of Rights is to the protection of our fundamental personal freedoms."[2] Likewise, Europe seeks to "guarantee" for its citizens effective competition and "the openness and competitiveness of the digital single market."[3]

The conventional wisdom is that increasing competition will make us better off. In contrast, increasing privacy protections can make us better or worse off, depending on the particular context and conditions. Both economic theory and the empirical analysis of privacy, according to one 2016 review, show that "[i]n some scenarios, privacy protection can decrease individual and societal welfare; in others, privacy protection enhances them."[4]

From this, policymakers could deduce that increasing privacy will not always improve our welfare, but increasing competition will. So, when privacy and competition clash, and one cannot calculate the welfare gains from increasing either, the policymaker might conclude that increasing competition (at the cost of privacy) is the prudent choice to maximize well-being. In uncritically assuming

that competition is always good, policymakers will ease up on privacy protection and open the data spigot to enable market participants greater access to personal data.

The trap, of course, is in assuming that the ensuing competition will always benefit us. As we saw in Chapter 4, competition, at times, is toxic. Apps and websites currently compete to secure more data about us. When the incentives are misaligned, as in ecosystems dependent on behavioral advertising revenue, increasing the competitive pressure, like increasing an arms race, will harm us. With 81,000 companies currently tracking us online, increasing this toxic competition will only pressure them to find ingenious ways to collect even more personal data *about* us, but not *for* us.

Even when the competition is not toxic, the incremental welfare gain from the increased competition may be outweighed by the welfare losses from the degradation in privacy. So, when privacy and competition conflict, policymakers cannot reflexively opt for more competition.

## B. Second Trap: When in Doubt, Opt for Privacy

The second trap is to overly rely on privacy's data minimization principles. Privacy, as we saw, is a fundamental right in Europe, California, and elsewhere.

Thus, promoting privacy is both an end itself (i.e., the "intrinsic value of privacy as a human right, or individuals' innate desires for privacy regardless of the associated economic benefits or lack thereof"[5]), and the means to promote other societal goals (for example, associational privacy can promote, at times, social change and a vibrant democracy).

In contrast, competition is not an end itself. We value competition only as the means for some greater end. A competitive process is effective only if it promotes broader societal or government objectives and represents the more efficient (or democratic) means to achieve these other objectives. Three consequences follow: First, there must be one or more intermediate or ultimate goals of competition law. Second, one must consider how, and under what circumstances, the competitive process can effectively promote these objectives. Third, competition's economic goals (such as promoting efficiency) must be balanced against other important societal objectives (such as privacy, autonomy, fairness, and justice).

So, what is the ultimate goal of competition? Let us posit, as St. Thomas Aquinas and Aristotle, among others, did, that happiness is logically its own

end.[6] If happiness is a complete and self-sufficient end for many individuals, observed Jeremy Bentham, then maximizing happiness is the proper end for the government.[7] The OECD, among others, is developing well-being metrics that policymakers can use to design policies that improve overall well-being.[8] Consequently, if promoting well-being is the proper (or at least a primary) end for government, then competition policy should advance (or at least not hinder) the community's ability to maximize overall well-being.[9]

A cornerstone for well-being and democracies is in enabling individuals to protect their privacy. As one state constitution notes, "[t]he right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."[10] Supreme Court Justice Louis Brandeis discerned this privacy right in the U.S. Constitution:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive right and the right most valued by civilized men.[11]

Likewise, Europe's 1995 privacy directive states that "data-processing systems are designed to serve man" and must respect our "fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals."[12] Consequently, privacy is both an end itself and can promote well-being, the ultimate end of any competition policy. When privacy and competition conflict, some policymakers might opt for greater privacy protection.

The trap is that a stringent privacy policy (in minimizing the amount of data collected, processed, and stored; and the uses for such data) can reduce overall well-being. We do not know what level of privacy protection will increase overall well-being. Just as too much personal data can exclude persons from the market (such as those with severe preexisting health conditions), so too the opposite poses risks. With too little personal data collected and shared, some individuals will be excluded from the marketplace, health and safety risks can increase, and overall well-being can decline.

For example, individuals will be excluded from receiving affordable offers for

credit when lenders have too little information from third parties about the borrowers' creditworthiness and risk.[13] As *The Wall Street Journal* reported in late 2019, "45 million to 60 million consumers lack the credit history needed to generate reliable credit scores under the current system, and millions more do not have access to affordable credit because of low scores."[14] This problem is "particularly acute for people with low incomes."[15] As a result, without sufficient personal data about their finances independently available to lenders, individuals are not offered credit or only at prohibitive terms.

In 2020, for example, the U.S. government's coronavirus stimulus package prohibited lenders that allow borrowers to defer their debt payments to report these payments as late to credit-reporting companies. This, in turn, caused lenders, without accurate information on applicants' creditworthiness, to pull back in offering credit.[16]

Here, to evaluate the borrower's creditworthiness, the lender relies on personal information of the borrower's economic and social activity from multiple sources. This dissemination of personal data "may alleviate adverse selection effects, address collateral constraints, and broaden the number of clients able to obtain a loan, but it may also lead to the exclusion of those that exhibit traits associated with risky financial behavior."[17] So in preventing the dissemination of personal information, stringent privacy policies can make it harder to obtain a loan or apply for a job. A vicious cycle can emerge: many poor, in their current living conditions, have less privacy than the wealthy.[18] In preventing the poor from accessing capital on better terms, privacy protections can trap them in poverty and misery.

Access to data can also foster health insights, improve security, reduce fraud, promote innovation, and provide other benefits. Thus, as two IMF officials observe, "A key question is whether, given the substantial benefits to consumers and markets from revealing personal data, granting strict user control rights would lead them to stop sharing their data in most cases, which may make some services unviable and stifle future innovation."[19] A strict data minimization policy might inhibit collecting and sharing personal data, even when the societal benefits are significant, as in health and geolocation data during the next pandemic. So, when privacy and competition conflict, policymakers cannot reflexively opt for more privacy.

### C. Third Trap: Confusing What Is Measurable with What Is Important

Increasing either competition or privacy might increase or reduce overall welfare, depending on the circumstances. When in doubt, policymakers cannot reflexively opt for one lever over the other. In avoiding the first two traps, policymakers will likely confront multiple trade-offs. In making these trade-offs, policymakers must avoid the third trap—confusing what is measurable with what is important. When receiving the Nobel Prize for economics, F.A. Hayek noted this fundamental problem in his field:

> Unlike the position that exists in the physical sciences, in economics and other disciplines that deal with essentially complex phenomena, the aspects of the events to be accounted for about which we can get quantitative data are necessarily limited and may not include the important ones. While in the physical sciences it is generally assumed, probably with good reason, that any important factor which determines the observed events will itself be directly observable and measurable, in the study of such complex phenomena as the market, which depend on the actions of many individuals, all the circumstances which will determine the outcome of a process [ . . .] will hardly ever be fully known or measurable. And while in the physical sciences the investigator will be able to measure what, on the basis of a prima facie theory, he thinks important, in the social sciences often that is treated as important which happens to be accessible to measurement.[20]

Nonetheless, despite Hayek's admonition in 1974, antitrust policy for the next 45 years focused on price, with less attention to quality and innovation. As Allen Grunes and I discuss in our book, *Big Data and Competition Policy*, antitrust enforcers had myopically evaluated mergers and restraints on what was quantifiable—such as the merger's likely impact on price or output—even when that was far less important than other non-quantifiable parameters of competition, such as quality, privacy, and innovation. They also ignored issues of systemic risk (that is, creating institutions too big to fail).[21] In reviewing Facebook's acquisition of Instagram and WhatsApp, the antitrust authorities never read (or ignored) the internal documents on how Facebook used its nowcasting radar to identify and kill nascent competitive threats. And they collectively failed to appreciate the merger's deleterious impact on privacy. Focusing on price in the digital economy gave an incomplete (and often wrong) conclusion.

But most agencies now look beyond price effects. In 2020, the FTC and nearly every state attorney general challenged Facebook's acquisitions of WhatsApp and Instagram, alleging that the mergers deprived users of, among

other things, better privacy and data collection options.[22] While the district court dismissed the monopolization complaints, it accepted that a loss in privacy would effectively mean that "millions . . . experienced a rise in the effective price of using Facebook."[23] Few, if any, policymakers view data-opolies as benign because their retail prices are low (Amazon) or free (Google and Facebook).

Nonetheless, Facebook sought to dismiss the FTC's and states' lawsuits, arguing that it cannot be a monopoly since it has not "increased prices or restricted output."[24] While the district court disagreed on that point, another court may agree. Moreover, in assessing the trade-off between privacy and competition, some policymakers may emphasize the cost savings from lower behavioral advertising rates while discounting the harder-to-quantify privacy harms (a topic explored in Chapter 10).

## D. Fourth Trap: Be Wary of What Looks Like Tremendous Gains for Privacy. Except They Aren't.

In January 2020, Google announced that it would phase out third-party cookies.[25] We can already block third-party cookies with Apple's Safari and Mozilla's Firefox web browsers. But Google controls the leading browser, Chrome, whose 64% global market share overshadows Safari (19%) and Firefox (4%).[26] It looks like a tremendous gain for privacy when the leading browser blocks by default a key surveillance technique. Except it isn't.

Likewise, Google requires advertisers who want to buy YouTube inventory to use Google's demand-side platform ("DSP") services. Google justifies its bundling of services as a way to protect our data and privacy.[27] It too looks like a great win for privacy, except it isn't.

When data-opolies promote privacy, policymakers may rejoice, chalking the conversion to public pressure, agency enforcement, or penitence by ethical, enlightened corporate leadership. But it could be a fourth trap, especially when data-opolies profit from behavioral advertising.

We increasingly hear data-opolies using privacy concerns to justify behavior, which coincidentally helps them maintain their dominance. In its 2019–2020 review of the digital advertising sector, the U.K. competition authority, for example, heard "concerns that large platforms use data protection regulations such as the General Data Protection Regulation (GDPR) as a justification for restricting access to valuable data for third parties, while retaining it for use within their ecosystems, thereby consolidating their data advantage and

entrenching their market power."[28]

Privacy could be a legitimate justification for their anticompetitive behavior, but there is likely more to the story. To see why, let us examine Google's recent privacy justifications.

### 1. Google's Bundling YouTube with DSP Services

As we saw, Google is dominant in search, search advertising, and the intermediary display advertising services for publishers and advertisers. In controlling the buy- and sell-side and leading advertising exchange, Google can ensure that a lot of personal data stays within its ecosystem. Very little is leaked to competitors; even the publishers and advertisers using Google's services have limited access to Google's data trove. Likewise, Facebook does not provide advertisers access to the personal data it collects. So to tap into this vast, unparalleled reservoir of personal data, advertisers must use Google's and Facebook's ad management tools.[29] This, alone, presents competition and privacy issues.

As we also saw in Chapter 4, if a company wants to advertise on YouTube, it must use Google's DSP services. Google justifies this anti-competitive tying arrangement as a way to protect our data and privacy.[30] No one, of course, wants their personal data to fall into the hands of malicious actors. But Google is still using our data for behavioral advertising. It is akin to Google telling other privacy violators to scram while it violates our privacy.

Although Google is not materially protecting our privacy, its bundling and lack of interoperability help maintain its dominance in the online display intermediation markets. Moreover, Google could preserve our privacy, the U.K. competition authority observed, with less restrictive alternatives.[31]

### 2. Google's Assault on Third-Party Cookies

The advertising world in 2020 was abuzz about the impending demise of third-party cookies.[32] To see why, let us start with the following premise: putting aside privacy, it would be more efficient and pro-competitive for online behavioral advertisers and publishers, if we were each branded with a unique identifier, along the lines of a Social Security number. With this identifier, publishers would immediately know our identity when we visit their apps or websites. Advertisers would immediately know whom they are targeting. And tracking us would be easier (as would assessing our behavior after seeing the ad). Publishers and

advertisers could rely on multiple exchanges and intermediaries to sell and buy display ads online.

Currently, we are not branded with a universal identifier. But Google has identifiers for many of us. Here is where it gets interesting. Given Google's vastly superior surveillance network (tracking us on 85% of the million most popular websites), Google's personal identifier for each of us is the de facto universal identifier.[33] Returning to our John Doe 123 example, given its extensive surveillance, Google will likely know who is about to visit the woodworking website.

Google shares the information on John Doe 123 with its own intermediaries (its ad exchange and ad-buying tools). But Google does not share the identity of John Doe 123 with others, even the publishers and advertisers using its services.[34] Instead, as the antitrust scholar Dina Srinivasan describes it, for John Doe 123, Google scrambles its identifier, giving the publisher one identifier (ABC789) for John Doe 123 and the advertiser another identifier (XVZ657).[35] Thus, because Google splits the identifier, no one, other than Google, can readily identify that the person about to visit the woodworking website is John Doe 123.[36]

Google says it splits the identifiers for everyone (but itself) to promote our privacy.[37] In a way, Google is preventing greater competition from its surveillance. But Google also profits when publishers and advertisers have different identifiers for the same person: it is harder for publishers to directly negotiate with advertisers or for either of them to use rival intermediaries.[38] On a superficial level, Google promotes privacy (in making it harder for advertisers and publishers to know what websites John Doe 123 visits). But on a fundamental level, privacy is significantly diminished. Because of Google's splitting identifiers, publishers and advertisers are more dependent on Google, thereby enabling one company to establish a vast surveillance network to better predict and manipulate our behavior. So, as the states allege in their monopolization complaint, Google "does not protect users' privacy when doing so harms Google."[39]

A game of cat-and-mouse ensues. Rival ad intermediaries lack access to Google's single identifier. To circumvent Google's restrictions, they use third-party cookies to assign users a proprietary ID, which they then synchronize with the Google-assigned ID. The third-party cookies enable the intermediaries to figure out that the person with the Google identifiers ABC789 (which the

publisher receives) and XVZ657 (which the advertiser receives) are indeed the same, namely John Doe 123.

But cookies are not an ideal workaround to Google's restraint. For one thing, cookie matching is inefficient.[40] It takes time for rival intermediaries to match that the person about to visit the woodworking website is John Doe 123.[41] And time is valuable when these online auctions occur within microseconds (the time the woodworking website is loaded on John Doe 123's computer or phone).[42] So, if the cookie syncing takes too long, the advertisers who use these rival intermediaries miss out on bidding.

Moreover, this cookie matching process is, as the U.K. competition authority noted, "prone to failure."[43] Around a third of the time, the cookies cannot sync.[44] Without knowing that the person is indeed John Doe 123, BMW will not bid (or bid less) when using these rival intermediaries.[45]

So Google, as the Gamemaker, erects a significant roadblock for rival intermediaries and then markets to advertisers and publishers how it is more efficient! In this rigged contest, many advertisers and publishers will seek to avoid the risk and losses from cookie matching, which Google created, and use Google's services.[46] While rival intermediaries are spending precious time trying to match cookies and identify the person, Google uses that time to mine its rich dataset on John Doe 123 to assess which ad to target him.[47] So Google's scrambling of IDs puts rival intermediaries at an informational and speed disadvantage, which puts them (and publishers and advertisers that use them) at a competitive disadvantage.[48]

But rival intermediaries in using third-party cookies can still successfully de-scramble Google's scrambling of identifiers about 70% of the time and identify that the person about to visit the particular website is indeed John Doe 123.

By allowing billions of Chrome browser users to now block third-party cookies, Google can further cripple rival intermediaries. With fewer third-party cookies collecting data on individuals, it will be harder for rival intermediaries to identify from Google's assigned hashtags that the person with the identifiers ABC789 (which the publisher received) and XVZ657 (which the advertiser received) are indeed the same, namely John Doe 123.

But won't blocking third-party cookies harm Google and Facebook as well? Not as much. Recall that both data-opolies directly collect a lot of personal data without the need for third-party cookies.[49] Facebook, for example, benefits even when browsers block third-party cookies, as Facebook has other ways to collect

our data. As the U.K. competition authority found, Facebook "encourages publishers and advertisers to implement its tracking Pixel using first-party cookies instead of third-party cookies, which circumvents browsers blocking third-party cookies."[50] Facebook told the U.K. competition authority that "this was 'to maintain choice for third parties to be able to share data with Facebook, similar data to which may otherwise not be available from browsers blocking third-party cookies.' "[51]

Google will continue to track us when we use Google's many services, such as YouTube, Maps, and its search engine. So many predicted that advertisers will likely switch to those with the most first-party data. Tellingly, 60.4% of data marketers primarily from North America, in a 2020 survey, "expected that they would be increasing spending/emphasis on use of first-party data because of the planned phase-out of third party cookies by browsers developers."[52] Only 37.7 percent said they "expected to increase interest in third-party identity resolution solutions."[53] And that is what happened. Ad buyers and smaller businesses spent more on Google. While Facebook's revenues were basically flat for the third quarter of 2021, Google's revenues increased 41%, its largest percentage gain in 14 years. Its profit for that quarter was $21.03 billion. "In the land of the blind, the one-eyed man is king," said Brian Wieser, GroupM's global president of business intelligence. "Whatever data they have [at Google] is better than what most others have."[54]

Blocking third-party cookies will primarily help Google (and to a lesser extent Facebook) fortify their market power and lock advertisers and publishers, like the woodworking website, into their advertising networks.[55]

But in early 2021, Google went further, announcing that it will no longer track us as individuals across the web.[56] A privacy gain? Yes and no. Google will still surveil us across its many services. When advertisers want to target us individually, they must advertise on the data-opolies' platforms, where Google, Amazon, and Facebook get 100% of the revenue. Moreover, Google will continue to use unique identifiers to surveil us when we use mobile apps. So, "a substantial slice of the digital ad ecosystem wouldn't be affected."[57]

But when we visit third-party websites, like the woodworking one, Google's ad network will place us into clusters of people with similar characteristics. That has some privacy benefits since we are not individually tracked, but it raises other risks. We go from George Orwell's *1984*—where "You had to live—did live, from habit that became instinct—in the assumption that every sound you

made was overheard and, except in darkness, every movement scrutinized"—to Aldous Huxley's *Brave New World*—where individuals fall into major classes named after the first five letters of the Greek alphabet, and then further subdivided within their class. While you may consider yourself part of the intellectually superior Alpha+ group, Google's unsupervised algorithm may instead relegate you to the Beta + group or even Beta -. As a result, you would not receive superior job openings, credit terms, or offers when visiting millions of websites.[58]

Likewise, in 2021, Apple changed its iPhone software so that we can stop third-party tracking for targeted ads. But Apple's privacy move will not prevent data-opolies from tracking us within their ecosystem (like YouTube).[59] Consequently, Facebook's CEO in March 2021 sounded more optimistic, noting that Apple's "move could strengthen his company's own in-app retail channel 'by making it harder for [advertisers] to basically use their data in order to find the customer that would want to use their products outside of [Facebook's] platforms.' "[60] So, while Facebook's quarterly revenues flattened in the third quarter of 2021 ($29 billion), that was significantly higher than its 2020 quarterly revenues (a 35% increase).[61]

The reality is that within the data-opolies' vast ecosystems, neither market forces nor the law protect our privacy. Instead, the data-opolies largely determine when our privacy is protected, when it is not, and from whom. As one Republican congressman told Google's CEO in 2020, "What your company is really doing is using [privacy] as a cudgel to beat down the competition."[62]

It is perfectly rational for data-opolies to use privacy to bludgeon rivals. Policymakers are hearing of other anticompetitive privacy measures.[63] The company Tile, for example, helps people find lost or misplaced items by embedding its finding software into the users' keys, wallet, purse, and other belongings. Its Chief Privacy Officer and General Counsel testified before Congress how "Apple has used the concept of privacy as a shield by making changes in the name of privacy that at the same time give it a competitive advantage."[64]

The data-opolies' privacy justifications can also stifle innovations that will actually promote our privacy. As Ram Shriram, an investor and founding board member of Google, told Congress:

> [p]rivacy does impact how you think about dominance, for example, in a market because Google and Apple both eliminated third-party cookies, which then makes your data a little more private. But it ironically will hurt the young companies that are trying to build digital advertising businesses while improving user privacy.[65]

Our privacy is still harmed when the data-opolies' first-party tracking displaces third-party tracking. As the data-opolies expand their ecosystem to the metaverse, healthcare, driverless cars, wearables, and digital assistants, their formidable first-party data advantage will increase. The more data they collect directly, the less reliant they will be on third-party cookies and trackers, and the more eagerly they will undermine the tracking tools upon which their smaller rivals rely. Indeed, as their algorithms improve in decoding our emotions, weaknesses, and thoughts, they may eventually require less data to predict and manipulate our behavior. So, the data-opolies will likely cede to us more of our data and privacy, but not our autonomy.

Consequently, when a data-opoly proclaims that it does not sell your data, it may not have your interests in mind. Instead, it may be selling something far more damaging to your autonomy and privacy: its algorithms' superior ability through trial and error to predict and manipulate your behavior.[66]

## E. Reflections

In 2020, 10 states challenged, among other things, Google's decision to have its Chrome browser block third-party cookies.[67] The U.K. competition authority is also investigating Google's "new proposals to underpin a healthy, ad-supported web without third-party cookies."[68] One concern is that Google's privacy measure may turn its browser into a critical bottleneck and further entrench Google's dominance for online advertising intermediation services.[69] In 2020, a trade association asked the French competition authority to stop Apple from allowing users to opt out of behavioral advertising.[70]

Consider the remedy in all three cases. Suppose the competition authorities block Google's alternative to individual tracking and tell Google to share its identifier with advertisers and publishers. Suppose Apple cannot ask users whether they want to be tracked for behavioral advertising (even though 85% in one survey prefer not being tracked[71] and most Apple users (84%) have declined being tracked when asked by Apple's privacy prompt[72]).

We may, as a result, be branded, like cattle, with a single universal identifier.

Competition likely would increase significantly:

- Regardless of which intermediary ad service they use, advertisers and publishers could identity us whenever we are online. They could increasingly track our offline behavior (such as monitoring our movements through our phones and the retailers' facial recognition software). No need for cookie synching. No delay in bidding.
- With the universal identifier, publishers and advertisers would be less reliant on Google. Google's dominance over the buy- and sell-side tools and ad exchange, upon which millions of advertisers and publishers currently rely, would diminish.
- The ad tech tax, which currently averages 35% of every advertising dollar spent, would likely shrink.
- As the ad tech tax decreases, publishers, like the woodworking website, would get more of the advertising dollar (say 80 to 90 cents for every advertising dollar, instead of 65 cents currently).
- With more ad revenue, publishers could invest more in their content.
- With a lower ad tech tax, advertisers could pass the savings to consumers with lower retail prices.

But is this the competition we want to promote? Antitrust is not the answer if it fosters a hyper-competitive bazaar based on "mining and monetizing knowledge about what is inside [our] minds."[73]

One can criticize the data-opolies' privacy justifications as pretextual when those same companies repeatedly violate our privacy, threaten and bully publishers into handing over our data,[74] and freely use our data within their walled ecosystems.[75] But if companies are required to incorporate increasingly stringent data minimization policies, they will likely rely on these privacy policies to justify their anticompetitive behavior.[76] Policymakers, however, cannot rely exclusively on the privacy lever. Doing so would chill innovation and reduce overall welfare. Nor can policymakers simply rely on competition when it results in our ruthlessly being tracked, targeted, and manipulated by even more firms.

So, even if policymakers avoid these four traps, they nonetheless will be confronted, at times, with a privacy-competition conflict. As Dante Alighieri described in his first Canto, they will find themselves "within a forest dark, for the straightforward pathway had been lost."[77] While there is no Virgil to follow,

several principles can help them navigate the privacy-competition divide. Let us turn to them next.

---

1 *See, e.g.*, Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772 (Sept. 24, 2019) ¶ 60 ("the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality"); Recital 4 to Regulation (EU) 2016/679, 2016 O.J. (L 119) 1 (EU) ("The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.").

2 United States v. Topco Assocs., Inc., 405 U.S. 596, 610 (1972).

3 *Report of the European Parliament Committee on Civil Liberties, Justice, and Home Affairs on the Digital Services Act and Fundamental Rights Issues Posed*, 2020/2022(INI) (Oct. 1, 2020), https://www.europarl.europa.eu/doceo/document/A-9-2020-0172_EN.html [https://perma.cc/9H74-9BZQ].

4 Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. Econ. Lit. 442, 443 (2016), http://dx.doi.org/10.1257/jel.54.2.442.

5 *Id.* at 449.

6 St. Thomas Aquinas, Aquinas's Shorter Summa: St. Thomas Aquinas's Own Concise Version of his Summa Theologica 353 (2002) ("[T]hat good which man chiefly and mainly desires must be of such a nature that it is not sought for the sake of something else and that it satisfies man. This good is commonly called happiness."); Aristotle, The Ethics of Aristotle: Nicomachean Ethics bk. 1, ch. 7, at 36 (J.A.K. Thompson trans., 1955).

7 *See* Jeremy Bentham, The Principles of Morals and Legislation ch. 13, § 1.1 (1988) (1781) ("[G]eneral object which all laws have, or ought to have, in common, is to augment the total happiness of the community.").

8 OECD, *How's Life? 2020: Measuring Well-Being*, https://www.oecd-ilibrary.org/sites/9870c393-en/index.html?itemId=/content/publication/9870c393-en (last visited Mar. 10, 2021) [https://perma.cc/9AKH-8586].

9 The benefits and potential limits of this approach are explored in Maurice E. Stucke, *Should Competition Policy Promote Happiness?*, 81 Fordham L. Rev. 2575 (2013).

10 State v. Scheetz, 950 P.2d 722, 724 (Mont. 1997) (quoting Montana's constitution); *see also* Welsh v. Roehm, 241 P.2d 816, 819 (Mont. 1952) ("The basis of the 'right of privacy' is the 'right to be let alone' and it is 'a part of the right to liberty and pursuit of happiness.' ") (quoting Barber v. Time, Inc., 59 S.W.2d 291, 294 (Mo. 1942)).

11 Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

12 Directive 95/46/EC, of the European Parliament and of the Council, 1995 O.J. (L 281)

31 (EC), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

13 Yan Carrière-Swallow & Vikram Haksar, *The Economics and Implications of Data: An Integrated Perspective*, International Monetary Fund Policy Paper No. 19/16 (Sept. 2019), https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596, at 20–21 (surveying empirical literature).

14 Yuka Hayashi, *Bad Credit? Regulators Back Ways for Risky Borrowers to Get Loans*, Wall St. J. (Dec. 3, 2019), https://www.wsj.com/articles/bad-credit-alternative-data-wins-support-as-a-way-to-ease-lending-11575420678.

15 *Id.*

16 For a recent example, *see* AnnaMaria Andriotis, *"Flying Blind into a Credit Storm": Widespread Deferrals Mean Banks Can't Tell Who's Creditworthy*, Wall St. J. (June 29, 2020), https://www.wsj.com/articles/flying-blind-into-a-credit-storm-widespread-deferrals-mean-banks-cant-tell-whos-creditworthy-11593423001.

17 Carrière-Swallow & Haksar, *supra* note 13, at 24.

18 *See, e.g.*, Carol S. Steiker, *"How Much Justice Can You Afford?"-A Response to Stuntz*, 67 Geo. Wash. L. Rev. 1290, 1291 (1999) (noting how the poor "simply have less privacy to begin with than the rich, for all the reasons Stuntz relates (the poor have smaller homes or apartments on less land, and share their dwellings with more people; the poor have less privacy at their places of work; the urban poor tend to spend more time on the street or other common areas)").

19 Carrière-Swallow & Haksar, *supra* note 13, at 14.

20 Friedrich August von Hayek, *Nobel Prize Lecture: The Pretence of Knowledge* (Dec. 11, 1974), https://www.nobelprize.org/prizes/economic-sciences/1974/hayek/lecture/ [https://perma.cc/VBJ3-TXMN].

21 Maurice E. Stucke & Allen P. Grunes, Big Data and Competition Policy ch. 7 (2016).

22 Complaint, Federal Trade Commission v. Facebook, No. 1:20-cv-03590-CRC (D.D.C. Dec. 9, 2020), https://www.ftc.gov/system/files/documents/cases/051_2021.01.21_revised_partially_redacte [https://perma.cc/B9VZ-L2B8]; Complaint, New York v. Facebook, No. 1:20-cv-03589-JEB (D.D.C., Dec. 9, 2020), https://ag.ny.gov/sites/default/files/state_of_new_york_et_al._v._facebook_inc._-_filed_public_complaint_12.11.2020.pdf [https://perma.cc/GYC7-44RX].

23 New York v. Facebook, Inc., No. CV 20-3589 (JEB), 2021 WL 2643724, at *8 (D.D.C. June 28, 2021).

24 Facebook, Press Release, Facebook Files Motions to Dismiss Lawsuits Brought by FTC, State Attorneys General, March 10, 2021, https://about.fb.com/news/2021/03/motions-to-dismiss-ftc-state-ag-lawsuits/.

25 AbdelKarim Mardini, *More Intuitive Privacy and Security Controls in Chrome*, The Keyword (May 19, 2020), https://blog.google/products/chrome/more-intuitive-privacy-and-

security-controls-chrome/ [https://perma.cc/DL2C-PS3B]; Gerrit De Vynck & Naomi Nix, *Google Follows Apple in Ending Third-Party "Cookies" in Ad-Tracking*, Bloomberg (Jan. 14, 2020), https://www.bloomberg.com/news/articles/2020-01-14/google-plans-to-move-forward-with-changes-to-ad-tracking-tools [https://perma.cc/SSR5-X6HD].

26 *Browser Market Share Worldwide—February 2021*, StatCounter GlobalStats, https://gs.statcounter.com/browser-market-share (last visited Mar. 10, 2021).

27 Google, *Online Platforms and Digital Advertising Comments on the Market Study Interim Report* ¶¶ 35, 37 (Apr. 8, 2020), https://assets.publishing.service.gov.uk/media/5e8c8290d3bf7f1fb7b91c2c/200212_Google_r [https://perma.cc/5F4G-DEW7] (stating that "restricting third-party access both to our own targeting data and our own inventory (such as YouTube inventory) is the best way to maintain the privacy of user information and prevent it from being leaked to potentially malicious actors" and "[t]hird-party DSPs with access to YouTube inventory could build profiles of users based on their viewing history, which would be a data protection risk").

28 UK Competition & Markets Authority, Online Platforms and Digital Advertising Market Study: Market Study Final Report (July 1, 2020) at ¶¶ 46 & 5.314, https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digit [https://perma.cc/DA5V-RHA5] [hereinafter CMA Final Report] (quoting Digital Competition Expert Panel, Unlocking Digital Competition at ¶ 4.42 (2019) (also known as the Furman Report), https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel [https://perma.cc/VK9M-3GV8]).

29 CMA Final Report at ¶ 5.310.

30 Google, Online Platforms and Digital Advertising Comments on the Market Study Interim Report ¶¶ 35, 37.

31 CMA Final Report at ¶ 5.265.

32 *What the End of Third-Party Cookies Means for Advertisers*, Deloitte Digital, https://www.deloittedigital.com/us/en/blog-list/2020/what-the-end-of-third-party-cookies-means-for-advertisers.html (last visited Mar. 10, 2021) [https://perma.cc/CTH5-CJ54].

33 Dina Srinivasan, *Why Google Dominates Advertising Markets*, 24 Stan. Tech. L. Rev. 55, 90 (2020), https://ssrn.com/abstract=3500919); Complaint ¶ 36, Texas v. Google, No. 4:20-cv-957 (E.D. Tex. Dec. 16, 2020), https://www.texasattorneygeneral.gov/sites/default/files/images/admin/2020/Press/20201216% [https://perma.cc/LTF3-K8XS] [hereinafter Tex. Google Compl.].

34 Srinivasan, *supra* note 33, at 95; Tex. Google Compl. ¶ 125.

35 *Id.* at 96; *see also* Tex. Google Compl. ¶ 125.

36 *Id.* at 96; Tex. Google Compl. ¶ 128 (alleging that "publishers and advertisers could not easily know that two different user IDs actually belonged to the same user, unless they used Google's ad buying tools and exchange"); CMA Final Report at ¶ 5.217.

37 Srinivasan, *supra* note 33, at 96-97; Tex. Google Compl. ¶ 140.

38 Srinivasan, *supra* note 33, at 97–101.

39 Tex. Google Compl. ¶ 140; *see also* CMA Final Report at ¶¶ 5.324–3.325 & 5.329

("our concern is that Google and Facebook have a clear incentive to apply a stricter interpretation of the requirements of data protection regulation when it comes to sharing data with third parties than for the use and sharing of data within their own ecosystems").

40 Srinivasan, *supra* note 33, at 99.

41 *Id.* at 99.

42 *See, e.g.*, Tex. Google Compl. ¶ 56 ("Within this timeframe, which is typically a mere fraction of a second, each ad buying tool must unpack the information contained in the bid request, gather personal information about the user, determine the appropriate price to bid on behalf of an advertiser, and return the bid response to the exchange before time expires.").

43 CMA Final Report at ¶ 5.234; *see also* Srinivasan, *supra* note 33, at 99–100.

44 CMA Final Report at ¶ 5.234 n. 391 ("As cookie IDs are specific to each provider, if the DSP and SSP are operated by different providers a process of cookie matching is required in order for the DSP to identify the relevant consumer information to associate to a given impression. This process is prone to failure and can result in approximately 30% failed matching.").

45 CMA Final Report Appendix M ¶ 128, https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#final-report ("When matching fails, the DSP cannot apply audience targeting or frequency/recency management to the impression, with the result that advertisers cannot understand the real value of the impression and the bids submitted by the DSP will therefore be lower."); Srinivasan, *supra* note 33, at 100.

46 Srinivasan, *supra* note 33, at 101 n. 104.

47 *Id.* at 101; Tex. Google Compl. ¶ 57 (alleging how an "exchange as large as Google's can exclude competition between the bidders in its auction by giving a subset of bidders an information advantage (e.g., more robust information about the user) or a speed advantage (e.g., longer timeouts, which translates to more time to return bids)").

48 Srinivasan, *supra* note 33, at 99; CMA Final Report Appendix M ¶ 430 ("When the DSP and the SSP are operated by the same firm, they use the same user identifier, eliminating the loss of data due to failed cookie matching; in addition, the low level of latency in the communications between the DSP and SSP means that the bid submitted by the DSP will always reach the SSP before the auction closes, unlike with third-party SSPs.").

49 Note by the European Union, Consumer Data Rights & Competition, OECD Doc. DAF/COMP/WD(2020)40 (June 12, 2020) at ¶ 45, https://one.oecd.org/document/DAF/COMP/WD(2020)40/en/pdf [https://perma.cc/Y66C-2UEV] (noting how "[l]arge platforms with many users and diverse product offerings are uniquely placed to gather first-party datasets, rich both in the number of users and the data points available for each user"); CMA Final Report ¶ 5.324 ("targeting using first-party data and authenticated user data does not require cross-site tracking and is unaffected by the demise of third-party cookies. Therefore, large incumbent platforms with leading consumer-facing services like Google and Facebook are significantly less dependent on third-party cookies for delivery of high-performing targeted ads and continued advertising revenues than, for instance, small publishers with free-to-read content that does not require log-in.").

50 CMA Final Report at ¶ 4.136.

51 CMA Final Report at ¶ 4.140.

52 *Effects of Phasing Out Third-Party Cookies on Data Marketing in North America 2020*, Statista (Feb. 10, 2021), https://www.statista.com/statistics/1202652/phase-out-cookies-data-marketing/.

53 *Id.*

54 Tripp Mickle, *Google Profit Nearly Doubles, Boosted by Red- Hot Ad Market*, Wall St. J. (Oct. 26, 2021).

55 Majority Staff of H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial and Administrative Law, Report and Recommendations: Investigation of Competition in Digital Markets at 230 (2020), https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429 [https://perma.cc/29LN-L4BL] [hereinafter House Report] (noting how "market participants are concerned that while Google phases out third-party cookies needed by other digital advertising companies, Google can still rely on data collected throughout its ecosystem"); CMA Final Report at ¶ 5.327 (noting how Google's privacy proposals will "turn Chrome (or Chromium browsers) into the key bottleneck for ad tech. It is likely, therefore, that Google's position at the centre of the ad tech ecosystem will remain. Market participants may be concerned that, under these proposals, Chrome would have the ability to use its position to favour Google's own ad tech intermediation services and raise barriers to entry.") & Appendix M at ¶¶ 544–545; Gerrit De Vynck, *Google's Chrome Becomes Web "Gatekeeper" and Rivals Complain*, Bloomberg (May 28, 2019), https://www.bloomberg.com/news/articles/2019-05-28/google-s-chrome-becomes-web-gatekeeper-and-rivals-complain.

56 David Temkin, Director of Product Management, Ads Privacy and Trust, *Charting a Course Towards a More Privacy-First Web*, Google (Mar. 3, 2021), https://www.communicateonline.me/category/industry-insights/post-details/charting-a-course-towards-a-more-privacy-first-web.

57 Sam Schechner & Keach Hagey, *Google to Stop Ad Sales Based on User Browsing*, Wall St. J. (Mar. 4, 2021).

58 Bennett Cyphers, *Google's FLoC Is a Terrible Idea*, EFF (March 3, 2021), https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea (discussing how Google's FLoC "is designed to help advertisers perform behavioral targeting without third-party cookies. A browser with FLoC enabled would collect information about its user's browsing habits, then use that information to assign its user to a "cohort" or group. Users with similar browsing habits—for some definition of 'similar'—would be grouped into the same cohort. Each user's browser will share a cohort ID, indicating which group they belong to, with websites and advertisers. According to the proposal, at least a few thousand users should belong to each cohort (though that's not a guarantee)").

59 Apple, User Privacy and Data Use, https://developer.apple.com/app-store/user-privacy-and-data-use/ (last visited Mar. 27, 2021) ("you'll be required to ask users for their permission to track them across apps and websites owned by other companies").

60 Patience Haggin & Tim Higgins, *Apple's Move to Block User Tracking Spawns New Digital Ad Strategies*, Wall St. J. (Mar. 26, 2021), https://www.wsj.com/articles/apples-move-to-block-user-tracking-spawns-new-digital-ad-strategies-11616751001?page=1

61 Facebook, Facebook Reports Third Quarter 2021 Results (Oct. 25, 2021), https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Third-Quarter-2021-Results/default.aspx.

62 Gilad Edelman, *The Big Tech Hearing Proved Congress Isn't Messing Around*, Wired (July 29, 2020), https://www.wired.com/story/big-tech-hearing-proved-congress-not-messing-around/ [https://perma.cc/9BL3-JCUR].

63 House Report at 54 (warning that "without adequate safeguards in place, measures that appear to improve privacy for consumers may also have anticompetitive effects"); *see also* CMA Final Report at ¶¶ 5.60, 5.324, & 5.325.

64 House Report at 54; *Hearing on Online Platforms and Market Power Part 5: Competitors in the Digital Economy Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. 70 (Jan. 17, 2020) (Testimony of Kristen Daru, Chief Privacy Officer and General Counsel for Tile, Inc.), https://www.govinfo.gov/content/pkg/CHRG-116hhrg40788/pdf/CHRG-116hhrg40788.pdf.

65 House Report at 54 (internal footnotes omitted).

66 Shoshana Zuboff, The Age of Surveillance Capitalism 76 (2019).

67 Tex. Google Compl. ¶¶ 228 (alleging that "Google's decision to phase out third-party cookies on Chrome only increases the information asymmetries, leaving publishers with fewer alternatives other than Google's user data. Because access to user data is only available on the [redacted] or through Google intermediaries, Google's decision to shut down third-party cookies on Chrome increases the information asymmetries between its exchange and other exchanges such as those in header bidding.") & 229 (alleging how "[redacted but presumably Google's Chrome proposal] will go further and charge even higher prices for the sale of personal user information in order to create a giant walled garden and increase its profit margins and eliminate competition").

68 S. Dent, *The UK Will Probe Google's Plan to Eliminate Third-Party Cookies in Chrome*, Engadget (Jan. 8, 2021), https://www.engadget.com/uk-regulators-google-chrome-privacy-sandbox-third-party-cookies-114953394.html [https://perma.cc/ZU3M-DFLS]; *see also* Press Release, U.K. Competition and Markets Authority, CMA to Investigate Google's 'Privacy Sandbox' Browser Changes (Jan. 8, 2021), https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes; Sam Schechner, *Google Chrome Privacy Plan Faces U.K. Competition Probe*, Wall St. J. (Jan. 8, 2021), https://www.wsj.com/articles/google-chrome-privacy-plan-faces-u-k-competition-probe-11610119589.

69 CMA Final Report ¶ 5.327:

> We note that, if successfully implemented, Google's main Privacy Sandbox proposals . . . may still permit some third-party personalised advertising (interest-based advertising and remarketing), albeit at a greater level of coarseness of targeting and measurement. However, those proposals will also turn Chrome (or Chromium browsers) into the key bottleneck for ad tech. It is likely, therefore, that Google's position at the centre of the ad tech ecosystem will remain. Market participants may be concerned that, under these proposals, Chrome would have the ability to use its position to favour Google's own ad tech intermediation services and raise barriers to entry.

70 Keach Hagey & Patience Haggin, *Apple Faces Antitrust Complaint in France Over Privacy Changes in iPhones*, Dow Jones (Oct. 28, 2020), https://www.morningstar.com/news/dow-jones/202010289706/apple-faces-antitrust-complaint-in-france-over-privacy-changes-in-iphones [https://perma.cc/7W9T-N3CV]. The French competition agency did not find Apple's conduct by itself an abuse of dominance, but noted in March 2021 that it was investigating whether Apple was self-preferencing by imposing stricter privacy rules on third-party apps than its own. L'Autorité de la concurrence, *Press release: Targeted advertising Apple's implementation of the ATT framework. The Autorité does not issue urgent interim measures against Apple but continues to investigate into the merits of the case* (Mar. 17, 2021), https://www.autoritedelaconcurrence.fr/en/press-release/targeted-advertising-apples-implementation-att-framework-autorite-does-not-issue; Sam Schechner, *Apple Notches a Legal Win in France Over App Privacy*, Wall St. J. (Mar. 18, 2021).

71 Hagey & Haggin, *supra* note 68.

72 Patience Haggin & Suzanne Vranica, *Apple's Privacy Change Is Hitting Tech and E-Commerce Companies. Here's Why*, Wall St. J. (Oct. 22, 2021), https://www.wsj.com/articles/apples-privacy-change-is-hitting-tech-and-e-commerce-companies-11634901357.

73 Complaint ¶ 6, Colorado v. Google, No. 1:20-cv-03715-APM (D.D.C. Dec. 17, 2020), https://coag.gov/app/uploads/2020/12/Colorado-et-al.-v.-Google-PUBLIC-REDACTED-Complaint.pdf.

74 Paresh Dave, *Google Stymies Media Companies from Chipping Away at Its Data Dominance*, Reuters (June 30, 2020), https://www.reuters.com/article/us-tech-antitrust-google-focus/google-stymies-media-companies-from-chipping-away-at-its-data-dominance-idUSKBN24110K. [https://perma.cc/H73F-9GXY]

75 UK Competition & Markets Authority, Online Platforms and Digital Advertising Market Study: Market Study Final Report ¶ 5.320 (July 1, 2020), https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digit [https://perma.cc/DA5V-RHA5] [hereinafter CMA Final Report].

76 Srinivasan, *supra* note 33, at 55, 106, n. 115 (noting that Google used the California Consumer Privacy Act to not permit non-Google exchanges and buying tools to bid for publishers' ad space).

77 Dante Alighieri, The Inferno, canto I, http://www.online-literature.com/dante/inferno/1/ [https://perma.cc/9LBS-QEYS].

# 9

# A Way Forward

## Developing a Post-millennial Antitrust/Privacy/Consumer Protection Framework

When privacy policies hamper competition or when competition policies degrade privacy, what should policymakers do, besides avoiding the four traps?

First, they must recalibrate their privacy, consumer protection, and competition policies. The current laws have failed to do the job. Even if the competition authorities successfully prosecute Google, Apple, Facebook, and Amazon, the fundamental misalignment of incentives remains. Even if every data-opoly is dismantled, the unhealthy competition from behavioral advertising will continue. Given the economies of scale, network effects, and incentives to hoard data and attention, market forces, under the current legal framework, will only beget new data-opolies.

Second, as we saw with Facebook's and Google's attack on Australia, no jurisdiction can unilaterally address the risks posed by data-opolies. Policymakers must coordinate to align the competition, consumer protection, and privacy laws.

Third, in recalibrating their policies, policymakers must ensure that the ensuing competition actually benefits us. Toxic competition is not inevitable. It is shaped by the legal framework and formal and informal norms. So why leave the quasi-regulatory state to the data-opolies? The democratically entrusted policymakers should redesign the rules to ensure that the ensuing competition serves us, rather than our serving it, and the competition brings out the best in rivals, not their worst. The surveillance economy flunks both criteria.

Fourth, in recalibrating the privacy, consumer protection, and competition policies, policymakers must ensure that we will have greater control over our personal data, privacy, and autonomy. The law must secure, as Justice Brandeis recognized, the "right to be let alone-the most comprehensive of rights and the right most valued by civilized men."[1]

Once the consumer protection, privacy, and data protection policies are properly aligned, we can make more informed choices about how our data is

processed.[2] We will have greater trust in online markets.[3] Once legal guardrails are in place and incentives are aligned, privacy can become a critical non-price component of competition. When companies compete in promoting (rather than degrading) privacy, there will be greater incentives and opportunities to offer technologies and alternative business models that protect our privacy while unleashing the potential value from non-rivalrous data.[4]

To get there, policymakers must fix the competition and consumer protection levers.

## A. Fixing the Competition and Consumer Protection Levers

To deter many of the data-opolies' abuses, policymakers can start with the proposals outlined in Chapter 3. Making it harder for data-opolies to acquire or kill nascent competitive threats will promote disruptive innovation and competition, as will preventing the data-opolies from both operating the platform and competing on it. But in the many online markets dependent on behavioral advertising, toxic competition will remain. These proposals do not address the misalignment of incentives, where companies compete to degrade rather than promote our privacy. Governments cannot simply order companies to promote our privacy interests. Nor will command-and-control regulations successfully stimulate privacy innovations. For that, we rely on competition, which policymakers must ensure is healthy rather than toxic. The competition will remain toxic when companies cannot afford to opt out unilaterally, or will profit more in exploiting our weaknesses than helping us address them. Thus, to align the data collectors' and individuals' interests more closely, at least two things must be done.

First, guardrails are needed to prevent abusive practices. In a first for any statute, the California Privacy Rights Act of 2020 states that any agreement "obtained through the use of dark patterns does not constitute consent."[5] As we saw, data-opolies use default settings and dark patterns to give us the illusion of control while making it harder for us to protect our privacy. "There appears to be a substantial market failure where dark patterns are concerned—what is good for ecommerce profits is bad for consumers."[6] Thus, through legislation and enforcement, the government has a responsibility to prevent exploitative practices, like dark patterns, used to manipulate our consent and behavior.[7]

But a more effective way to prevent exploitative, deceptive, and unfair competition methods is to eliminate the economic incentive and benefits in

engaging in this behavior. Consider Facebook. The FTC first sued Facebook in 2011 for its deceptive privacy settings and statements.[8] The dominant social network made many promises to its users that it failed to keep, including the following:

- representing that third-party apps would have access only to the Facebook user information that they needed to operate, when in fact, "the apps could access nearly all of users' personal data—data the apps didn't need";
- telling "users they could restrict sharing of data to limited audiences—for example with 'Friends Only,' " when in fact, "selecting 'Friends Only' did not prevent their information from being shared with third-party applications their friends used";
- claiming it certified the security of participating apps under its "Verified Apps" program when it didn't; and
- promising users that "it would not share their personal information with advertisers" when it did.[9]

Facebook settled, obligating itself to live up to its privacy promises to its users.[10] But Facebook soon thereafter broke its promise. Facebook, the FTC found, continued to subvert "users' privacy choices to serve its own business interests."[11] It continued to deceive users by sharing their and their friends' information with app developers. So when 305,000 Facebook users installed the app "This Is Your Digital Life," Facebook handed over not only their data but also sensitive personal data of these Facebook users' 87 million friends. The app then funneled this data to Cambridge Analytica, which mined it to persuade many Americans to vote for Donald Trump (and millions of others not to vote) in the 2016 elections.[12] Facebook not only violated the 2011 consent decree, but it lied about new things.[13] For example, Facebook asked users for their telephone numbers ostensibly for a two-factor authentication security feature to secure their accounts. But without telling consumers, Facebook used their telephone numbers for advertising purposes. In 2019, in a 3-2 decision, the FTC imposed a record $5 billion penalty, added new obligations on Facebook, and devised a new governance structure for the company. So, what happened to its stock? As the company's co-founder observed, "the day after the company predicted in an earnings call that it would need to pay up to $5 billion as a penalty for its negligence—a slap on the wrist—Facebook's shares surged 7 percent, adding $30 billion to its value, six times the size of the fine."[14]

Facebook's repeated privacy violations are revealing in several ways.

*First*, it illustrates the shortcomings of the enforcement under Section 5 of the FTC Act in protecting our privacy. While the FTC ordered Facebook in 2011 to establish and maintain a "comprehensive privacy program" designed to protect privacy and personal information,[15] the opposite happened. Facebook repeatedly violated the FTC order and used personal data as currency with third-party apps to increase its profits and power. In determining whether to continue granting a particular app developer access to Facebook users' personal data, the data-opoly

> considered how large a financial benefit the developer would provide to Facebook, such as through spending money on advertisements or offering reciprocal data-sharing arrangements.
>
> At one point in 2013, for instance, Facebook considered whether to maintain or remove data permissions for third-party developers based on whether the developer spent at least $250,000 in mobile advertising with Facebook.[16]

So neither privacy law nor the risk of being in contempt of an FTC order deterred Facebook.

*Second*, the risk of antitrust enforcement did not deter Facebook either. This is not surprising. Before the Google and Facebook monopolization cases in 2020, the United States rarely brought monopolization cases. Its last significant prosecution was in the 1990s against Microsoft.[17] Moreover, the FTC neglected its intended role "to continuously monitor business practices" and bring cases under its stand-alone authority under section 5 of the FTC Act.[18] Instead of targeting monopolies, the FTC and DOJ "targeted their enforcement efforts on relatively small players—including ice skating teachers and organists—raising questions about their enforcement priorities."[19]

A *third*, perhaps more glaring, problem is the FTC's response to the data-opoly's recidivism. The Cambridge Analytica scandal exposed how Facebook was sharing vast amounts of personal data with third parties without the users' and their friends' consent, and contrary to its requirements under the FTC order. Confronted with a repeat privacy offender, the FTC in 2019 could have reined in the data-opoly, simply by asking *why* it continued to violate users' privacy. But a majority of Commissioners didn't.

All five FTC commissioners recognized that personal data was a crucial source of Facebook's power. It was undisputed that Facebook's incentive was to continue to amass personal data to target users with behavioral ads. Given

Facebook's continued dominance, its incentives under its behavioral advertising-dependent business model, and users' inability to switch to viable alternatives, the FTC could have required, as Germany's antitrust agency did in its prosecution of Facebook,[20] substantive privacy remedies.

Tellingly, the FTC did not. The 2019 consent decree permitted Facebook to continue to harvest personal data for behavioral advertising. Nor did the FTC limit (i) what data Facebook could share with third parties; (ii) the extent to which Facebook could combine user data internally from what it collected from Instagram, Facebook, and WhatsApp; and (iii) the data Facebook could collect from users and nonusers when they were not even on Facebook.

The settlement failed to address the underlying cause of Facebook's exploitative behavior, namely, its behavioral advertising-dependent business model. This failure, for the two dissenting FTC commissioners, was a deal-breaker. Commissioner Rebecca Kelly Slaughter could not "view the order as adequately deterrent without both meaningful limitations on how Facebook collects, uses, and shares data and public transparency regarding Facebook's data use and order compliance."[21] As Commissioner Rohit Chopra noted, "Facebook's violations were a direct result of the company's behavioral advertising business model," and the FTC's settlement did "little to change [Facebook's] business model or practices that led to the recidivism."[22] But for three FTC commissioners, any substantive data and privacy protections were beyond the agency's power: "Our 100-year-old statute does not give us free rein to impose these restrictions."[23]

So, to meaningfully change behavior, policymakers must change incentives. Courts have long sought to align incentives when a fiduciary duty is owed. As one state supreme court observed in 1855:

> It is one of the canons of a court of equity that one who undertakes to act for others cannot in the same matter act for himself. Where confidence is reposed, duties and obligations arise which equity will enforce. A trustee . . . will not be allowed to mix up his own interests and affairs with those of the beneficiary. This doctrine has its foundation not so much in the commission of actual fraud, but in that profound knowledge of the human heart, which dictated that hallowed petition, "lead us not into temptation, but deliver us from evil," and that caused the announcement of the infallible truth, that "a man cannot serve two masters."
>
> The right to sell and to buy cannot exist in the same person, because of the antagonistic interest in the two positions.[24]

Equitable remedies, such as the doctrine of constructive trusts, are illustrative.[25] Their purpose is to close the door to the agent's temptation to fraud and keep the agent's eye single to the principal's rights and welfare.

Since behavioral advertising distorts the market participants' incentives, pitting the data collector's interests against our interests, the law must close the door to this temptation of those who receive our confidential, sensitive information. For that, we next turn to the privacy lever.

## B. Fixing the Privacy Lever

Privacy law can end the toxic competition where many companies currently outcompete one other to degrade our privacy and channel the competition toward finding ways to promote our privacy. Figure 9.1 identifies a spectrum of privacy policies proposed as of 2021 to target a vital source of the data-opoly's power while securing many of the benefits of data's non-rivalrous nature.


**Figure 9.1** Spectrum of Privacy Policies to Curb the Surveillance Economy

Let us examine each policy's benefits and shortcomings.

### 1. Stronger Guidelines

At the least restrictive end of the spectrum is stronger guidelines. The European Data Protection Board, for example, drafted guidelines to clarify when the collection and processing of personal data are objectively necessary for the performance of a contract. "As a general rule, processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services."[26] Returning to our example of Google Maps, Google could not justify its using our geolocation data for behavioral advertising purposes as necessary "simply because such advertising indirectly funds the provision of the service."[27] More robust guidelines can curtail some of the data-opoly's discretion under the GDPR.

But control over our data and privacy will depend on the guidelines' efficaciousness. The privacy agencies would still confront the "whack-a-mole" problem, where the data-opoly relies on other bases for collecting the data (such

as consent under Article 6(1)(a) of the GDPR). The resource-constrained privacy agencies must still monitor the firms to ensure that they are heeding the guidelines.

Moreover, guidelines alone will not curb surveillance capitalism, as they do not change incentives. So guidelines alone will not provide us with greater control over our data, privacy, and autonomy.

## 2. Stronger Disclosure Requirements

The European Commission is seeking to supplement the GDPR with additional disclosure requirements for powerful gatekeepers, including the extent to which they are profiling users. As the Digital Markets Act proposes,

> Ensuring an adequate level of transparency of profiling practices employed by gatekeepers facilitates contestability of core platform services, by putting external pressure on gatekeepers to prevent making deep consumer profiling the industry standard, given that potential entrants or start-up providers cannot access data to the same extent and depth, and at a similar scale. Enhanced transparency should allow other providers of core platform services to differentiate themselves better through the use of superior privacy guaranteeing facilities.[28]

The Commission's Digital Services Act would also increase transparency in online advertising.[29] "[V]ery large online platforms" that display ads would have to disclose additional information,[30] and the Commission would help facilitate industry codes of conduct.[31]

As we saw in chapter 5, data-opolies face little competitive pressure to change their opaque privacy policies, where they fail to specify what data they collect and how they exactly use the data.[32]

About 74% of Facebook users in 2019 did not know that Facebook categorized them in specific groups, including their political and multicultural affinities, for advertising purposes.[33] In increasing transparency, Europe's Digital Services Act and Digital Markets Act might let more Europeans know that the ads they see result from profiling.

But even if data-opolies disclose more information, so what? Increased transparency and reputational effects work where privacy competition is already robust. They will not work in markets dominated by data-opolies or where the prevailing business model relies on behavioral advertising. For example, seeing how the social network profiled and categorized them, 58% of Facebook users

were “not comfortable with Facebook compiling this information.”[34] Twenty-seven percent felt that Facebook’s categorization of them did not accurately represent them.[35] But what recourse do they have? The current notice-and-consent regime is meaningless when no viable competitive alternatives exist, and the bargaining power is so unequal.[36] Facebook gives us the choice of “either accepting the ‘whole package’ or doing without the service.”[37] Unless our friends and relatives all switch to another social network, none of us individually can feasibly switch without sacrificing the ability to interact with our family and friends, a core function of any social network. The same is true in every digital market with strong network effects.

Even with greater transparency, one cannot assume that individuals effectively consent to this surveillance and manipulation. It is simply exploitative. Even with greater transparency, the surveillance economy would likely continue. Many publishers cannot afford to unilaterally switch to contextual advertising when their rivals stick with behavioral advertising. So, even with greater transparency, few websites and apps can unilaterally opt out of this arms race.

Indeed, greater transparency, paradoxically, could hurt us. In one 2019 lawsuit, Facebook argued that its users did not expect privacy.[38] Suppose people use social media to communicate sensitive information with a few friends. According to Facebook, they have no right to complain of a privacy violation if the social media company turns around and shares that information with a virtually unlimited audience. The district court rejected this argument.

But the court left open whether users consented to the transfer of data to third parties, like Cambridge Analytica. If users agreed, in fine print, to the data-opoly disseminating their sensitive information, they were not injured in a legal sense.

Whether users consented to the alleged conduct is an issue of contract interpretation governed by state law. In the *Facebook* case, California law, the court acknowledged, requires it “to pretend that users actually read Facebook’s contractual language before clicking their acceptance, even though we all know virtually none of them did.”[39] Even though Facebook uses defaults and dark patterns to nudge consent, nonetheless under California law, “the contract language must be assessed objectively, from the perspective of a reasonable Facebook user.”[40]

So, greater transparency can insulate firms from privacy claims in the United States. Even when individuals lack viable privacy-friendly alternatives, the

courts must "assume as a legal matter (even if it's not true as a factual matter) that users reviewed, understood, and agreed to all of [the firm's] contractual terms when they signed up for their accounts."[41] Consequently, reliance on greater transparency and reputational effects will not check data-opolies[42] or the surveillance economy.

## 3. Limited Opt-Out

As the California Privacy Rights Act of 2020 (CPRA) recognizes, some advertising-supported business models can be "non-invasive" and "pro-privacy." So the law targets the behavioral advertising model.[43] To give Californians greater control over their data and effectuate the law's data minimization principles, the CPRA provides Californians a right to opt out of having their "sensitive personal data" used for behavioral advertising.[44]

Californians can also opt out of having their data being sold or shared with others, including "for cross-context behavioral advertising."[45]

The CPRA is a substantial improvement over the 2018 law's "hoard but regulate" approach. Californians can prevent Facebook from sharing their personal data with others and others sharing their data with the social network. Moreover, Californians can limit data-opolies and any other company from using their "sensitive personal data" for behavioral advertising.

The law, however, will not meaningfully deter the toxic competition promoted by behavioral advertising and prevent data-hoarding and surveillance.

First, the law allows customers to opt out of cross-context behavioral advertising.[46] But data-opolies can collect and use first-party data (except "sensitive personal information") for behavioral advertising. For example, Facebook could continue to surveil users on its social network, collect data about them, and use that data to target them with behavioral ads and manipulate their behavior.

Second, the statute's opt-out provision for behavioral advertising for first-party data applies only to "sensitive personal information," which is narrowly defined as:

(l) personal information that reveals
  (A) a consumer's social security, driver's license, state identification card, or passport number;
  (B) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
  (C) a consumer's precise geolocation;
  (D) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
  (E) the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication;
  (F) a consumer's genetic data; and
(2) the processing of biometric information for the purpose of uniquely identifying a
(A) consumer;
  (B) personal information collected and analyzed concerning a consumer's health; or
  (C) personal information collected and analyzed concerning a consumer's sex life or sexual orientation.[47]

While that is a good start, data-opolies can continue to harvest a lot of personal data across their many services that fall outside this definition. When you "Like" something, that, by itself, does not reveal any "sensitive personal information" under the statute. But as we saw, with enough seemingly benign "Likes," one could learn revealing insights about a Facebook user, including sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. So, even under the CPRA, data-opolies can continue to draw inferences from the vast amount and variety of information they collect about our preferences, characteristics, psychological traits and predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. Even for sensitive personal information, if it is "publicly available," as defined under the statute,[48] then data-opolies can use it for behavioral advertising or any other purpose.

Third, the California privacy statute can paradoxically increase the data-opolies' power. Even when Californians opt out of their data being sold to or shared with third parties, the data-opoly can continue to collect first-party data when we're in their expanding ecosystems. So, the law's opt-out provision primarily hinders smaller rivals from pooling personal data to better compete against the data-opolies. With their significant first-party data advantage, Google and Facebook already capture most digital advertising revenues, with Amazon a

distant third. Suppose other jurisdictions adopt the CPRA's approach. In that case, these three companies, which already dominate multiple markets, will have an even greater incentive to expand their ecosystem to collect more first-party personal data. So, the privacy law can help data-opolies dominate the behavioral advertising ecosystem for years.

Fourth, the CPRA contemplates some limits on profiling. But it does not prevent data-opolies from aggregating data (other than sensitive personal data) across their many different services and leveraging that data to maintain or extend their monopoly.[49] For example, if the Californian resident opts out, Google cannot use her geolocation data for behavioral advertising. But Google could use her geolocation data to improve a variety of its services, including helping its search engine develop "location-related search features."[50] So, Google could use its data advantage (such as in tracking users' movements) to maintain its dominance for search and other services. In dominating search, Google will dominate search advertising, where it can target users with behavioral ads.

Finally, the law has a gaping exception. With any opt-out (or opt-in) regime, the company might retaliate against individuals who exercise their legal rights. To prevent this retaliation, the law must include a strict non-discrimination/non-retaliation provision. On the plus side, the CPRA prohibits the use of dark patterns to obtain consent. The statute also prevents any company from discriminating against any individual who opts out of having their data shared with third parties or limits the use of their sensitive personal information.[51] So far so good. But the law then allows these data-opolies to employ other means to pressure individuals to not opt for the statute's privacy protections. A data-opoly (or any other firm), under the CPRA, can charge "a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data."[52]

That presents a significant loophole for the data-opoly. The state would have an impossible task in proving the value provided to the business by the consumer's data. As we saw in Chapter 5 and as the CPRA itself recognizes,[53] individuals do not know how much their data is worth. But even if there were a market price for the consumer data, what is determinative is the value the data provides to the particular business. This information is mainly within the data-collector's control and discretion. Individuals certainly will not know how much value their data provides to the business. Only the company would know this.

Suppose the company degrades the quality of services for those who opt out. The state enforcement agency, under the law, must quantify the difference in quality, a difficult task, and prove that amount exceeds the data's value to the business, an even harder task. Basically, the agency would have to show the financial incentives "are unjust, unreasonable, coercive, or usurious in nature."[54] Once one factors in information asymmetry and data-opolies' superior bargaining power, consumers will likely be cheated. The law provides broad latitude to the data-opoly to offer incentives that can be so attractive that they effectively punish users who opt out.[55]

So, even without "dark patterns," the data-opolies can turn to other weapons in their behavioral economics armory to dissuade Californians against opting out. Under behavioral economics' Prospect Theory, losses closer to a reference point hurt more than the joy from comparable gains.[56] Data-opolies will likely use Prospect Theory to their advantage. They will emphasize upfront the cost of opting for privacy. Many people will probably weigh the immediate loss far more heavily than the harder-to-quantify, long-term benefits in not having their data used for behavioral advertising.

Of course, things can change. The new state privacy agency and California Attorney General, for example, can update and add new categories of personal and sensitive personal information through regulations.[57] A broader definition of sensitive personal information can dampen the toxic competition and data-opolies' power. But there are more straightforward, effective policy alternatives to regain our privacy and autonomy and curb surveillance capitalism.

So the permitted use under [2][ii] [Section 1798.140(e)(4)] envisions only "non-personalized advertising," which is defined as "advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business, with the exception of the consumer's precise geolocation." CPRA § 1798.140(t). Thus, one question is whether [2] adds to or qualifies [1]. Could Facebook, for example, argue that behavioral advertising qualifies under [1] as it is necessary to perform its free services and is reasonably expected by the average user? That interpretation would effectively defeat the careful limitations of [2] for sensitive personal information and curtail the statute's objective of giving consumers control over limiting the use of their sensitive personal information whenever the service is free. CPRA § 3(A)(2).

## 4. Opt-Out

Next along the spectrum are policies that enable individuals to opt out of being tracked for behavioral advertising purposes and having their data aggregated.

Under one proposal, if we opt out of being tracked, the company can collect and process our personal data only if it is "necessary for the operation of the website, service, or application."[58] But the proposed legislation explicitly excludes "behavioral advertising" from qualifying as "necessary."[59] First- and third parties (such as data brokers and ad networks like Google's and Facebook's) can collect data only to analyze how or whether we engaged with the product or service (and the data has to be de-identified and cannot be used to develop a user profile). Moreover, companies cannot retaliate if individuals opt out of being tracked. Google or Facebook, for example, could not deny access to, or service from, their websites, services, or applications. Nor could they provide those who opt out with worse service or access.

The "full opt-out" approach incorporates the California Privacy Rights Act's benefits and enables individuals to prevent firms from using their personal data for behavioral advertising and profiling. This approach operationalizes the data minimization principles by expressly stating that behavioral advertising is not a necessary purpose and preventing data-opolies from coercing consent.

One weakness, relative to the hybrid and opt-in approaches, is the default option, that is, requiring users to opt out of behavioral advertising and profiling.[60] As we saw, some data-opolies are already designing privacy *out* of their policies through dark patterns and default options. As the behavioral economics literature and everyday experience show, the default setting can affect the outcome—even when transaction costs are nominal. Many people stick with the default option.[61] While the U.K. competition authority expected defaults to influence behavior, the agency was surprised how strong an effect defaults had in the digital economy:

> . . . default behaviour by consumers has had a profound impact on the shape of competition in both search and social media. First, defaults play a very important role in influencing consumers' use of search engines, and second, default settings and the way in which choices are presented to consumers have a strong influence on the ability of platforms – particularly social media platforms – to collect data about their users, and the ability of users in turn to control the use of their data.[62]

To exploit our status quo bias, Google, as we saw, spends billions of dollars annually to be the default search engine on Apple devices.[63]

Moreover, because relatively few people opt out, the decision to do so can raise its own privacy concerns. “For example, an individual’s decision to opt out may—often unintentionally—be reflected in a data release or analysis and invite scrutiny into whether the choice to opt out was motivated by the need to hide compromising information.”[64]

Thus, one major issue will be over the default: Should individuals have to opt out of behavioral advertising, profiling, and combining data to create profiles about them, or should they have to opt into the surveillance?[65] Data-opolies would prefer the former. It gives individuals the illusion of control, even though many will stick with the default, especially if they have to navigate the data-opoly’s website through multiple clicks to opt out. Why then require individuals to opt into privacy when, as we will see next, that is what most of us prefer?

## 5. Hybrid Approach

Under a hybrid approach, the default setting (opt-out or opt-in) depends on the collector’s market power.

To address Google’s and Facebook’s dominance of the online advertising market, the U.K. Competition and Markets Authority (CMA) considered multiple remedies, including a code of conduct. One operating principle was that powerful platforms (that is, those with “strategic market status”) could not collect more data than necessary.[66] To give U.K. residents greater control over their data, the CMA proposed an opt-out for platforms without significant market power. They must provide consumers an option to use their services without requiring consumer data for personalized ads.[67] So, the default is to allow surveillance and behavioral advertising. But for powerful platforms, U.K. residents must choose whether they want to be tracked or not and whether they want their data collected for personalized advertising purposes.[68] Residents could easily change options down the road. As the CMA found, most U.K. residents had a clear preference for privacy as the default. Individuals would have to opt-in, rather than opt-out, for personal data collected for behavioral advertising.[69] While consumers initially preferred more relevant ads (which is the data-opolies’ justification for behavioral advertising), their minds changed once they understood how targeted advertising works.[70] While Facebook disagreed with the CMA’s findings, it could offer *no* evidence that contradicted the surveys and other evidence on which the CMA relied.[71] Indeed, as we saw in the last chapter, most Apple users (84%) declined to be tracked when asked by Apple’s privacy

prompt.

Nevertheless, the CMA's hybrid approach has several infirmities. First, the government must determine who is or isn't a monopoly, and the defaults can change over time—decisions that can embroil the agency in litigation for years.

Second, opt-in/opt-out can be confusing. Individuals might assume that because data-opolies cannot track them for behavioral advertising purposes, other firms cannot as well.

Third, as we saw in Chapter 4, behavioral advertising promotes toxic competition, with or without data-opolies. So, firms without monopoly power would still compete to addict us, extract our data, and predict which behavioral ads will most effectively achieve the desired behavior.

Fourth, data-opolies would likely adjust. They could depend on consumers sticking with the default option, which would mean that the firms without monopoly power would still collect data for behavioral advertising purposes and funnel that data to the data-opolies.

Finally, data-opolies, in being able to offer incentives to engage in behavioral ads, can resort to their behavioral economics arsenal to find ways to nudge individuals to consent.[72]

Another hybrid approach is the Bundeskartellamt's proposed antitrust remedy against Facebook. German residents can use Facebook without being tracked when they visit third-party websites or apps.[73] Their data from Instagram, Facebook, and WhatsApp cannot be combined without their consent. The competition agency determined that the data-opoly's processing of this third-party data and combining the data internally were not objectively necessary to provide its social network services.[74]

Nevertheless, in some ways, Germany's proposed remedy is more permissive. Facebook can continue to track users while on the social network and collect first-party data for behavioral advertising purposes. Facebook can continue to treat personal data as currency in exchanging it with other websites and apps. Thus, Germany's hybrid approach does not significantly curb Facebook's perverse incentives under its behavioral-advertising revenue model, and the data-opoly's abuses will likely continue.

### 6. Opt-In

Most of us want greater control over our privacy and autonomy and dislike the surveillance and manipulation underlying behavioral advertising. So, the next

policy option sets privacy as the default. Unless we freely and knowingly opt for behavioral advertising and personal profiles, no firm can collect or use our personal data for behavioral advertising or profile us by aggregating the data collected about us across the firm's different services and from third parties.[75]

The opt-in policy would include other privacy protections, such as a strict non-discrimination provision and prohibition of abusive practices, like dark patterns, to nudge our consent. If we stick with the privacy-friendly default, we could continue watching a YouTube video, for example, without any degradation in service. Nor would those who opt for behavioral advertising receive any discounts or other additional benefits.

Among the opt-in approach's benefits is its operationalizing the privacy-by-design features with minimal hassle for individuals. Firms could only collect and use data that they need to provide the specific service. Individuals have greater control in choosing whether they want behavioral ads and personalized services.

One potential risk of the "opt-in" approach is continued behavioral advertising. Many Americans have signed the FTC's Do Not Call List (241.5 million telephone numbers by 2020[76]). While the program is touted as one of the FTC's successes, many Americans still get many spam calls. The FTC received nearly four million complaints about spam calls in 2020.[77] So, if we get an unwanted call, it could be an illegal robocall. Yet, even if we opt out of telemarketing calls, we can still get, under the FTC rules, "political calls, charitable calls, debt collection calls, purely informational calls, and surveys."[78] The unwanted call might be from some firm that we permitted, in fine print in some clickwrap, to call us. Or it could be from a firm with whom we recently did business.

Telemarketers make a pittance compared to Google and Facebook, whose $200+ billion in revenues from behavioral advertising in 2019 exceeded most countries' GDP. Even with a privacy-friendly default, strong prohibitions against the use of dark patterns, and strong non-discrimination protections, the profits from behavioral advertising are too alluring to allow us to stick with the default. Consequently, companies would multiply their efforts to acquire our consent or argue that their use of our data did not fall within the statutory definition of behavioral advertising.

Finally, even with an opt-in approach, some people will opt for behavioral advertising—whether for the belief that it will yield more relevant ads or some other perceived benefit. These users will be surveilled, profiled, and categorized

into specific groups (such as shopaholics) based on, among other things, their lifestyle, interests, motivators, and personality. In mining publicly available information, data-opolies can make inferences about the rest of us based on our age, residence, occupation, gender, political contributions, and other public data. The data-opoly might pair us with a "lookalike audience"[79] of those who opted for behavioral advertising based on common qualities (for example, similar demographics or interests). Or we might be placed in similar advertising groups (such as shopaholics). So behavioral advertising will continue, but there might be even more significant risks that privacy-sensitive users will be placed in the wrong group.

## 7. Banning Surveillance

One concern is that unless behavioral advertising and profiling are banned altogether, the temptation will remain given the profit opportunity. So the last option targets surveillance capitalism itself, by democratically deciding to (i) prohibit the collection and use of personal data for behavioral advertising, which the European Parliament urged in October 2020;[80] (ii) limit firms from combining data about us to profile us (except as otherwise allowed with adequate safeguards, such as credit reports under the Fair Credit Reporting Act); and (iii) enable us to decide, without penalty, the right to limit at the onset what data is collected about us and for what non-advertising purpose.

One issue is defining behavioral advertising. A good start is the California Privacy Rights Act of 2020, which defines cross-context behavioral advertising as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, *other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.*"[81] One danger under this definition is the data-opolies' mining data directly from their own apps and websites. So policymakers could modify the definition to the following:

> the targeting of advertising to an individual based in whole or in part on the individual's personal information, whether obtained from the individual's offline or online activities or behavior.[82]

Personal information would include any inferences drawn from information used "to create a profile about a consumer reflecting the consumer's preferences,

characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[83]

## C. Reflections

Where along the spectrum should the privacy policy be set? Although each proposal seeks to address a key source of the data-opolies' power—namely, the ability to extract personal data to manipulate behavior to maximize engagement and advertising revenues, the more privacy-focused proposals use defaults and choice architecture to help us avoid surveillance. And defaults matter. If privacy is a fundamental human right and if data-opolies have the incentives to game the system to continue their surveillance, profiling, and behavioral manipulation, it makes sense to opt for a more privacy-centered option.

In weighing the options, one must avoid the trap that behavioral advertising is solely about providing more relevant ads. Competition in the digital platform economy is for *attention* and *manipulation*. Under the guise of personalizing and improving their services, firms design their apps and products like slot machines to attract and addict us.[84] The next chapter explores the toll from the surveillance economy on our privacy, autonomy, well-being, and democracy.

Consequently, to regain our autonomy and privacy and safeguard democracy, the surveillance apparatus must be dismantled. A ban on behavioral advertising, by itself, would be inadequate. Google and Facebook, left with contextual advertising, would still have the incentive to appeal to our emotions to addict us and display more ads to us. Policymakers cannot afford to ignore attention markets and the manipulation of our emotions, thoughts, and behavior.[85]

But tackling the toxic competition for our attention is more challenging, given the implications for free speech and public discourse. The aim of any engrossing book, movie, podcast, play, or opera is to engage us.

So, the law should allow us to avoid being profiled, avoid having our data amalgamated, and avoid personalized recommendations. While this may be harder for digital assistants, we should be afforded this choice, especially when the next generation of cars and smart appliances will have (or require) a digital assistant. We should decide, without penalty, the right to limit at the onset what data is collected about us and for what purpose.

So let us next consider the likely benefits and risks in dismantling the surveillance economy.

1 Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

2 Australian Competition and Consumer Commission, Digital Platforms Inquiry—Final Report at 5 (2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report [https://perma.cc/M36S-YQJ4] [hereinafter ACCC Final Report].

3 *Id.* at 5.

4 *Id*.

5 California Privacy Rights Act of 2020 § 1798.140(h), https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf [hereinafter CPRA]. The CPRA defines dark patterns "as a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation." CPRA § 1798.140(l).

6 Majority Staff of H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial and Administrative Law, Report and Recommendations: Investigation of Competition in Digital Markets at 53 (2020), https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429 [https://perma.cc/29LN-L4BL] [hereinafter House Report]; *see also* Chris Jay Hoofnagle, Federal Trade Commission Privacy Law and Policy 347 (2016) (noting that consumer protection "means moving beyond contract law norms").

7 European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 (Adopted on Oct. 20, 2020) 19, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_ [hereinafter EDPB 2020 Guidelines] (stating that dark patterns are "contrary to the spirit of Article 25" of the GDPR and data controller under the GDPR cannot "present the processing options in such a manner that makes it difficult for data subjects to abstain from sharing their data, or make it difficult for the data subjects to adjust their privacy settings and limit the processing"). For the anticompetitive effects of dark patterns *see, e.g.*, Gregory Day & Abbey Stemler, *Are Dark Patterns Anticompetitive?*, 72 Ala. L. Rev. 1 (2020).

8 *In re* Facebook, Inc., FTC File No. 092 3184 No. C-4365 (F.T.C. Nov. 29, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf [https://perma.cc/3NJ3-DZE4].

9 Press Release, Federal Trade Commission, Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep [https://perma.cc/4K58-H2XV].

10 Press Release, Federal Trade Commission, FTC Approves Final Settlement with Facebook (Aug. 10, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook

11 Complaint ¶ 4, United States v. Facebook, Inc., No. 1:19-cv-2184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-

24-19.pdf [https://perma.cc/U844-H6R9] [hereinafter Facebook 2019 Compl.].

12 *Facebook Scandal "Hit 87 Million Users,"* BBC (Apr. 4, 2018), https://www.bbc.com/news/technology-43649018; Jamie Ross, *Trump's 2016 Campaign Listed Millions of Black Voters It Wanted to Stop From Voting, Leak Reveals*, Daily Beast (Sep. 29, 2020), https://www.thedailybeast.com/trumps-2016-campaign-listed-millions-of-black-voters-it-wanted-to-stop-from-voting-leak-reveals?source=articles&via=rss.

13 Facebook 2019 Compl. at ¶¶ 128–143.

14 Chris Hughes, *It's Time to Break Up Facebook*, N.Y. Times (May 9, 2019), https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html [https://perma.cc/4ABN-LN7M].

15 Press Release, Facebook Settles FTC Charges That It Deceived Consumers, *supra* note 9.

16 Facebook 2019 Compl. at ¶¶ 88–89. In April 2015, Facebook removed general access to affected friend data but Facebook privately granted continued access to Friend Data to more than two dozen developers—the Whitelisted Developers—which included gaming, retail, and technology companies, as well as third-party developers of dating apps and other social-media services. Facebook 2019 Compl. at ¶ 8.

17 House Report at 402.

18 House Report at 402.

19 House Report at 403.

20 Press Release, Bundeskartellamt, Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2 [https://perma.cc/L9PC-Y48K].

21 Fed. Trade Comm'n, *In re* Facebook, Inc. (FTC File No. 1823109), Dissenting Statement of Commissioner Rebecca Kelly Slaughter (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_24-19.pdf [https://perma.cc/U3AR-E5YN].

22 Fed. Trade Comm'n, *In re* Facebook, Inc. (FTC File No. 1823109), Dissenting Statement of Commissioner Rohit Chopra (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_st 24-19.pdf [https://perma.cc/5U9N-SJN7].

23 Fed. Trade Comm'n, *In re* Facebook, Inc. (FTC File No. 1823109), Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_24-19.pdf [https://perma.cc/2CJS-B2JT].

24 Tisdale v. Tisdale, 34 Tenn. (2 Sneed) 596, 608 (1855).

25 Under this equitable remedy, the defendant obtains or holds a legal right to certain property, which the defendant obtained by wrongful means (such as fraud, duress, or breach of fiduciary duty). Although defendant has a good legal title to property, defendant in equity

and good conscience should not hold and enjoy that property. So the court imposes on defendant an equitable duty to convey the property to the plaintiff.

26 European Data Protection Board, *Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects—Version Adopted After Public Consultation* ¶ 52 (Oct. 8, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf [https://perma.cc/Z556-66NG] [hereinafter EDPB 2019 Guidelines]; *see also* EDPB 2020 Guidelines ¶¶ 40-53.

27 EDPB 2019 Guidelines ¶ 53.

28 European Commission, Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) at 29 (Dec. 15, 2020), https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf [https://perma.cc/G87S-Q88U] [hereinafter Digital Markets Act] (requiring at a minimum that gatekeepers describe "the basis upon which profiling is performed, including whether personal data and data derived from user activity is relied on, the processing applied, the purpose for which the profile is prepared and eventually used, the impact of such profiling on the gatekeeper's services, and the steps taken to enable end users to be aware of the relevant use of such profiling, as well as to seek their consent"). The gatekeeper must also submit to the European Commission "an independently audited description of any techniques for profiling of consumers that the gatekeeper applies to or across its core platform services." Digital Markets Act Art. 13.

29 Under Article 24 of the Digital Services Act, "online platforms that display advertising on their online interfaces shall ensure that the recipients of the service can identify, for each specific advertisement displayed to each individual recipient, in a clear and unambiguous manner and in real time: (a) that the information displayed is an advertisement; (b) the natural or legal person on whose behalf the advertisement is displayed; [and] (c) meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed." European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC (Dec. 15, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en [https://perma.cc/6XT3-MGZN] [hereinafter Digital Services Act or DSA].

30 Under Article 30 of the Digital Services Act, these "very large online platforms," as defined under the DSA, would have to compile and make publicly available additional information, including "(a) the content of the advertisement; (b) the natural or legal person on whose behalf the advertisement is displayed; (c) the period during which the advertisement was displayed; (d) whether the advertisement was intended to be displayed specifically to one or more particular groups of recipients of the service and if so, the main parameters used for that purpose; (e) the total number of recipients of the service reached and, where applicable, aggregate numbers for the group or groups of recipients to whom the advertisement was targeted specifically."

31 Under Article 36 of the Digital Services Act, the European Commission would "encourage and facilitate the drawing up of codes of conduct at Union level between, online platforms and other relevant service providers, such as providers of online advertising intermediary services or organisations representing recipients of the service and civil society organisations or relevant authorities to contribute to further transparency in online advertising beyond the requirements of Articles 24 and 30." The Commission would encourage the development and application of the codes of conduct within a specified time period, and ensure that the codes of conduct address at least the transmission of information held by providers of online advertising intermediaries to recipients of the service with regard to requirements set out in the DSA.

32 ACCC Final Report at 374; OECD, Big Data: Bringing Competition Policy to the Digital Era: Background Note by the Secretariat, at 18, DAF/COMP(2016)14 at 25 (Apr. 26, 2017), https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf [hereinafter OECD Big Data Report].

33 Paul Hitlin & Lee Rainie, *Facebook Algorithms and Personal Data*, Pew Res. Center (Jan. 16, 2019), https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/ [https://perma.cc/6P64-P764].

34 *Id.*

35 Press Release, Bundeskartellamt, Preliminary Assessment in Facebook Proceeding: Facebook's Collection and Use of Data from Third-Party Sources Is Abusive (Dec. 19, 2017), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2 [https://perma.cc/PUS6-SRFS].

36 Hoofnagle, *supra* note 6, at 346.

37 Bundeskartellamt Dec. 19, 2017 Press Release, *supra* note 35.

38 In re Facebook, Inc., Consumer Priv. User Profile Litig., 402 F. Supp. 3d 767, 776 (N.D. Cal. 2019).

39 *Facebook*, 402 F. Supp. 3d at 789.

40 *Id.*

41 *Id.* at 777.

42 Yan Carrière-Swallow & Vikram Haksar, *The Economics and Implications of Data: An Integrated Perspective*, International Monetary Fund Policy Paper No. 19/16 (Sept. 2019), https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596 at 5.

43 CPRA ¶ I (noting the use of "technologies and tools that are opaque to consumers to collect and trade vast amounts of personal information, to track them across the internet, and to create detailed profiles of their individual interests").

44 The opt-out for behavioral advertising, however, might be subject to dispute. Under section 1798.121(a) of the CPRA, a consumer can, at any time, direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive

personal information:

[1] "to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services,"
[2] to perform the services set forth in Section 1798.140(e)(2), (4), (5), and (8), where companies can use sensitive personal data:
  [i] when "helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes";
  [ii] for "short-term, transient use, including but not limited to non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business;"
  [iii] for performing services on the business's behalf, "including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business;" and
  [iv] when "undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business;" and
[3] as authorized by regulations adopted pursuant to Section 1798.185(a)(19)(C).

45 CPRA § 1798.140(ah)(1). This opt-out would apply "whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged." *Id*.

46 The statute defines cross-context behavioral advertising as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts." CPRA § 1798.140(k).

47 CPRA § 1798.140(ae). The opt-out provision is CPRA § 1798.121.

48 CPRA § 1798.140(v)(2):

> "Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, "publicly available" means: information that is lawfully made available from federal, state, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.

49 The CPRA, however, does envision the Attorney General issuing regulations regarding profiling which the statute defines as "any form of automated processing of personal Information . . . to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." § 1798.140(z). Thus, the Attorney General may issue regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185.

50 CMA Final Report ¶ 3.90.

51 CPRA § 1798.125(a)(1).

52 CPRA § 1798.125(a)(2).

53 CPRA ¶ F.

54 CPRA § 1798.125(b)(4).

55 CMA Final Report ¶ 8.96, n. 482.

56 Daniel Kahneman, *Maps of Bounded Rationality: Psychology for Behavioral Economics*, 93 Am. Econ. Rev. 1449, 1456 (2003); Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision Under Risk*, 47 Econometrica 263, 268 (1979).

57 CPRA § 1798.185(a)(1).

58 Do Not Track Act, S. 1578, 116th Congress (2019), https://www.govinfo.gov/content/pkg/BILLS-116s1578is/pdf/BILLS-116s1578is.pdf.

59 Do Not Track Act, *supra* note 58 ("For purposes of this subsection, a covered website, service, or application that collects data for the purpose of designing or displaying targeted advertisements shall be considered to be collecting more data than is necessary to operate such website, service, or application.").

60 *See, e.g.*, Hoofnagle, *supra* note 6, at 183-85 (identifying problems with defaults requiring users to opt in to privacy protections).

61 Richard H. Thaler & Cass R. Sunstein, Nudge: Improving Decisions About Health, Wealth, and Happiness 78, 129–30 (2008); OECD, *Consumer Policy Toolkit 46–47* (2010), https://read.oecd.org/10.1787/9789264079663-en; Stefano DellaVigna, *Psychology and Economics: Evidence from the Field*, 47 J. Econ. Literature 315, 322 n.11 (2009); Eric J. Johnson et al., *Defaults, Framing and Privacy: Why Opting In–Opting Out*, 13 Marketing Letters 5–15 (2003) (consent to receive e-mail marketing); C. Whan Park et al., *Choosing What I Want*

*Versus Rejecting What I Do Not Want: An Application of Decision Framing to Product Option Choice Decisions*, 37 J. Mktg. Rsch. 187–202 (2000) (car option purchases); European Consumer Consultative Group, Opinion on Private Damages Actions 4 (2010), http://ec.europa.eu/consumers/empowerment/docs/ECCG_opinion_on_actions_for_damages_ [https://perma.cc/F4CY-J333] (in European countries, where the default option was opt-in, so that consumers had to opt into the class, the rate of participation in class actions for consumer claims was less than 1%; under opt-out regimes, where the default is that one is a class member unless one opts out, participation rates were typically very high (97% in the Netherlands and almost 100% in Portugal)).

62 CMA Final Report ¶ 32.

63 Plus, as the European Commission found, and the United States and states alleged in their monopolization complaint, Google engaged in anticompetitive tying arrangements to be the default search engine on Android devices. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52019XC1128(02); Complaint ¶ 56, United States v. Google, No. 1:20-cv-03010 (D.D.C. Oct. 20, 2020), https://www.justice.gov/opa/press-release/file/1328941/download.

64 Alexandra Wood et al., *Differential Privacy: A Primer for a Non-Technical Audience*, 21 Vand. J. Ent. & Tech. L. 209, 264 (2018).

65 Reno v. Condon, 528 U.S. 141, 144–45 (2000) (noting how Congress amended the Driver's Privacy Protection Act so that "States may not imply consent from a driver's failure to take advantage of a state-afforded opportunity to block disclosure, but must rather obtain a driver's affirmative consent to disclose the driver's personal information for use in surveys, marketing, solicitations, and other restricted purposes").

66 UK Competition & Markets Authority, Online Platforms & Digital Advertising: Market Study Interim Report ¶ 6.41 (2019), https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pd [hereinafter CMA Interim Report].

67 CMA Final Report at ¶ 97; CMA Interim Report at ¶ 6.94.

68 CMA Final Report at ¶ 97; CMA Interim Report at ¶ 6.105.

69 CMA Final Report at ¶ 8.94.

70 CMA Final Report at ¶¶ 4.68 ("once consumers understand more about how targeted advertising works, they become more concerned about the data processing that is involved and can potentially be less willing to receive advertising that is personalized") & 4.70.

71 CMA Final Report at ¶ 4.70; *see also* Chang-Dae Ham, *Exploring How Consumers Cope with Online Behavioral Advertising*, 36 Int'l J. Advert. 632 (2016), https://doi.org/10.1080/02650487.2016.1239878.

72 The CMA also proposed a quasi-non-discrimination provision. CMA Final Report at ¶ 97; CMA Interim Report at ¶ 6.108. U.K. residents could continue to use the data-opolies' services, whether watching a YouTube video or posting on Facebook. Data-opolies could use personal data to improve their services, such as more relevant responses to a search query. However, when users opt for privacy, the platforms could not retaliate by degrading (or

denying) the service. But data-opolies could offer users incentives to part with their data for behavioral advertising purposes, which raises similar concerns of abuse as with California's 2020 privacy statute.

73 Bundeskartellamt, Case Summary, Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing, at 10 (Feb. 15, 2019), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufs 22-16.pdf?__blob=publicationFile&v=4 [hereinafter Bundeskartellamt Facebook Case Summary] (enabling German residents to prohibit Facebook from tracking them when they visit other websites that use "Facebook Business Tools," such as its social plugins ("Like" or "Share" buttons), Facebook login, and other analytics services (Facebook Analytics) that are implemented through "Facebook Pixel" or mobile "software development kits" (SDKs)).

74 Bundeskartellamt Facebook Case Summary, *supra* note 73 ("Processing data from third-party sources to the extent determined by Facebook in its terms and conditions is neither required for offering the social network as such nor for monetising the network through personalised advertising, as a personalised network could also be based to a large extent on the user data processed in the context of operating the social network.").

75 For the opt-in for aggregation, but not behavioral advertising, *see* Article 5 of the Digital Markets Act, which would prevent powerful gatekeepers "from combining user data gathered from core platform services with user data gathered from other services offered by the gatekeeper or third parties without proactive user consent."

76 Press Release, Federal Trade Commission, FTC Releases FY 2020 National Do Not Call Registry Data Book (Oct. 27, 2020), https://www.ftc.gov/news-events/press-releases/2020/10/ftc-releases-fy-2020-national-do-not-call-registry-data-book [https://perma.cc/5R86-G4LN].

77 *Id.*

78 Federal Trade Commission, *National Do Not Call Registry: What the Registry Doesn't Do* (June 2019), https://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry#doesntdo [https://perma.cc/FC46-PP5M].

79 Facebook, *About Lookalike Audiences*, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last accessed Mar. 27, 2021),

80 Samuel Stolton, *Parliament Adopts Ambitious Stance on EU's Future Regulation of Digital Platforms*, EURACTIV (Oct. 21, 2020), https://www.euractiv.com/section/digital/news/parliament-adopts-ambitious-stance-on-eus-future-regulation-of-digital-platforms/ [https://perma.cc/EL5Q-ZMPK].

81 CPRA § 1798.140 (k) (emphasis added).

82 Personal information would include, as the California Privacy Rights Act of 2020 defines, "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including the CPRA's 12 categories of information (such as biometric information).

83 CPRA § 1798.140(v)(1)(K).

84 Tristan Harris, *How Technology Is Hijacking Your Mind—From a Magician and Google Design Ethicist*, Medium (May 18, 2016), https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3 [https://perma.cc/4E44-L2JW].

85 *See, e.g.*, John M. Newman, *Antitrust in Attention Markets: Objections and Responses*, 59 Santa Clara L. Rev. 743 (2020); Tim Wu, *Blind Spot: The Attention Economy and the Law*, 82 Antitrust L.J. 771 (2019).

# 10
# Responding to Potential Criticisms to a Ban on Surveillance Capitalism

Who made the following argument about the erosion of trust online and the need for alternatives?

> In fact, 72% of people feel that almost all of what they do online is being tracked by advertisers, technology firms or other companies, and 81% say that the potential risks they face because of data collection outweigh the benefits, according to a study by Pew Research Center. If digital advertising doesn't evolve to address the growing concerns people have about their privacy and how their personal identity is being used, we risk the future of the free and open web. . . .
>
> People shouldn't have to accept being tracked across the web in order to get the benefits of relevant advertising. And advertisers don't need to track individual consumers across the web to get the performance benefits of digital advertising.[1]

It was Google in 2021. Few, if anyone, will argue that nothing needs to be done.

Some might argue for the more modest proposals (e.g., improved privacy guidelines and greater transparency), since there are already signs of promise. Apple in 2021 offered the option of avoiding third-party tracking, which slowed the growth of revenues for some firms, like Facebook and Snap. As Facebook told investors, Apple's privacy measure posed two challenges: it decreased the accuracy of Facebook's ad targeting, which increased the cost of driving outcomes for its advertisers. And measuring the outcomes the ads had on individuals became more difficult.[2]

Google is experimenting with replacing individual tracking (when we are on other websites) with its FLoC option of placing us in groups. Europe's GDPR, bolstered by the Digital Markets Act and Digital Services Act, will increase transparency. Consequently, some will advocate to allow time to see whether stronger guidelines and greater transparency will work. Consumers might demand a broader range of ad-supported and paid content and choose the options that match their privacy interests. If greater transparency fails, then policymakers can resort to default options and possibly a ban on behavioral advertising.

But the surveillance economy will persist, and the harm to our privacy, well-

being, autonomy, and democracy will increase. Consequently, others, like the European Data Protection Supervisor, are arguing that policymakers should consider banning "online targeted advertising based on pervasive tracking and restrict the categories of data that can be processed for such advertising methods."[3]

Let us consider the likely criticisms of a ban on behavioral advertising, limits on profiling and amalgamating personal data, and allowing individuals to opt out of personalized services.

## A. Do You Want Relevant Ads or Porn?

In banning behavioral advertising, we would get less relevant ads. That is what Google, Apple, Facebook, and Amazon stated in early 2021, should we opt for a more privacy-friendly option.[4]

When we presented our earlier books at antitrust conferences, a lawyer representing Google would respond that we want relevant ads, not "porn ads." I first thought he was joking, given the starkness of his alternatives—either surveillance capitalism (where the data-opolies primarily profit) or non-stop ads from pornographers. It is what *Wired* magazine calls a "meso-idea, an idea that has ceased to be true but that people continue to repeat, ad infinitum, as if it still was."[5]

The reality is that data-opolies have also marginalized the porn industry:

> The big tech companies behind the big platforms control not only the gateway services (the iPhone app store, Google Search, the Facebook social network) but the gateway devices (the iPhone, Android phones, Google Chromecast, the Amazon Fire TV, the Oculus Rift virtual reality headset). And for the most part, they've shut porn out.[6]

But Google no longer raises the porn/relevant ads dichotomy. It now recognizes that companies need to do more to protect privacy and stop individual tracking. As Google states, we can have relevant advertising without third-party cookies and "any technology used for tracking individual people as they browse the web."[7]

Others, like Facebook, might disagree. While we might not get porn ads, we may get less relevant ads.

Despite behavioral advertising proliferating over the past decade, there is no compelling evidence that most individuals prefer it. Instead, as we saw, most

people oppose the surveillance apparatus of behavioral advertising. We feel less threatened by contextual ads than behavioral ads. Few, if any of us, like being surveilled and manipulated. Thus, many, in a 2020 study, were threatened by behavioral advertising, feeling that the advertiser "threatened my freedom to choose," "tried to make a decision for me," "tried to manipulate me," and "tried to pressure me."[8] As a result, the study's participants viewed behavioral ads negatively and were less likely to buy the advertised product.[9] The study's authors suggest that marketers "reduce surveillance cues." While practical advice, the suggestion of hiding the creepy surveillance calls into question the intrinsic value of behavioral advertising. As Cambridge Analytica's whistleblower noted, this mixture of secrecy and manipulation is anti-democratic:

> I think it's worse than bullying, because people don't necessarily know it's being done to them. At least bullying respects the agency of people because they know . . . if you do not respect the agency of people, anything that you're doing after that point is not conducive to a democracy. And fundamentally, information warfare is not conducive to democracy.[10]

## B. Smaller Publishers and Advertisers Will Pay the Price

One potential trade-off from a ban on behavioral advertising and profiling is greater inefficiency in advertising. The U.S. merchant John Wanamaker is credited with saying this: "Half the money I spend on advertising is wasted; the trouble is I don't know which half."[11] Data collection and tracking can help advertisers target those users interested in their products (such as those looking to buy a new SUV). Advertisers can choose the most cost-effective app or website to target the person. Why spend $354,823.27 for a full-page color ad in *The Wall Street Journal*[12] when that same reader can be targeted on other webpages for a fraction of that amount? Thus, if behavioral ads were banned, it can be costlier for smaller advertisers to target those who may be interested in their products and assess their ads' effectiveness.

Facebook, for example, argues that behavioral advertising benefits small businesses: "While it's difficult to quantify the impact to content creators and publishers at this point with so many unknowns, in testing we've seen publishers experience more than a 50% drop in revenue when personalization was removed from mobile app ad install campaigns."[13]

As we saw in Chapter 4, it is unsettled whether most advertisers and publishers are significantly benefiting from behavioral advertising. One common belief is that advertisers must benefit; otherwise, why are they increasing their advertising with Facebook and Google? But the emerging economic findings are mixed, as two IMF officials noted in 2019.[14]

Moreover, as behavioral advertising becomes creepier and more intrusive, advertisers can lose goodwill and customer trust,[15] especially when their ads are embedded in divisive, conspiratorial, racist, or otherwise offensive content used to attract and maintain our attention.

Even if behavioral advertising is more efficient, it remains a rigged game. Google and Facebook capture most of the online ad revenues and profits. Amazon is the only potentially significant rival on the horizon. Apple reaps billions of dollars annually from the behavioral advertising spoils, and its privacy policies advantage its own advertising business (according to Facebook).

But what about Facebook's study of a 50% drop in revenue when a publisher does not use behavioral ads? It appears from Facebook's brief description that ad revenues declined when some publishers delivered personalized ads and others did not.[16] But we know that already. As market participants have observed, behavioral advertising is an arms race. In any arms race, the key is de-escalation. Every country would be better off if no other government invested in germ or nuclear warfare. Therefore, governments bear the responsibility to stop this toxic competition—whether it is the race for cheaper labor through human degradation (e.g., prohibiting child or slave labor), campaign spending,[17] or environmental degradation.

Advertising is no different. As we saw in Chapter 4, market participants cannot opt out of behavioral advertising if their rivals continue to rely on it. That is true for both publishers and advertisers. Nor can the rivals agree among themselves to refrain from behavioral advertising (without running afoul of the antitrust laws). But no publisher or advertiser would be at a competitive disadvantage if none of their rivals could engage in behavioral advertising. Antitrust scholar Robert Steiner, who was also the Kenner Products toy company's former president, described his concerns about the industry self-regulation of toy commercials in the 1960s and 1970s. Initially favoring industry self-policing, he feared the greater anticompetitive consequences of deceptive advertising. Absent regulation, some toy manufacturers would air misleading ads, which would pull down the toy industry. Unless his company matched "the

exaggerations and sometimes the outright deceptions of certain competitors, our commercials might not be exciting enough to move our toys off the shelves."[18] To prevent this race to the bottom, where dishonest advertisers drive out honest dealers, the law often requires mandatory disclosures and prohibits deceptive ads and practices.[19]

And we already have some guardrails. The Children's Online Privacy Protection Act, for example, seeks to limit profiling and targeting of children with behavioral ads without parental consent, but allows contextual advertising.[20] With contextual advertising as the norm, small businesses are not left with expensive traditional advertising outlets. For example, they can still target the 1.4 billion Facebook users who connect with each other in the 10 + million niche groups Facebook offers.[21] Indeed, it is telling that Google, which developed over the years the leading surveillance network across the web, now argues that "advertisers don't need to track individual consumers across the web to get the performance benefits of digital advertising."[22]

## C. Consumers Will Be Harmed with Fewer Free Services

Another concern is that without the revenues from behavioral ads, many websites, apps, and platforms might no longer offer free services, which would have a regressive effect.[23]

But a ban on surveillance would not prohibit all advertising, only behavioral advertising. Publishers could still rely on contextual advertising revenue models and offer free services (as broadcast television and radio stations have done for decades). But the micro-targeting and manipulation of individuals would stop.

If behavioral advertising were banned, Google, for example, could still sell search ads based on our search terms, and online display advertisers could target anyone visiting a sports website with sports-related ads or based on the general demographics of its audience. A Google official testified before Congress that most search ads depend on context, not personal data.[24] Google is already doing this to a certain extent for political advertising.[25] Likewise, DuckDuckGo currently offers a free search engine funded by contextual advertising based on our search terms (not by tracking and profiling us). As the privacy-friendly search engine notes,

> It is a myth that search engines need to track you to make money on Web search. When you type in a search, we can show an ad just based on that search term. For example, if you type in, "car" we show a car ad. That doesn't involve tracking because it is based on the keyword and not the person.[26]

Consequently, banning behavioral advertising and limiting profiling would likely level the playing field. Traditional media and millions of websites and apps could now compete for our loyalty and trust through quality, helpful information, rather than surgically incise our neurosis, fears, and emotions.

## D. First Amendment Concerns

Restrictions on behavioral advertising might run afoul of the First Amendment of the U.S. Constitution. In *Sorrell v. IMS Health Inc.*, pharmacies were collecting data about doctors' prescriptions, which they then sold to "data miners," who produced reports on each doctor's prescriber behavior.[27] Drug manufacturers then used the data miners' reports to refine and target their marketing tactics and increase sales of their branded drugs to the prescribing doctors.

In response, Vermont prohibited the pharmacies from selling this data for marketing purposes without the prescribing doctor's consent.

Several data miners and an association of brand-name drug manufacturers challenged the state law, contending that it violated their First Amendment free speech rights.

The Supreme Court ruled in the data miners' and brand-name drug manufacturers' favor. The Court first observed that the challenged law warranted heightened judicial scrutiny because it disfavored speech with a particular content (i.e., marketing) and particular speakers (i.e., the data miners engaged in marketing on the drug manufacturers' behalf).

Vermont responded that its prohibitions safeguarded medical privacy, including physician confidentiality and the integrity of the doctor-patient relationship. The Court disagreed. The state law did not directly advance these privacy interests, because the pharmacies, under the law, could share "prescriber-identifying information with anyone for any reason save one: They must not allow the information to be used for marketing."[28] The law did not promote privacy when the information was available to "an almost limitless audience"—such as insurers, researchers, journalists, and the state itself. Many could access the data except a narrow class of disfavored speakers (those engaged in

marketing on behalf of pharmaceutical manufacturers) for a disfavored purpose (marketing).[29]

The Court left open an alternative. The state could advance its asserted privacy interest if its law limited "the information's sale or disclosure in only a few narrow and well-justified circumstances."[30]

That presents a dilemma for U.S. policymakers when personal data is non-rivalrous. The whole point is to share personal data when it increases overall welfare and limit only those uses where it does not. Economists might favor that surgical approach, but such discrimination could violate the First Amendment protections afforded to these disfavored speakers (behavioral advertisers and their enablers) for their disfavored purpose (behavioral advertising).

To avoid running afoul of the First Amendment, the government has several options. First, it could rely on another substantial governmental interest (besides privacy) and show that its statute directly advances that interest and is drawn to achieve that interest. Alternatively, the government can rely on privacy as a substantial governmental interest. But the law must limit the data's collection and use to what is objectively necessary to provide the service or product and restrict the data's disclosure (absent de-identification) to a few narrow, well-justified circumstances. Or third, the government could argue that its privacy law is not targeting particular messages or speakers (such as advertisers) but addresses the underlying surveillance apparatus of behavioral advertising instead.[31]

## E. Examining the Toll from the Surveillance Economy

Let us suppose, on a quality-adjusted basis, behavioral ads for some advertisers are more cost-effective in driving sales than contextual ads.[32] What is good for the advertiser is not necessarily good for the individual or society.[33] Let us consider some of the harms from behavioral advertising and the surveillance and manipulation of behavior.

### 1. Cost to Privacy

Behavioral advertising will only become more intrusive to our privacy and autonomy. Data-opolies are already stalking us across the web and predicting and manipulating our behavior. Facebook already tracks the behavior of people who broke up from long-term relationships and highlights specific ways that advertisers can appeal to them: "Whether people are binge-watching on the

couch, scrolling through their feeds or exploring new places, mobile is where you will have the best opportunity to reach them."[34]

It is what comes next that will significantly wear down our privacy. As one 2020 survey of the literature found, delivering more deeply personalized advertisements "that retain a sense of serendipitous experience," will require "ever larger, more recent and potentially more sensitive data."[35]

Advertisers have already gone far beyond intent-based marketing (where your searching on the web reflects what you are looking to purchase or do) to emotion-based marketing.[36] A chief scientist of an AI and natural language processing company in 2020, for example, heard one thing from many marketing departments: "How can we use AI to better understand consumers' emotional states?"[37] Deciphering our facial expressions is posing a challenge for deep learning algorithms. Nevertheless, that is the marketers' aim, as the computer scientist noted:

> You can imagine how this technology could be deployed across millions of camera-enabled PCs, gaming consoles, or TVs to track consumer reactions in a similar way. In the realm of text, a social media platform could start rewarding advertisers differently based on perceived emotional reactions of consumers as determined by the text they leave in the comments sections.[38]

To monitor your emotional reactions to different types of content, Facebook, for example, in 2015, patented "techniques for emotion detection and content delivery."[39] Facebook's technology would capture your facial expression through your smartphone or laptop camera, "even when [you] are not actively using the camera."[40] Facebook could "determine which emotions a piece of content elicits, which could be useful for Facebook as well as the content producers," and "deliver content to the user based on the displayed emotion, which could help Facebook keep users more engaged."[41]

Not to be outdone, Microsoft patented even creepier technology – an "emotional/cognitive state-triggered recording system." The technology automatically records events upon detecting a change in your emotions, including "happiness, sadness, anger, fear, disappointment, or pride," and cognitive states such as "focused, engaged, distracted, bored, sleepy, confused, or frustrated."[42] Microsoft's technology detects, for example, when you are happy and records what is making you happy. In its patent, Microsoft provides its vision of the future:

> In the illustrated example, the user attends a work meeting between 9:00 am and 10:00 am and attends her son's baseball game between 5:30 pm and 7:00 pm.
>
> At approximately 9:10 am, a co-worker announces that all company employees will be receiving a bonus next week. This announcement evokes feelings of happiness for the user, triggering emotional/cognitive state-triggered recording system to record a happiness-based video segment. Later during the same meeting, a heated discussion about an error that was made in processing a customer order evokes feelings of anger for the user. The emotional/cognitive state-triggered recording system detects the user's anger, and in response, records an anger-based video segment.
>
> At 5:30, the user attends her son's baseball game. The user gets excited when her son is first up to bat. The emotional/cognitive state-triggered recording system detects the user's excitement, and in response, records an excitement-based video segment. Later in the game, the user's son hits a homerun, causing the user to feel proud of her son. The emotional/cognitive state-triggered recording system detects the user's feelings of pride, and in response, records a proud-based video segment. Still later in the game, the user's son collides with another player and falls to the ground, obviously in pain. This scenario evokes feelings of fear in the user. The emotional/cognitive state-triggered recording system detects the user's fear, and in response, records a fear-based video segment.
>
> At the end of the day, the user is able to review the various video segments that were recorded throughout the day. In some examples, the video segments also include metadata, which may include, for example, an indication of the detected emotional/cognitive state that triggered the recording, ongoing or periodic emotional/cognitive state indicators during the video segment, and/or an overlay that includes a dot, highlight, or other visual indicator of where the user was looking while the video was being recorded.[43]

The patented technology would also allow you to share your current emotions electronically with others walking down the street.

The surveillance, of course, will not be passive but experimental, testing our emotional reactions and behavior to stimuli. Imagine future data-opolies with access to this "emotional/cognitive state-triggered recording system." We could enter the realm of personalized movies, where a horror film might include childhood images that traumatized you. Ads will evoke pictures to stimulate the emotions to prompt the desired action. To increase profits under the behavioral advertising business model, firms will compete to invent even more intrusive surveillance techniques. Imagine technologies, that like T.S. Eliot's "magic lantern," will throw your nerves "in patterns on a screen."[44]

Building upon Microsoft's "emotional/cognitive state-triggered recording systems" will be neurotechnologies that can read your thoughts. In transitioning

to a metaverse company, Facebook, for example, is funding research in the brain-computer interface, where machine learning can decode our brain activity in real-time.[45] Once our brain activity is tracked and coded, algorithms can better detect, predict, and influence our thoughts, moods, and emotions.

As our privacy deteriorates, we will suffer more significant "psychological harms (like shame, embarrassment, ridicule, and humiliation), relationship harms, vulnerability harms, chilling effects, and power imbalances."[46] As our privacy degrades, self-expression and intellectual life will decrease. As the President's Commission on Law Enforcement and Administration of Justice observed in 1967:

> In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas.[47]

That self-censorship can be our future, where we operate under the constant suspicion that our thoughts, words and behavior are being monitored and evaluated by some omnipresent "emotional/cognitive state-triggered recording system."

## 2. Cost of Data Breach

The surveillance economy in amassing more data about us exposes us to greater risks of identity theft. Data-opolies, for example, have greater incentives to prevent a breach than do typical firms. But even they can be subject to data breaches or illegal data access. With even more personal data collected about our emotions, personality traits, and thoughts, hackers, marketers, political consultants, among others, have even greater incentives to find ways to circumvent or breach any security measures.[48] The concentration of even more personal data from these neurotechnologies and the refinement in profiling our fears, emotions, and weaknesses mean that if this information were breached, the harm done could be orders of magnitude greater than a data breach ten years ago —basically, a "database of ruin."[49] While we may be outraged, if behavioral advertising is the norm, firms have less reason to worry about our switching to rivals.[50]

## 3. Behavioral Discrimination

In targeting us at the right time (when we feel worthless, vulnerable, or overconfident) with the right appeal, behavioral advertising can induce us to buy things we might not otherwise have wanted at the highest price we are willing to pay.

Consumers' personality traits can strongly influence their shopping behavior. So, one 2019 study, sought to examine whether an online retailer could predict a particular customer's psychological traits in real time (i.e., while they were browsing the webpage).[51] It could. Based solely from the consumers' browsing behavior, such as how they might move the mouse across a web page, the machine learning "personality trait prediction algorithm" could accurately predict multiple traits of the study's participants, including their need for arousal, and each of the so-called Big 5 personality traits: Openness to experiences, Conscientiousness, Extraversion, Agreeableness, and Neuroticism.

Many of us view this behavioral discrimination as unfair.[52] Not only is it exploitative, behavioral discrimination can have other adverse effects, such as not investing or spending on things we actually know would benefit us over the long term (such as retirement).[53] Nonetheless, expect a shopping environment designed to manipulate your buying behavior. If you are a consumer with a high need for arousal, expect more "violent, sexual, and fear-provoking content," precisely because you will likely buy more impulsively and "react more favorably" to that content.[54]

## 4. Costs of "Brain Hacking"

When interviewed on the television show *60 Minutes*, Tristan Harris, a former Google product manager, discussed the toxic competition of "brain hacking" to secure our attention:

> And it's not because anyone is evil or has bad intentions. It's because the game is getting attention at all costs. And the problem is it becomes this race to the bottom of the brainstem, where if I go lower on the brainstem to get you, you know, using my product, I win.[55]

The race to addict us and manipulate our behavior wreaks our autonomy and well-being. We know that we spend a lot more time on our phones. In 2018, U.S. adults spent on average nearly four hours a day looking at their phone, computer, or tablet. By 2019, Americans were spending on average 6 hours and 31 minutes online each day. Europeans and Americans spend slightly less time online than

the surveyed worldwide average of 6 hours and 42 minutes.[56] Still, 6 hours per day over the course of one's lifetime translates to a quarter of one's life.

In 2016, *The New York Times* noted, we spent on average more time on Facebook, Instagram, and Messenger (50 minutes per day), than on any other leisure activity except watching television programs and movies (on average 2.8 hours per day).[57] That was more time than we spent reading (19 minutes), or participating in sports or exercise (17 minutes), or social events (4 minutes). By 2018, individuals spent more time on Facebook alone (48.6 minutes) "than on Snapchat (21 minutes) or Twitter (21.6 minutes)."[58] By 2020, over half of the world's population (3.96 billion people) were using online social networks[59] and were spending even more time on these networks—on average, 143 minutes.[60]

After Facebook, we spend a lot of time on YouTube. YouTube, by 2020, reached more adults between 25- and 49-year-olds than all cable networks combined.[61] As of the third quarter of 2020, 77% of U.S. internet users aged 15 to 25 years accessed YouTube,[62] and 92% of YouTube's U.S. audience accessed the video platform every week, and 62% watched YouTube videos every day.[63] Overall, according to Google, YouTube has over two billion active users; every day, "people watch over a billion hours of video and generate billions of views."[64] With over 500 hours of content uploaded to YouTube every minute,[65] there is enough to keep us watching for many more minutes per day.

Of the total time spent online by U.K. users in February 2020, 37% was on sites owned by either Google or Facebook.[66] U.K. consumers spent around 83% of their total time online on about the top 1,000 properties, which included Apple's and Amazon's, "with the remaining 17% split between an extremely long tail of websites."[67]

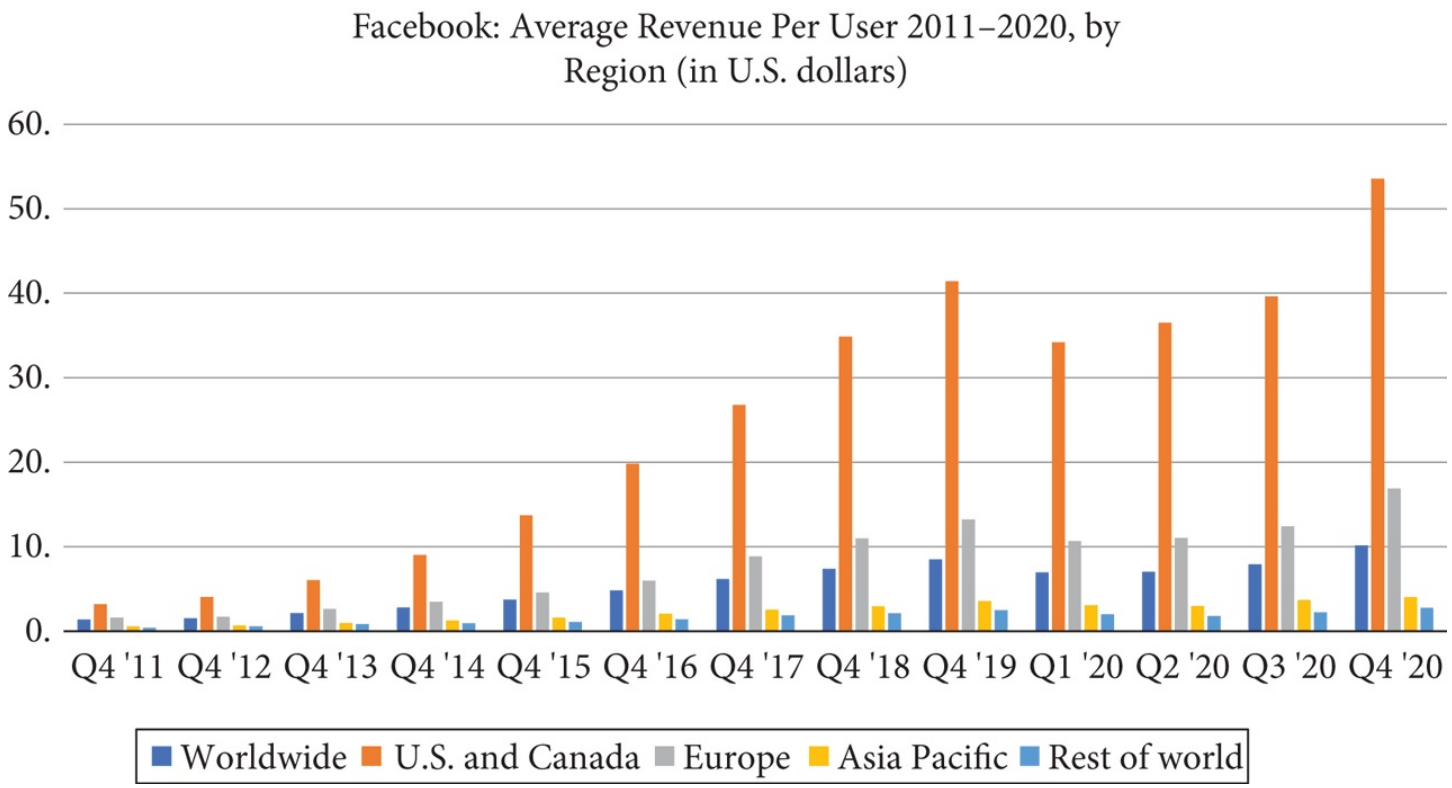


**Figure 10.1** *Source*: H. Tankovska, *Facebook's Average Revenue per User as of 4th Quarter 2020, by Region*, Statista (Feb. 15, 2021), https://www.statista.com/statistics/251328/facebooks-average-revenue-per-user-by-region/ [https://perma.cc/ZPX3-WFBE].

Who primarily profits as we spend more time online? The data-opolies. As Figure 10.1 reflects, in the United States and Canada, Facebook's average revenue per user increased from $3.20 in 2011 to $53.56 per user, by the end of 2020.

As Figure 10.2 shows, Google's behavioral advertising revenues from YouTube more than doubled between 2017 and 2020.

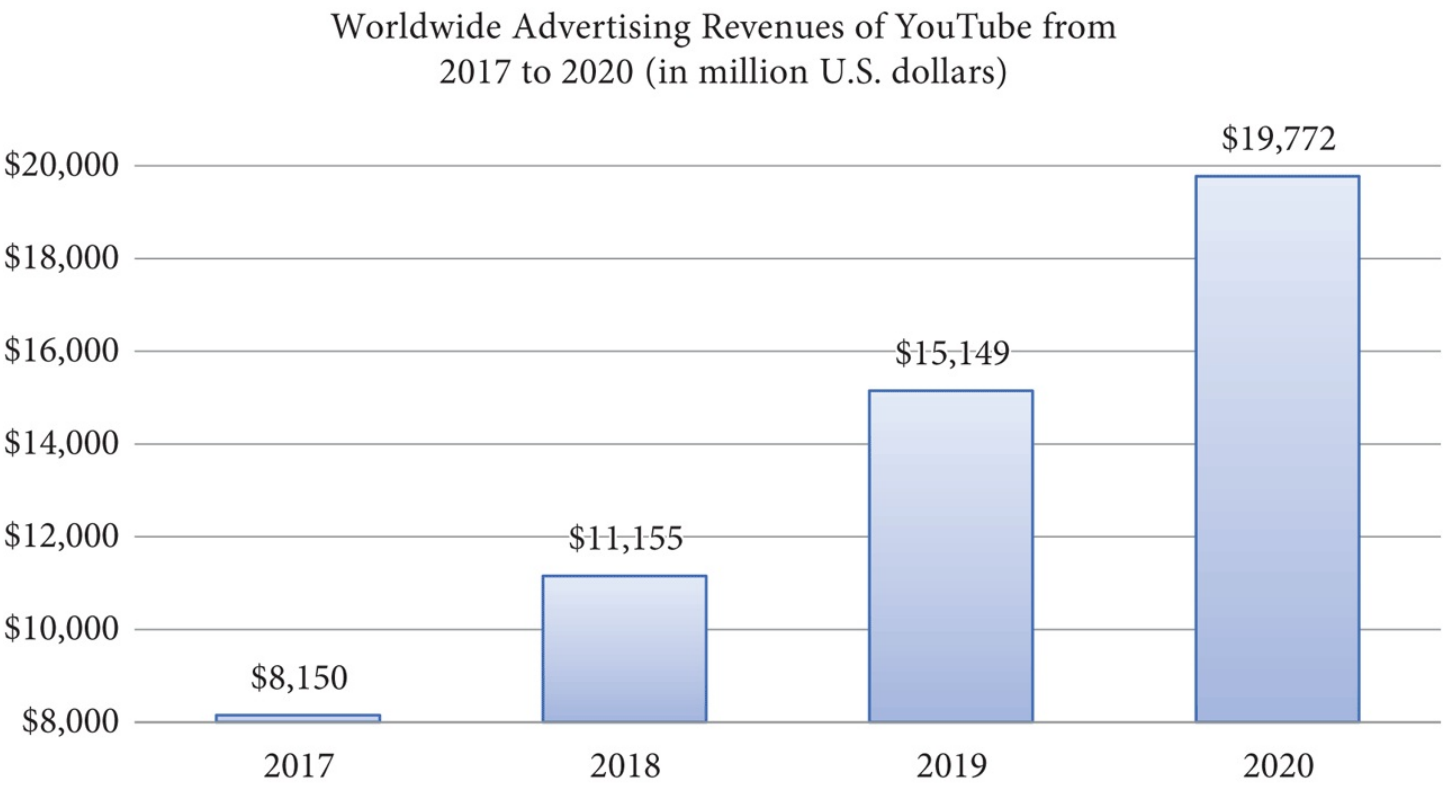


**Figure 10.2** *Source*: Google. You Tube's Worldwide Advertising Revenues

While the data-opolies have profited from our attention and data, have we benefited commensurately? As Facebook's co-founder noted, "We pay for Facebook with our data and our attention, and by either measure, it doesn't come cheap."[68] Let us consider some of the other costs from behavioral advertising's surveillance, addictions, and manipulation.

Psychologists have now defined as disorders "social network site addiction,"[69] "Facebook addiction,"[70] and the fear of being without one's phone —"nomophobia" (no mobile phone phobia).[71] Among the negative consequences of social network site addiction are "being overly concerned" about social network sites, being "driven by a strong motivation to log on to or use" social networks, and "devot[ing] so much time and effort" to social networks "that it impairs other social activities, studies/job, interpersonal relationships, and/or psychological health and well-being."[72]

Facebook researchers internally raised similar concerns about this addiction, which they estimated to affect approximately 1 in 8 Facebook users.[73] That's about 360 million people. Among the symptoms Facebook observed were "sleep disruption—(1) Delaying/reducing sleep hours due to loss of time control; (2) Waking up and checking FB prolonging a return to sleep; and (3) Sleep loss due to disturbing content, like politics or violence."[74] At times, "parents focused

more on FB than caring for or bonding with their children," the Facebook researchers noted.[75]

The time we spend on social media eats into other activities—like reading, sleep, studying, and actually doing things with other people.[76]

As Figure 10.3 reflects, fewer Americans are doing what you are doing right now—reading for personal interest.

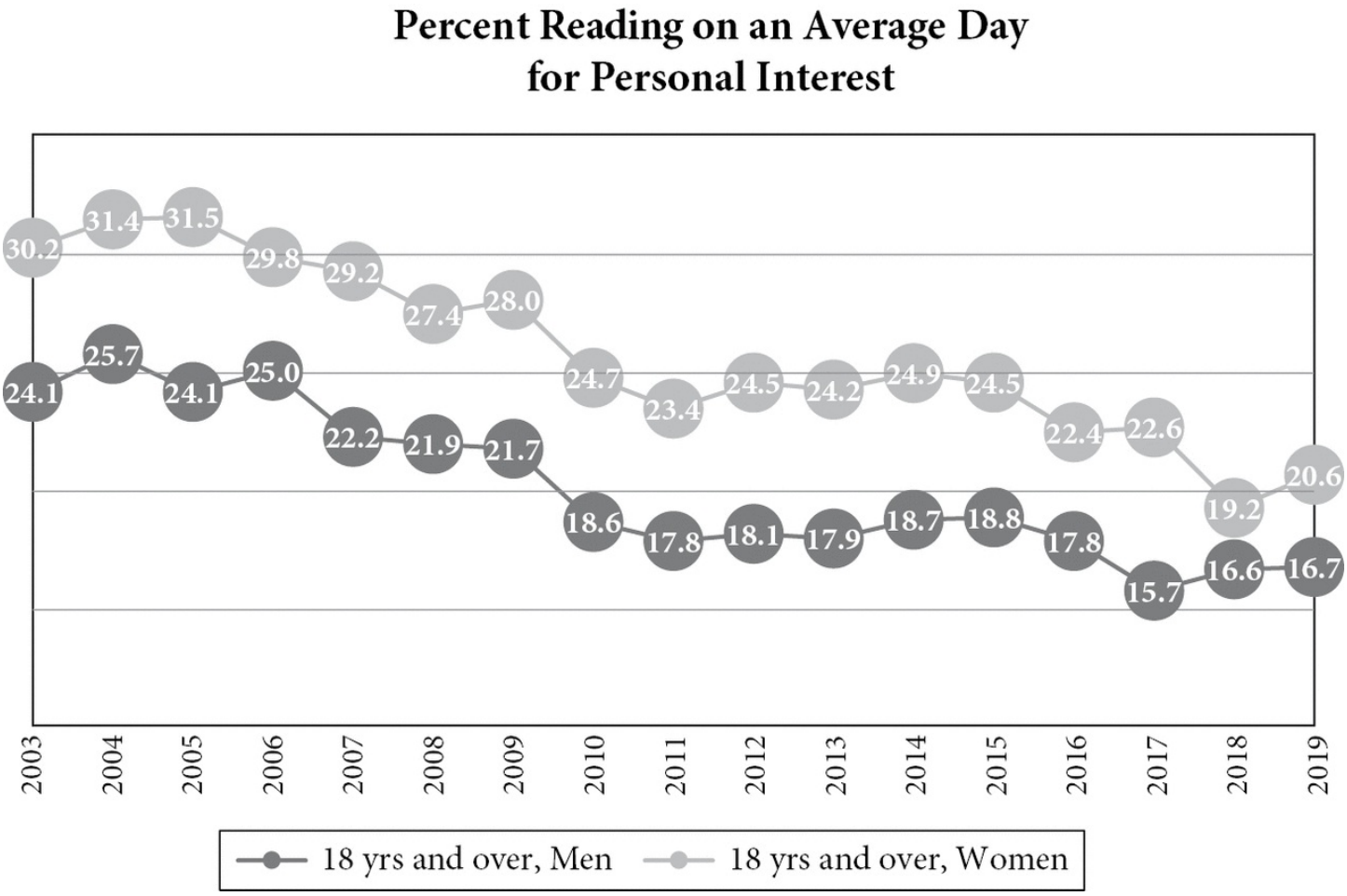


**Figure 10.3** *Source*: U.S. Bureau of Labor Statistics, American Time Use Survey

Of those who still read for personal interest, they spend on average less time reading. Figure 10.4 shows that Americans in 2019 spent less than 20 minutes a day reading for pleasure.

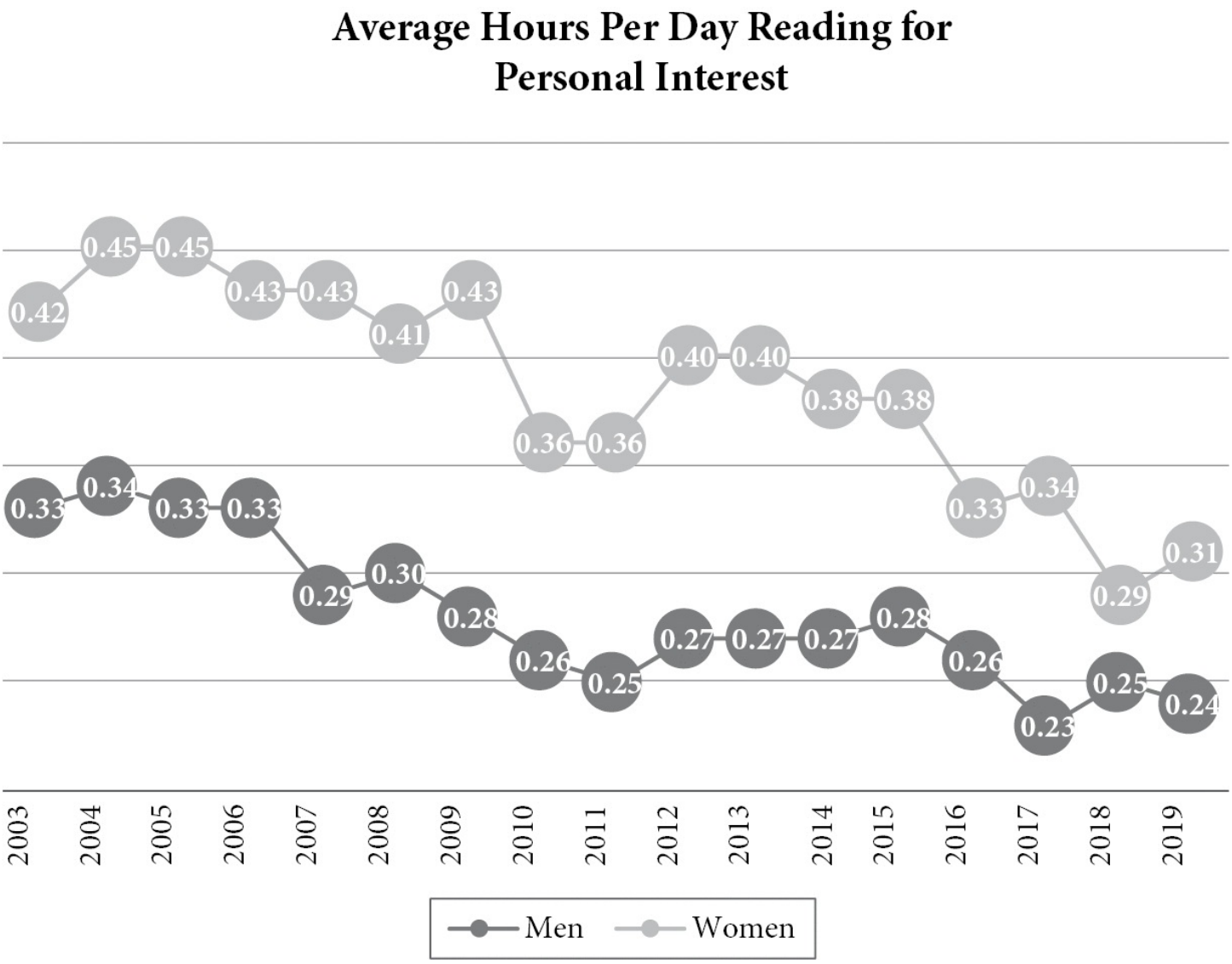


**Figure 10.4** *Source*: U.S. Bureau of Labor Statistics, American Time Use Survey

Americans between 15 and 44 years old read even less—on average for 10 minutes or less per day.[77]

So how did so many of us get hooked on our phones? “Your kid is not weak-willed because he can’t get off his phone,” one neuroscientist noted, “Your kid’s brain is being engineered to get him to stay on his phone.”[78] Facebook’s goal, among other things, is

> to increase a metric called L6/7, the fraction of people who logged in to Facebook six of the previous seven days. L6/7 is just one of myriad ways in which Facebook has measured “engagement”—the propensity of people to use its platform in any way, whether it’s by posting things, commenting on them, liking or sharing them, or just looking at them.[79]

A former employee explained that as a product manager at Facebook, "your only job is to get an extra minute. It's immoral. They don't ask where it's coming from. They can monetize a minute of activity at a certain rate. So the only metric is getting another minute."[80]

To get us to watch more YouTube videos, Google uses our data to train its YouTube recommender algorithms to sustain our attention by taking us down the rabbit hole of more disturbing content, including racist and conspiratorial rants.[81]

But is isn't just the data-opolies. As we saw in Chapter 4, millions of free websites and apps, to compete for behavioral advertising revenue, must attract and retain us by exploiting our weaknesses.[82] Yes, the choice is ultimately ours, Facebook's co-founder Chris Hughes noted, "but it doesn't feel like a choice. Facebook seeps into every corner of our lives to capture as much of our attention and data as possible and, without any alternative, we make the trade."[83]

## 5. Costs of Exploiting "the Human Brain's Attraction to Divisiveness"

"Our algorithms exploit the human brain's attraction to divisiveness." That was from an internal 2018 Facebook presentation. " 'If left unchecked,' the presentation warned, Facebook would feed users 'more and more divisive content in an effort to gain user attention & increase time on the platform.' "[84] *The Wall Street Journal* reported how a Facebook researcher and sociologist

> found extremist content thriving in more than one-third of large German political groups on the platform. Swamped with racist, conspiracy-minded and pro-Russian content, the groups were disproportionately influenced by a subset of hyperactive users, the presentation notes. Most of them were private or secret. The high number of extremist groups was concerning, the presentation says. Worse was Facebook's realization that its algorithms were responsible for their growth. The 2016 presentation states that "64% of all extremist group joins are due to our recommendation tools" and that most of the activity came from the platform's "Groups You Should Join" and "Discover" algorithms: "Our recommendation systems grow the problem."[85]

Facebook's algorithms reward inflammatory content in order to increase users' time in Facebook groups and on the social network.[86] In urging Facebook to stop the spread of hate, the American Psychological Association noted how the platform's "sharing of hate speech not only traumatizes both the intended victims and observers but may also prompt those who see it to become more prejudiced."[87]

But it is not only divisiveness. Facebook also exploits other feelings, like melancholy. Facebook's researchers found that its "users with a tendency to post or engage with melancholy content—a possible sign of depression—could easily spiral into consuming increasingly negative material that risked further worsening their mental health."[88] The Facebook team "proposed tweaking the content-ranking models for these users to stop maximizing engagement alone, so they would be shown less of the depressing stuff." So, they asked Facebook's leadership the following question: "Should we be optimizing for engagement if you find that somebody is in a vulnerable state of mind?"[89] The answer for an ethical organization is clear. But for Facebook or any other competitor in the surveillance economy, anything that reduced user engagement, "even for reasons such as not exacerbating someone's depression, led to a lot of hemming and hawing among [corporate] leadership."[90]

Now consider the implications that surveillance and manipulation have on our children's mental health. In 2016, Facebook directed its employees "to focus on winning what they viewed as a race for teen users, according to former Instagram executives."[91] They won. By 2021, over 40 percent of Instagram's users were 22 years old and younger, and about 22 million teens were logging onto Instagram in the U.S. each day. On average, teens in the U.S. spent 50% more time on Instagram than on Facebook.

Internally Facebook knew of Instagram's harmful effects on millions of teens, and also knew that some of the problems were specific to Instagram, not social media generally.[92] Among Facebook's internal findings were

"Thirty-two percent of teen girls said that when they felt bad about their bodies, Instagram made them feel worse." Facebook's researchers said in a March 2020 internal slide presentation. "Comparisons on Instagram can change how young women view and describe themselves."

"We make body image issues worse for one in three teen girls," said another internal slide from 2019.

According to another internal study, many teens in the U.S. and U.K., who recently felt that they had to create the perfect image, were not attractive, and did not have enough money, reported that these feelings originated when they were on Instagram. Over 40% of Instagram users who reported feeling "not attractive" said the feeling began on the app.

"One in five teens say that Instagram makes them feel worse about themselves, with U.K. girls the most negative."

“Teens who struggle with mental health say Instagram makes it worse.”

“Teens blame Instagram for increases in the rate of anxiety and depression,” said another Facebook slide. “This reaction was unprompted and consistent across all groups.”

Among the ways that Instagram harms their mental health is “[i]nappropriate advertisements targeted to vulnerable groups.”

Among teens who reported suicidal thoughts, 13% of British users and 6% of American users traced the desire to kill themselves to Instagram.

As Facebook internally noted, teens regularly reported wanting to spend less time on Instagram, but they “often feel ‘addicted’ and know that what they’re seeing is bad for their mental health but feel unable to stop themselves.” Indeed, Facebook researchers warned “that the Explore page, which serves users photos and videos curated by an algorithm, can send users deep into content that can be harmful.”

Here again the research was shared with top management, but the company, as internally reported, “made minimal efforts to address these issues and plays them down in public.” As a former researcher said, “We’re standing directly between people and their bonuses.”

But the surveillance economy reaches beyond teens and even preteens. The data-opolies are finding ways to engage toddlers during playdates. Most kids did not use Facebook Messenger Kids during playdates as “parents viewed the app as a way for kids to communicate with others when they’re *not* together.”[93] To increase the toddlers’ usage of its texting app during playdates, one Facebook official asked, “Is there a way to leverage playdates to drive word of hand/growth among kids?”

As FTC Commissioner Rohit Chopra noted in his agency’s third case against Google for privacy violations, this time for baiting “children using nursery rhymes, cartoons, and other kid-directed content on curated YouTube channels to feed its massively profitable behavioral advertising business”:

> Google’s behavioral advertising business model, and the technology that supports it, seems to fuel dark and disturbing content, which includes the content on YouTube Kids. Parents and medical experts are concerned about the prevalence of fear-inducing videos that influence brain development and negatively affect mental health. The long-term harmful effects of the company’s conduct are difficult to measure.[94]

The behavioral advertising business model rewards this behavior, and we bear its

costs.

## 6. Costs from “Echo Chambers” and “Filter Bubbles”

Behavioral advertising does not incentivize platforms to provide us with ideologically diverse, high-quality, responsible journalism.[95] Behavioral advertising targets people, not content. If we are drawn to YouTube videos of street fights, a behavioral advertiser will target us there. Consequently, the news we receive from the platforms that depend on behavioral advertising revenue is skewed to what will attract and maintain our attention.

Many people now receive their news from social media platforms.[96] And the news they receive shapes their views. As Australia’s competition authority noted, simply the “way in which digital platforms rank news stories can have a significant impact on the ways people arrive at and understand the importance of particular items of news.”[97]

So we are witnessing a divide between those who get their news primarily from social media versus traditional news media. As one 2020 study from Pew Research found, “Americans who primarily turn to social media for political news are less aware and knowledgeable about a wide range of events and issues in the news,” including critical facts of the COVID-19 pandemic such as the ability of hospitals across the country to treat patients or availability of testing for COVID-19.[98] On the other hand, Americans who primarily turn to social media are more likely to have heard false or unproven claims, such as the powerful elites intentionally planned the coronavirus outbreak or that 5G wireless technology weakens our immune system causing the deaths from COVID-19.

This is not by accident. To attract and addict us, platforms, under the guise of personalization, filter the information we receive based on our preferences, reduce the viewpoints, and thereby promote “echo chambers” and “filter bubbles.”[99] Filter bubbles, McNamee notes, “promote engagement, which makes them central to the business models of Facebook and Google.”[100] Facebook, for example, has sought to patent technologies to infer your personality traits from your posts and messages—“judging your degree of extroversion, openness or emotional stability, then using those characteristics to select which news stories or ads to display.”[101]

So, the behavioral advertising model rewards “echo chambers” and “filter bubbles,” while society bears the cost from the increase in conspiracy theories, rancor, polarization, and extremism. This also degrades public deliberation, a

foundation for democracies, juries, and civic engagement.

## 7. Cost of Discord

"It's no good fighting an election campaign on the facts," Cambridge Analytica's managing director told an undercover reporter, "because actually it's all about emotion."[102] To target U.S. voters and appeal to their hopes, neuroses, and fears, the political consulting firm needed to train its algorithm to predict and map personality traits. That required lots of personal data, which came from Facebook.

Political advertising is a subset of behavioral advertising. Candidates and political parties micro-target voters, based on thousands of categories, including a "user's household income, education level, profession, marital or homeownership status or the age of their children."[103] So, we see a separate arm race where political candidates, to win, resort to behavioral advertising. In 2020, two members of Congress proposed legislation to halt micro-targeting with political ads, precisely because it "fractures our open democratic debate into millions of private, unchecked silos, allowing for the spread of false promises, polarizing lies, disinformation, fake news, and voter suppression."[104]

Even if behavioral micro-targeting were banned for political ads, the platforms themselves can be weaponized to undermine democracy. The data-opolies were teaming up to fight disinformation on their social media platforms before the 2020 U.S. presidential elections.[105] But China, Russia, and Iran were already using the powerful platforms "to increase discord and to undermine confidence in our democratic process."[106] What is remarkable is that these repressive regimes' postings did not stand out. That is because, as some have observed, "Facebook created a town hall for fighting."[107]

Facebook built a machine to foster divisive, extreme positions to attract our attention and data. This negativity has spread to political parties. To ensure that their Facebook posts travel as far and fast as possible, political parties in Europe, Taiwan, and India became more negative themselves: "One [political] party's social media management team estimates that they have shifted the proportion of their posts from 50/50 positive/negative to 80% negative, explicitly as a function of the change to [Facebook's] algorithm," wrote two Facebook researchers in 2019.[108] Facebook also admitted in 2018 that the lies and hate speech on its platform helped fuel a genocidal anti-Muslim campaign in Myanmar for several years.[109] It promised to implement reforms. Nonetheless, in 2019 and 2020

Facebook and WhatsApp were spreading in India "fear-mongering" anti-Muslim content, which was contributing to the violence.[110] The company also knew that two Hindu nationalist groups with ties to India's ruling political party were among those posting the inflammatory content. The company researchers heard first-hand the concerns of "so much hatred going on" Facebook. One Muslim man told the Facebook researchers that he feared for his life. "It's scary, it's really scary."

But when Facebook's efforts to moderate content and curb misinformation, extremism, and political polarization substantially conflicted with the corporate goals of sustaining our attention and growth, Facebook's senior leadership reportedly opted for growth.[111]

Even if a data-opoly did not bait us with discord, other platforms to maximize behavioral advertising revenues would. One 2018 Harvard study, for example, found that YouTube at that time lumped "Fox News and GOP accounts into the same community as conspiracy theory channels like Alex Jones." Thus, if you are a conservative on YouTube, "you're only one or two clicks away from extreme far-right channels, conspiracy theories, and radicalizing content."[112] Google has promised to crack down on some of these conspiracy and extremist channels. However, its recommendation algorithm, which drives over 70% of the YouTube videos watched, continued to point viewers to white supremacist videos, hate speech, and other disturbing content.[113]

Unsurprisingly, YouTube and Facebook groups helped spread disinformation about the presidential 2020 elections, leading up to a subset of Trump supporters storming the U.S. Capitol.[114] The source of the problem is not the data-opolies per se, but their behavioral advertising business model. As Hany Farid, a professor at the University of California, Berkeley noted, "When you're in the business of maximizing engagement, you're not interested in truth. You're not interested in harm, divisiveness, conspiracy. In fact, those are your friends."[115]

## 8. Impact on Traditional Media

The marketplace of ideas cannot function well when conspiracy theories, disinformation, and clickbait crowd out responsible journalism. One study examined the dispersion of all verified true and false news stories distributed on Twitter between 2006 to 2017.[116] In reviewing nearly 126,000 stories tweeted by about 3 million people over 4.5 million times, the study found that "falsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all

categories of information."[117] Falsehoods "were 70% more likely to be retweeted than the truth," the study found "even when controlling for the account age, activity level, and number of followers and followees of the original tweeter, as well as whether the original tweeter was a verified user."

So another cost of behavioral advertising is its impact on traditional media that cannot effectively compete in this ecosystem. False stories are likelier to be rewarded online with attention (and being reshared). Put simply, companies profit from this disinformation when it induces us to spend more time on their platforms and within their behavioral advertising network. That means less time (and less advertising money) for local newspapers, radio stations, and television stations.

But even when the traditional media turn to behavioral advertising, they, unlike the data-opolies, lack the surveillance apparatus to effectively capture significantly more revenues. Google and Facebook accounted for 48% of local ad revenues in 2018 in the United States. By 2018, Google's *local* ad revenues ($19 billion) had already surpassed the ad revenues for all 11,044 commercial radio stations in the United States.[118] By 2020, Google was "projected to exceed the combined ad revenue of all TV and radio stations in the [United States] by over $8 billion."[119]

So how did that happen? As the former chair of the Federal Communications Commission observed, "This is not because they are a part of the local community, but because their ubiquitous collection allows them to know more about the members of the local community than even the neighbors."[120]

With less advertising revenue, traditional news media are laying off journalists.[121] The total number of newsroom employees in the newspaper sector in 2018 was 37,900, half the level from 2006 (74,410).[122] The 2020 pandemic accelerated the layoffs, with 60 local newsrooms closing.[123] Connecticut's *Hartford Courant* closed its printing plant, then its news office, and its remaining employees began work remotely.[124] Fewer journalists mean less investigative journalism and fewer reporters covering city hall and the state capitol.[125] As of 2020, half of all U.S. counties have only one local newspaper, "usually a weekly," and 225 counties are what the University of North Carolina calls "news deserts," without any local newspaper.[126]

And when the local newspaper closes, corruption and waste will likely increase. One study, for example, found that newspaper closures had a significantly adverse impact on municipal borrowing costs. This effect was

causal and not driven by underlying economic conditions. Overall, the Internet did not fill the void. As the study concluded, "local newspapers hold their governments accountable, keeping municipal borrowing costs low and ultimately saving local taxpayers money."[127]

Newspapers are beset with many other problems (such as hedge fund owners who further degrade the newspapers' quality to extract more money from them). But behavioral advertising does not reward quality investigative journalism; instead, it's killing it.

## 9. Costs of Behavioral Advertising in Weakening Trust in Markets

For online markets to deliver their benefits, we must trust firms and their use of our data. But as technology evolves and more personal data is collected, we are increasingly concerned that companies are using our data for their benefit, not ours.[128] About 81% of American in 2019 believed "that the potential risks they face because of data collection by companies outweigh the benefits"; 79% were concerned about the way companies were using their data, and 81% felt they had "little or no control over how these entities use their personal information."[129] Markets are built on trust, and many people do not trust the way companies use their data.[130]

The distrust from behavioral advertising imposes an actual economic cost when consumers choose not "to share their data, to limit their data sharing with companies, or even to lie when providing information."[131] When individuals forgo the services they otherwise would have used if privacy competition were robust, this loss represents what economists call a deadweight welfare loss. In other words, as distrust increases, society overall becomes worse off.[132]

Thus, privacy and data protection, besides safeguarding a fundamental, inalienable right, can "build trust in online markets"[133] and "empower consumers to make more informed choices about how their data is processed."[134] Behavioral advertising's surveillance and profiling erode that trust.

## 10. Costs to Democracy

The loss of trust and increase in rancor have already taken a toll on democracies. But at a more fundamental level, surveillance capitalism is incompatible with democracy.[135] Economic power translates to political power, which can be wielded against disfavored voices and opponents.[136]

First are the costs of *government capture*. The fewer the number of firms

controlling the personal data and surveillance apparatus, the greater the potential risk that a government will "capture" the firm. Companies need things from governments; governments often want access to data. With only a few firms, this can increase their likelihood of secretly cooperating with the government to provide access to data.[137] China, for example, relies on its data-opolies to better monitor its population,[138] which prompted security concerns about the video platform TikTok.[139]

But even without data-opolies, the government can easily tap into the personal data amassed for the surveillance economy. Ordinarily, the government needs a search warrant, supported by probable cause, to track Americans through their smartphones.[140] Why? Because the Fourth Amendment of the U.S. Constitution seeks to secure "the privacies of life" against "arbitrary power."[141]

So, if the Constitution seeks "to place obstacles in the way of a too permeating police surveillance,"[142] how then did the U.S. Department of Homeland Security obtain millions of Americans' location data without any warrant? How did they track down and arrest undocumented immigrants at the U.S.-Mexico border? The Trump administration tapped into the surveillance economy. It purchased access to a commercially-available database that maps the movements of millions of cell phones in America.[143] How did the marketers get that location data? Most likely from the apps on our phones.[144]

As the Supreme Court noted, our geolocation data from our smartphones provide anyone with this data with "near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[145] So by 2021, approximately 62% of the world's population have these ankle monitors, which many governments can use to monitor dissidents at home or abroad.[146]

Next is the risk of *covert surveillance*. Even if the government cannot capture the surveillance data, the rich data-trove increases a government's incentive to circumvent the company's privacy protections to tap into the personal data. So, when the government cannot strike a deal to access our data directly, it can do so covertly.[147] One example, according to WikiLeaks, is the Central Intelligence Agency's "Weeping Angel" program. The CIA hacked smart televisions, transforming them into covert microphones. The CIA could also remotely hack and control popular smartphones, which could be instructed to send the CIA "the user's geolocation, audio and text communications as well as covertly activate the phone's camera and microphone."[148]

## F. Reflections

As legal scholars Lina M. Khan and David E. Pozen note, "experts debate whether and under what conditions online behavioral advertising actually enhances consumer welfare."[149] Amassing the volume and variety of personal data can potentially lower advertising costs in targeting the right customers with the right message and product at the right time. Lower advertising costs could conceivably benefit consumers with lower retail prices. Google, for example, points out that "online advertising prices in the U.S. have fallen more than 40% since 2010."[150]

But as Phaedrus observed, "Things are not always what they seem; the first appearance deceives many; the intelligence of a few perceives what has been carefully hidden." As one industry executive testified before Congress, some of this 40% decline in online advertising prices is attributable to the industry-wide shift to mobile advertising, which is cheaper than ads on desktop computers. Moreover, the quality of advertising may be deteriorating, in that advertisers are paying less but are also getting less.[151]

But even if behavioral ads now cost less, that is only a small part of the equation. Behavioral advertising is no longer about divining our intentions. It is about driving our behavior and emotions—whether to vote and for whom, what to think, how to feel, and what to buy. Consequently, even if behavioral advertising provides some quantifiable short-term gains, policymakers must avoid the trap of confusing what is measurable with what is important. The surveillance and manipulation apparatus can impose far greater costs and risks to our economy, privacy, autonomy, well-being, and democracy. That is why we need to pull the plug on the surveillance economy.

---

1 David Temkin, Director of Product Management, Ads Privacy and Trust, *Charting A Course Towards A More Privacy-First Web*, Google (Mar. 3, 2021), https://blog.google/products/ads-commerce/a-more-privacy-first-web/.

2 Facebook, Inc., Third Quarter 2021 Results Conference Call at 5 (Oct. 25, 2021), https://s21.q4cdn.com/399680738/files/doc_financials/2021/q3/FB-Q3-2021-Earnings-Call-Transcript.pdf.

3 Press Release, European Data Protection Supervisor, EDPS Opinions on the Digital Services Act and the Digital Markets Act (Feb. 10, 2021), https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opinions-digital-services-act-and-

digital_en [https://perma.cc/4AQ2-8AXG].

4 Facebook, https://www.facebook.com/adpreferences/ad_settings ("If you turn off this setting, we'll still show you ads on Facebook, but they may not be as relevant to you."); Google Safety Center, *Ads That Respect Your Privacy*, https://safety.google/privacy/ads-and-data/ (last visited Mar. 12, 2021) [https://perma.cc/DXU9-468C] ("You can also turn off personalized ads altogether. You'll still see ads, but they'll most likely be less relevant."); Apple, *Control Personalized Ads on the App Store, Apple News, and Stocks* (Jan. 7, 2021), https://support.apple.com/en-us/HT202074 [https://perma.cc/283Q-S8XT] ("If you don't want to receive personalized ads, you can choose to turn off the Personalized Ads setting on your iPhone, iPad and iPod touch, and Mac. This may not decrease the number of ads you receive, but the ads may be less relevant to you."); Amazon, *Interest-Based Ads*, https://www.amazon.com/b?node=5160028011 (last visited Mar. 12, 2021) [https://perma.cc/J58V-CC7N] ("Amazon offers you choices about receiving interest-based ads from us. You can choose not to receive interest-based ads from Amazon. You will still see ads but they will not be personalized.").

5 Cade Metz, *The Porn Business Isn't Anything like You Think It Is*, Wired (Oct. 15, 2015), https://www.wired.com/2015/10/the-porn-business-isnt-anything-like-you-think-it-is/ [https://perma.cc/7CTS-R9FH].

6 *Id.*

7 Temkin, *supra* note 1.

8 Lisa Farman, Maria Leonora (Nori) Comello, & Jeffrey R. Edwards, *Are Consumers Put Off by Retargeted Ads on Social Media? Evidence for Perceptions of Marketing Surveillance and Decreased Ad Effectiveness*, 64 J. Broad. & Elec. Media 298, 306 (2020), https://doi.org/10.1080/08838151.2020.1767292.

9 *Id.*; Chang-Dae Ham, *Exploring How Consumers Cope with Online Behavioral Advertising*, 36 Int'l J. Advert. 632, https://doi.org/10.1080/02650487.2016.1239878.

10 Shoshana Zuboff, The Age of Surveillance Capitalism 281 (2019) (quoting Chris Wylie).

16 Facebook, The Value of Personalized Ads to a Thriving App Ecosystem (June 18, 2020), https://developers.facebook.com/blog/post/2020/06/18/value-of-personalized-ads-thriving-app-ecosystem/ (stating that it "ran a test that constrained delivery to just mobile app install ads for a small portion of Audience Network Traffic, then compared personalized ranking to non-personalized ranking. We observed more than a 50% drop in publisher revenue between these two treatments, with no changes made to targeting.").

17 *See, e.g.*, Burt Neuborne, *Toward A Democracy-Centered Reading of the First Amendment*, 93 Nw. U. L. Rev. 1055, 1062–63 (1999) ("uncontrolled campaign spending often resembles a classic arms race spiral, where opposing participants become trapped in a prisoners' dilemma that can only be resolved by collective action").

18 Robert L. Steiner, *Double Standards in the Regulation of Toy Advertising*, 56 U. Cin. L. Rev. 1259, 1264 (1988).

19 FTC v. Winsted Hosiery Co., 258 U.S. 483, 494 (1922) ("The honest manufacturer's business may suffer, not merely through a competitor's deceiving his direct customer, the

retailer, but also through the competitor's putting into the hands of the retailer an unlawful instrument, which enables the retailer to increase his own sales of the dishonest goods, thereby lessening the market for the honest product."); George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. Econ. 488, 495 (1970) (noting that the cost of dishonesty includes "loss incurred from driving legitimate business out of existence"); Maurice E. Stucke, *How Do (and Should) Competition Authorities Treat a Dominant Firm's Deception?*, 63 SMU L. Rev. 1069, 1073–74 (2010).

20 16 C.F.R. § 312.2. Absent parental consent, companies cannot use any persistent identifiers to amass a profile on a specific individual or for behavioral advertising. As the FTC notes, "The primary goal of COPPA is to place parents in control over what information is collected from their young children online." Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* (July 2020) https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 [https://perma.cc/L2H5-92VZ]. One problem is that companies can circumvent COPPA by claiming that their commercial websites and online services are not "directed" to children under 13 years old, and that they did not have actual knowledge that they are collecting, using, or disclosing personal information from children under 13 years old.

21 Facebook IQ: Digital Research and Insights, *Gen Z: Getting to Know the 'Me Is We' Generation* (Oct. 22, 2019), https://www.facebook.com/business/news/insights/generation-z.

22 Temkin, *supra* note 1.

11 Gerald Chait, *Half the Money I Spend on Advertising Is Wasted; the Trouble Is I Don't Know Which Half*, B2B Marketing (Mar. 18, 2015), https://www.b2bmarketing.net/en-gb/resources/blog/half-money-i-spend-advertising-wasted-trouble-i-dont-know-which-half [https://perma.cc/F4W5-QTFU].

12 Wall Street Journal, General Advertising Rate Card, Effective January 1, 2018, https://images.dowjones.com/wp-content/uploads/sites/183/2018/07/13141526/WSJM-2066_U.S._general_advertising_rate_card-2018-v7.pdf [https://perma.cc/94KH-UZTV].

13 Facebook, Speaking Up for Small Businesses, Update on Feb. 1 at 7AM PT, https://www.facebook.com/business/news/ios-14-apple-privacy-update-impacts-small-business-ads.

14 Yan Carrière-Swallow & Vikram Haksar, *The Economics and Implications of Data: An Integrated Perspective*, International Monetary Fund Policy Paper No. 19/16 (Sept. 2019), https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596 at 11 (noting the difficulty in "[a]ssessing how valuable personal data can be" even for "the agents that have direct incentives to do so," and how "an incipient literature quantifying the effectiveness of this practice suggests that, although the gains from targeting ads do appear to be statistically significant, their causal impact on sales appears to be economically modest and inferior to the outlays spent on targeting"); *see also* Alessandro Acquisti, Curtis Taylor, & Liad Wagman, *The Economics of Privacy*, 54 J. Econ. Lit. 442, 464 (2016), http://dx.doi.org/10.1257/jel.54.2.442; Anthony Samuel et al., *Programmatic*

*Advertising: An Exegesis of Consumer Concerns*, 116 Comput. Hum. Behav. 106657, at § 2.1.1 (2021), https://doi.org/10.1016/j.chb.2020.106657 (noting from survey of literature that programmatic advertising "is not transparent in terms of its cost or consumer viewable effectiveness"); Natasha Lomas, *The Case Against Behavioral Advertising Is Stacking Up*, TechCrunch (Jan. 20, 2019), https://techcrunch.com/2019/01/20/dont-be-creepy/ [https://perma.cc/BER7-YQSF].

15 Samuel et al., *supra* note 14, at § 5 (noting the risk of reduced purchase intention and purposeful contrariance leading to resentment and activism, and for those positing programmatic advertising "as a functional panacea, customer elenchus or refutation also needs to be considered").

23 *Hearing on Stacking the Tech: Has Google Harmed Competition in Online Advertising? Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. (Sept. 15, 2020) (Written Testimony of Donald Harrison, President, Global Partnerships, Corporate Development, and Area 120, Google LLC), https://www.judiciary.senate.gov/download/09/15/2020/harrison-testimony [hereinafter Harrison Testimony] (testifying that "[t]he free and open internet we all enjoy is made possible by advertising. Without it, websites would be forced to adopt subscription models—putting their content behind paywalls—or shut down their operations entirely. This would harm consumers with higher prices and reduced choice online.").

24 Harrison Testimony, *supra* note 23.

25 Under Google's 2019 policy, "political ads can only be targeted based on users' age, gender, and location at the postal-code level. Political advertisers will also still be able to display ads based on the content of the page a user is viewing. Advertisers would no longer be able to target political ads based on users' interests inferred from browsing or search history." Patience Haggin, *Google to Restrict Political Ad Targeting on Its Platforms*, Wall St. J. (Nov. 20, 2019), https://www.wsj.com/articles/google-to-restrict-political-ad-targeting-on-its-platforms-11574293253. More generally, the CMA heard from its inquiry that behavioral advertising "is more important in display than in search advertising—because in search, the most valuable data for selecting which ads to show is the search query itself, so that contextual advertising performs very well without much need for additional consumer data." UK Competition & Markets Authority, Online Platforms and Digital Advertising Market Study: Market Study Final Report ¶ 4.33 (July 1, 2020), https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digit [https://perma.cc/DA5V-RHA5] [hereinafter CMA Final Report].

26 DuckDuckGo, *DuckDuckGo Help Pages: Advertising and Affiliates*, https://help.duckduckgo.com/duckduckgo-help-pages/company/advertising-and-affiliates/ (last visited Mar. 12, 2021) [https://perma.cc/M7J5-2RBE].

27 564 U.S. 552 (2011) (6–3).

28 *Sorrell*, 564 U.S. at 572.

29 *Sorrell*, 564 U.S. at 573.

30 *Id.* (citing Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §

1320d–2; 45 C.F.R. pts. 160 and 164 (2010)).

31 Felix T. Wu, *The Commercial Difference*, 58 Wm. & Mary L. Rev. 2005, 2060 (2017).

32 Australian Competition and Consumer Commission, Digital Platforms Inquiry—Final Report at 131 (2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report [https://perma.cc/M36S-YQJ4] [hereinafter ACCC Final Report] (noting Business Chamber submits that in response to a survey of Australian Business Chamber members, that 71% had used digital platforms to advertise and indicated online advertising had positively affected their business; 62% indicated that online advertising had increased customers; 43% indicated it had increased sales; and 34% indicated it helped reduce costs). Behavioral advertising could lower consumers' search costs by providing them relevant ads. Yan Lau, Fed. Trade Comm'n, A Brief Primer on the Economics of Targeted Advertising at 5-6 (Jan. 2020), https://www.ftc.gov/system/files/documents/reports/brief-primer-economics-targeted-advertising/economic_issues_paper_-_economics_of_targeted_advertising.pdf. But that assumes rational consumers with preexisting and stable preferences and strong willpower who are searching for products that meet their specifications. It is less relevant when behavioral advertising can create and fulfill demand. *See, e.g.*, Complaint ¶ 28, United States v. Google, No. 1:20-cv-03010 (D.D.C. Oct. 20, 2020), https://www.justice.gov/opa/press-release/file/1328941/download (alleging that marketers and advertisers "typically refer to a 'purchase funnel' or 'customer acquisition funnel' to describe the average consumer's various states of mind leading up to a potential purchase, and the type of advertising most effective at each state").

33 Carrière-Swallow & Haksar, *supra* note 14, at 11 ("Acquiring data may thus generate considerable commercial (private) value for a data collector, but without necessarily increasing social welfare. If a firm enjoys market power, then gaining data about their customers' personal characteristics—say, their income or wealth—can allow them to implement price discrimination strategies that extract the consumer's surplus.").

34 Andrew Hutchinson, *Facebook Releases New Research into How People Respond After a Break-Up*, Social Media Today (Feb. 4, 2017), https://www.socialmediatoday.com/social-business/facebook-releases-new-research-how-people-respond-after-break.

35 Samuel et al., *supra* note 14, at 4.

36 Sophie Kleber, *Three Ways AI Is Getting More Emotional*, *in* Artificial Intelligence: The Insights You Need From Harvard Business Review 137 (Thomas H. Davenport et al., eds. 2019).

37 Paul Barba, *Emotion Detection Is a Hot Ask in Marketing, But the Tech Just Isn't Ready Yet*, Venture Beat (May 2, 2020), https://venturebeat.com/2020/05/02/emotion-detection-is-a-hot-ask-in-marketing-but-the-tech-just-isnt-ready-yet/ [https://perma.cc/HJ6R-NX6V].

38 *Id.*

39 *Facebook's Emotion Tech: Patents Show New Ways For Detecting And Responding To Users' Feelings*, CB Insights (June 1, 2017), https://www.cbinsights.com/research/facebook-emotion-patents-analysis/ (describing Patent Application Publication No.:US2015/0242679A1 (Publication Date: Aug. 27, 2015), https://patentimages.storage.googleapis.com/2d/e4/fb/6cd2fb81899dcd/US20150242679A1.p

40 *Facebook's Emotion Tech*, *supra* note 41.

41 *Id.*

42 US Patent for Emotional/cognitive State Presentation (Patent # 10,762,429), https://patents.justia.com/patent/10762429.

43 *Id.*

44 T.S. Eliot, The Love Song of J. Alfred Prufrock, 6 Poetry 130 (June 1915).

45 *See, e.g.*, Mark Chevillet on Hands-free Communication Without Saying a word, ApplySci Silicon Valley (March 3, 2020), https://youtu.be/-lmAJUIo1Mg; Facebook, *Imagining a New Interface: Hands-free Communication Without Saying a Word* (March 30, 2020), https://tech.fb.com/imagining-a-new-interface-hands-free-communication-without-saying-a-word/; Robin Marks, "Neuroprosthesis" Restores Words to Man with Paralysis: Technology Could Lead to More Natural Communication for People Who Have Suffered Speech Loss, University of California San Francisco (July 14, 2021), https://www.ucsf.edu/news/2021/07/420946/neuroprosthesis-restores-words-man-paralysis?utm_source=ucsf_fb&utm_medium=fb&utm_campaign=2021_neuroprosthesisresults.

46 Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, 2014 Wis. L. Rev. 861, 887 (citing Daniel J. Solove, Understanding Privacy 174–79 (2008)).

47 President's Comm'n on Law Enf't & Admin. of Justice, The Challenge of Crime in a Free Society 202 (1967), https://www.ncjrs.gov/pdffiles1/nij/42.pdf [https://perma.cc/L9ER-Q4AM].

48 *See, e.g.*, Facebook, Inc., 2017 Form 10-K at 13 (https://www.sec.gov/Archives/edgar/data/1326801/000132680118000009/fb-12312017x10k.htm) ("As a result of our prominence, the size of our user base, and the types and volume of personal data on our systems, we believe that we are a particularly attractive target for such [data] breaches and attacks.").

49 Chris Jay Hoofnagle, Federal Trade Commission Privacy Law and Policy 332 (2016) (*quoting* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010)).

50 Acquisti et al., *supra* note 14, at 476 (noting that while firms should be induced by strict data breach disclosure laws to secure their customers' data, several studies that examine the financial impact of such disclosures on firms have come up with "mixed and primarily mild results").

51 Daniel Ringbeck et al., Toward Personalized Online Shopping: Predicting Personality Traits Based on Online Shopping Behavior (June 18, 2019), http://dx.doi.org/10.2139/ssrn.3406297.

52 *See* Ariel Ezrachi & Maurice E. Stucke, Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy (2016) (collecting some of the research).

53 *See, e.g.*, Oren Bar-Gill, *Algorithmic Price Discrimination: When Demand Is a Function of Both Preferences and (Mis)Perceptions*, 86 U. Chi. L. Rev. 217 (2019); Etye Steinberg, *Big Data and Personalized Pricing*, 30 Bus. Ethics Q. 97, https://doi.org/10.1017/beq.2019.19 (arguing that what is wrong with using big data to

personalize prices is that it unfairly undermines consumers' ability to benefit from the market, which is the very point of having a market).

54 Ringbeck et al., *supra* note 54.

55 *60 Minutes: What Is "Brain Hacking"? Tech Insiders on Why You Should Care* (CBS television broadcast Apr. 9, 2017), https://www.cbsnews.com/news/brain-hacking-tech-insiders-60-minutes/ [https://perma.cc/9KWS-B29A].

56 *Time per Day Spent Using the Internet*, Digital Information World, https://www.digitalinformationworld.com/2019/02/internet-users-spend-more-than-a-quarter-of-their-lives-online.html#postimages-1 (last visited Mar. 13, 2021) [https://perma.cc/DU38-C9GF].

57 James B. Stewart, *Facebook Has 50 Minutes of Your Time Each Day. It Wants More*, N.Y. Times (May 5, 2016), https://nyti.ms/1TpIVI7 https://perma.cc/DC3P-78CA].

58 Majority Staff of H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial and Administrative Law, Report and Recommendations: Investigation of Competition in Digital Markets at 138 (2020), https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429 [https://perma.cc/29LN-L4BL] [hereinafter House Report].

59 H. Tankovska, *Social Media—Statistics & Facts*, Statista (Feb. 25, 2021), https://www.statista.com/topics/1164/social-networks/ [https://perma.cc/AMQ9-CJ9L].

60 Katherine Buchholz, *Where Do People Spend the Most Time on Social Media?*, Statista (Nov. 17, 2020), https://www.statista.com/chart/18983/time-spent-on-social-media/ [https://perma.cc/6CZZ-L2QQ].

61 Georgia Wells, *Google Rides Global Ad Recovery to Record Revenue*, Wall St. J. (Feb. 2, 2021), https://www.wsj.com/articles/google-alphabet-googl-4q-earnings-report-2020-11612236441.

62 H. Tankovska, *Percentage of U.S. Internet Users Who Use YouTube as of 3rd Quarter 2020, by Age Group*, Statista (Jan. 26, 2021), https://www.statista.com/statistics/296227/us-youtube-reach-age-gender/ [https://perma.cc/SVE6-777Q].

63 *Id.*

64 *YouTube for Press*, YouTube Official Blog, https://blog.youtube/press/ (last visited Mar. 13, 2021) [https://perma.cc/LN83-AM4M].

65 *Id.*

66 CMA Final Report ¶ 2.15; *see also* House Report at 92 (noting that according to "Facebook's internal market data, YouTube and Facebook's family of products were by far the most popular social media sites by Monthly Active Persons (MAP) as of December 2019").

67 CMA Final Report ¶ 2.16.

68 Chris Hughes, *It's Time to Break Up Facebook*, N.Y. Times (May 9, 2019), https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html.

69 Cecilie Schou Andreassen & Ståle Pallesen, *Social Network Site Addiction—An Overview*, 20 Current Pharm. Design 4053 (2014).

70 Gustavo Ferreira da Veiga et al., *Emerging Adults and Facebook Use: The Validation of the Bergen Facebook Addiction Scale (BFAS)*, 17 Int'l J. Mental Health & Addiction 279 (2018), https://doi.org/10.1007/s11469-018-0018-2; Julia Brailovskaia & Jürgen Margraf, *Facebook Addiction Disorder (FAD) among German Students—a Longitudinal Approach*, 12 PLoS One e0189719 (2017), https://doi.org/10.1371/journal.pone.0189719 (noting how Facebook use is very attractive for narcissists, and could make them especially vulnerable to Facebook Addiction Disorder).

71 Daria J. Kuss & Mark D. Griffiths, *Social Networking Sites and Addiction: Ten Lessons Learned*, 14 Int'l J. Env't Rsch. & Pub. Health 311 (2017); Andreassen & Pallesen, *supra* note 72; *see also* Brailovskaia, *supra* note 73 (defining Facebook Addiction Disorder through six typical characteristics of addiction disorders: "salience (e.g., permanent thinking of Facebook use), tolerance (e.g., requiring increasing time on Facebook to achieve previous positive using effect), mood modification (e.g., mood improvement by Facebook use), relapse (reverting to earlier use pattern after ineffective attempts to reduce Facebook use), withdrawal symptoms (e.g., becoming nervous without possibility to use Facebook), and conflict (e.g., interpersonal problems caused by intensive Facebook use)").

72 Andreassen & Pallesen, *supra* note 72.

73 Georgia Wells et al., *Is Facebook Bad for You? It Is for About 360 Million Users, Company Surveys Suggest*, Wall St. J. (Nov. 5, 2021).

74 *Id*.

75 *Id.*

76 For the impact of smartphones on children, *see* Jean M. Twenge, iGen: Why Today's Super-Connected Kids Are Growing Up Less Rebellious, More Tolerant, Less Happy–and Completely Unprepared for Adulthood (2017).

77 News Release, U.S. Dep't of Labor, Bureau of Labor Statistics, American Time Use Survey—2019 Results (June 25, 2020), https://www.bls.gov/news.release/pdf/atus.pdf [https://perma.cc/ERL6-QNDJ].

78 Haley Sweetland Edwards, *You're Addicted to Your Smartphone. This Company Thinks It Can Change That*, Time (April 12, 2018), https://time.com/5237434/youre-addicted-to-your-smartphone-this-company-thinks-it-can-change-that/.

79 Karen Hao, *How Facebook Got Addicted to Spreading Misinformation: The Company's AI Algorithms Gave It an Insatiable Habit for Lies and Hate Speech. Now the Man Who Built Them Can't Fix the Problem*, MIT Tech. Rev. (Mar. 11, 2021).

80 House Report at 135.

81 Zeynep Tufekci, *YouTube, the Great Radicalizer*, N.Y. Times (Mar. 10, 2018), https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html [https://perma.cc/7CC2-R8ZE]; Dissenting Statement of Commissioner Rohit Chopra, *In re Google LLC and YouTube, LLC* Commission File No. 1723083 (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtu [https://perma.cc/PNM6-LETP].

82 Tristan Harris, *How Technology Is Hijacking Your Mind—From a Magician and*

*Google Design Ethicist*, Medium (May 18, 2016), https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3 [https://perma.cc/4E44-L2JW]; Edwards, *supra* note 81.

83 Hughes, *supra* note 71.

84 Jeff Horwitz & Deepa Seetharaman, *Facebook Executives Shut Down Efforts to Make the Site Less Divisive*, Wall St. J. (May 26, 2020), https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499.

85 *Id.*

86 Hao, *supra* note 82; Wells et al., *Is Facebook Bad for You?*, *supra* note 77.

87 Letter from American Psychological Association to Mark Zuckerberg, Founder and Chief Executive Officer, Facebook (Aug. 2, 2020), https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-20200729-SD015.pdf [https://perma.cc/H9ZB-7V7Q].

88 Hao, *supra* note 82.

89 *Id.* (noting that a "Facebook spokesperson said she could not find documentation for this proposal").

90 *Id.*

91 Georgia Wells et al., Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show - Its own in-depth research shows a significant teen mental-health issue that Facebook plays down in public, Wall St. J. (Sept. 14, 2021), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=article_inline.

92 *Id.*

93 Georgia Wells & Jeff Horwitz, *Facebook's Effort to Attract Preteens Goes Beyond Instagram Kids, Documents Show*, Wall St. J. (Sept. 28, 2021).

94 Fed. Trade Comm'n, In re Google LLC And YouTube, LLC (FTC File No. 1723083), Dissenting Statement of Commissioner Rohit Chopra Regarding YouTube (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtu [https://perma.cc/48Y2-PS98]; Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 Berkeley Bus. L.J. 39 (2019), https://lawcat.berkeley.edu/record/1128876?ln=en (empirical study of social network market history concluding that "Facebook's ability today to extract surveillance in its exchange with consumers merely reflects an ability to extract monopoly rents from consumers that contradicts their own welfare").

95 Due to pervasive psychological confirmation biases, users are unlikely to want to hear both the conservative and liberal slant for every news story. *See* Andrea M. Matwyshyn, *The Law of the Zebra*, 28 Berkeley Tech. L.J. 155, 210 (2013) ("Particularly when the topic is an emotionally-charged or threatening issue, confirmation bias is a common occurrence.").

96 Elsa Shearer & Amy Mitchell, *News Use Across Social Media Platforms in 2020*, Pew Res. Center (Jan. 12, 2021), https://www.journalism.org/2021/01/12/news-use-across-social-media-platforms-in-2020/ [https://perma.cc/Z35Y-44RM]; Elisa Shearer & Katerina Eva

Matsa, *News Use Across Social Media Platforms 2018*, Pew Res. Center (Sept. 10, 2018), https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/ [https://perma.cc/8D5J-SCN4]; Elisa Shearer & Jeffrey Gottfried, *News Use Across Social Media Platforms 2017*, Pew Res. Center (Sept. 7, 2017), http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/ [https://perma.cc/PB2B-VHBP].

97 ACCC Final Report at 172.

98 Amy Mitchell et al., *Americans Who Mainly Get Their News on Social Media Are Less Engaged, Less Knowledgeable*, Pew Res. Center (July 30, 2020), https://www.journalism.org/2020/07/30/americans-who-mainly-get-their-news-on-social-media-are-less-engaged-less-knowledgeable/ [https://perma.cc/V7JJ-65XP].

99 ACCC Final Report at 22; Eytan Bakshy et al., *Exposure to Ideologically Diverse News and Opinion on Facebook*, 348 Science 1130, 1130 (2015) (observing from study of over 10 million Facebook users "substantial polarization among hard [news] content shared by users, with the most frequently shared links clearly aligned with largely liberal or conservative populations" and how individual choice further substantially limited users' exposure to ideologically cross-cutting content); Org. for Econ. Co-operation & Dev., *Algorithms and Collusion: Note by the European Union*, at 2, DAF/COMP/WD(2017)12 (June 14, 2017), https://one.oecd.org/document/DAF/COMP/WD(2017)12/en/pdf (noting that when it comes to recommending newspaper articles, personalization can limit the range of views that consumers are exposed to, which is the so-called "filter bubble" or "echo chamber" phenomenon); Sofia Grafanaki, *Drowning in Big Data: Abundance of Choice, Scarcity of Attention and the Personalization Trap, A Case for Regulation*, 24 Rich. J.L. & Tech. 1, 31 (2017) (discussing how most personalization algorithms "are prone to produce such filter bubbles, as their goal is to show users content that will be the most relevant and engaging," that Facebook "gives each post a relevancy score for each user, measuring whether and how that user is likely to interact with (i.e. click, like, share, and comment on) the specific post").

100 Roger McNamee, Zucked: Waking Up to the Facebook Catastrophe 87 (2019); *see also* Hao, *supra* note 82 (noting how a "former Facebook AI researcher who joined in 2018 says he and his team conducted 'study after study' confirming the same basic idea: models that maximize engagement increase polarization. They could easily track how strongly users agreed or disagreed on different issues, what content they liked to engage with, and how their stances changed as a result. Regardless of the issue, the models learned to feed users increasingly extreme viewpoints. 'Over time they measurably become more polarized,' he says.").

101 Sahil Chinoy, *What 7 Creepy Patents Reveal About Facebook*, N.Y. Times (June 21, 2018), https://nyti.ms/2MGqm7T [https://perma.cc/2NGK-26LX].

102 Justin Carissimo, *Cambridge Analytica CEO Alexander Nix Describes "Shadow" Election Tactics*, CBS News (Mar. 19, 2018), https://www.cbsnews.com/news/cambridge-analytica-ceo-alexander-nix-data-firm-describes-shadow-election-tactics-2018-03-19/ [https://perma.cc/QDP3-CVL2].

103 Haggin, *supra* note 24; *see also* Sam Schechner et al., *Political Campaigns Know Where You've Been. They're Tracking Your Phone*, Wall St. J. (Oct. 10, 2019), https://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889.

104 Henry Kenyon, *Democratic House Bills Aim to Stop Microtargeted Online Political Ads*, CQ Roll Call Washington Data Privacy Briefing, May 28, 2020, 2020 WL 2764822 (reporting on Rep. Anna G. Eshoo's The Banning Microtargeted Political Ads Act and Rep. David Cicilline's The Protecting Democracy from Disinformation Act).

105 Mike Isaac & Kate Conger, *Google, Facebook and Others Broaden Group to Secure U.S. Election*, N.Y. Times (Aug. 12, 2020), https://www.nytimes.com/2020/08/12/technology/google-facebook-coalition-us-election.html [https://perma.cc/LD6D-BPZ5].

106 Press Release, Office of the Dir. Nat'l Intel., Statement by NCSC Director William Evanina: 100 Days Until Election 2020 (July 24, 2020), https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020 [https://perma.cc/YZ7G-MHE6].

107 Charlie Warzel, *What Facebook Fed the Baby Boomers*, N.Y. Times (Nov. 24, 2020), https://www.nytimes.com/2020/11/24/opinion/facebook-disinformation-boomers.html [https://perma.cc/5X23-Q3YG].

108 Keach Hagey & Jeff Horwitz, Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead., Wall St. J. (Sept. 15, 2021).

109 Alex Warofka, Product Policy Manager, An Independent Assessment of the Human Rights Impact of Facebook in Myanmar, Facebook (Nov. 5, 2018), https://about.fb.com/news/2018/11/myanmar-hria/ (noting that a commissioned report concluded that, before 2018, "we weren't doing enough to help prevent our platform from being used to foment division and incite offline violence. We agree that we can and should do more."); Hao, *supra* note 82.

110 Newley Purnell & Jeff Horwitz, Facebook Services Are Used to Spread Religious Hatred in India, Internal Documents Show, Wall St. J. (Oct. 23, 2021).

111 Hao, *supra* note 82.

112 Jonas Kaiser & Adrian Rauchfleisch, *Unite the Right? How YouTube's Recommendation Algorithm Connects the U.S. Far-Right*, Medium (Apr. 11, 2018), https://medium.com/@MediaManipulation/unite-the-right-how-youtubes-recommendation-algorithm-connects-the-u-s-far-right-9f1387ccfabd [https://perma.cc/E4BS-2L44].

113 Annie Y. Chen et al., Exposure to Alternative & Extremist Content on YouTube, Anti-Defamation League (2021), https://www.adl.org/news/press-releases/despite-remediation-efforts-adl-finds-youtube-still-amplifies-extremist-content (study finding that YouTube plays an important role in exposing people to potentially harmful content, and that 9% of YouTube users who participated in a national study viewed at least one video from an extremist channel, and 22% viewed at least one video from an alternative channel that could serve as a gateway to extremist content, and were likely to see similar video recommended by

YouTube's algorithm); Tripp Mickle, *YouTube's Search Algorithm Directs Viewers to False and Sexualized Videos, Study Finds: More than 70% of videos flagged by study participants as objectionable were recommended by YouTube, according to Mozilla*, Wall St. J. (July 7, 2021), https://www.wsj.com/articles/youtubes-search-algorithm-directs-viewers-to-false-and-sexualized-videos-study-finds-11625644803; Ben Popken, *As Algorithms Take Over, YouTube's Recommendations Highlight a Human Problem*, NBC News (Apr. 19, 2018), https://www.nbcnews.com/tech/social-media/algorithms-take-over-youtube-s-recommendations-highlight-human-problem-n867596 [https://perma.cc/XE9N-F49P].

114 Jeff Horwitz, *Facebook Knew Calls for Violence Plagued 'Groups,' Now Plans Overhaul*, Wall St. J. (Jan. 31, 2021), https://www.wsj.com/articles/facebook-knew-calls-for-violence-plagued-groups-now-plans-overhaul-11612131374.

115 Hao, *supra* note 82.

116 Soroush Vosoughi, Deb Roy, & Sinan Aral, *The Spread of True and False News Online*, 359 Science 1146 (2018), https://doi.org/10.1126/science.aap9559.

117 *Id.*

118 Press Release, BIA Advisory Services, Google to Dominate Local Digital Advertising in 2018, According to BIA Advisory Services (May 7, 2018), http://www.biakelsey.com/google-dominate-local-digital-advertising-2018-according-bia-advisory-services/ [https://perma.cc/V74K-2Q5N].

119 House Report at 58 (quoting Submission from Nat'l Ass'n of Broads., to H. Comm. on the Judiciary, 2 (Oct. 14, 2019)), http://www.nab.org/documents/newsRoom/pdfs/09220_HJC_Local_Journalism_At_Risk_Sub

120 Tom Wheeler, *The Root of the Matter: Data and Duty*, Harv. Kennedy School, Shorenstein Center on Media, Politics, and Public Policy, Nov. 2018, at 20, https://shorensteincenter.org/wp-content/uploads/2018/11/Root-of-the-Matter-Wheeler.pdf?x78124 [https://perma.cc/8C34-7DF6].

121 House Report at 70.

122 *Newspapers Fact Sheet*, Pew Res. Center (July 9, 2019), https://www.journalism.org/fact-sheet/newspapers/ [https://perma.cc/VTD7-E97B].

123 Kristen Hare, *The Coronavirus Has Closed More Than 60 Local Newsrooms Across America. And Counting*, Poynter (Feb. 16, 2021), https://www.poynter.org/locally/2021/the-coronavirus-has-closed-more-than-60-local-newsrooms-across-america-and-counting/ [https://perma.cc/8JEB-PBUS].

124 Kristen Hare, *Here Are the Newsroom Layoffs, Furloughs and Closures That Happened During the Coronavirus Pandemic*, Poynter (Mar. 9, 2021), https://www.poynter.org/business-work/2021/here-are-the-newsroom-layoffs-furloughs-and-closures-caused-by-the-coronavirus/ [https://perma.cc/J8MH-JG9A].

125 Tony Proscio, *Out of Print: The Case for Philanthropic Support for Local Journalism in a Time of Market Upheaval*, Revson Found. (Jan. 31, 2018), http://revsonfoundation.org/files/2018/01/Out-of-Print-report-tony-proscio.pdf [https://perma.cc/DXM6-PCJV].

126 Penelope Muse Abernathy, *The Expanding News Desert*, U.N.C. Hussman Sch. of Journalism and Media, https://www.usnewsdeserts.com (last visited Mar. 13, 2021) [https://perma.cc/3ZAL-UTJ9].

127 Pengjie Gao et al., *Financing Dies in Darkness? The Impact of Newspaper Closures on Public Finance*, 135 Journal of Financial Economics 445–467 (2020), http://dx.doi.org/10.2139/ssrn.3175555 (finding that in the three years after a newspaper closed, municipal bond offering yields increased by 5.5 basis points, while yields in the secondary market increased by 6.4 basis points).

128 Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, Pew Res. Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/6K25-SMK6]; *Why Americans Don't Fully Trust Many Who Hold Positions of Power and Responsibility*, Pew Res. Center (Sept. 19, 2019), https://www.pewresearch.org/politics/2019/09/19/why-americans-dont-fully-trust-many-who-hold-positions-of-power-and-responsibility/ [https://perma.cc/L3WX-552S].

129 Auxier et al., *supra* note 131.

130 *Id.*

131 UK Competition and Markets Authority, The Commercial Use of Consumer Data: Report on the CMA's Call For Information 146 (2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_cc

132 Background Note by the Secretariat, Consumer Data Rights and Competition ¶ 62, OECD Doc. DAF/COMP(2020)1 (Apr. 29, 2020), https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf [https://perma.cc/SQ48-WEPD]; ACCC Final Report at 138; Carrière-Swallow & Haksar, *supra* note 14, at 16–17:

> . . . the private incentives to invest in data security are unlikely to lead to socially optimal levels of investment in cybersecurity (Kashyap and Wetherilt 2019). Nonrivalry and partial excludability make private contracts difficult to enforce, because the harm caused by misuse of data is difficult to trace to a specific breach. With incomplete contract enforceability ex post, an efficient digital economy requires agents to trust that their information will be adequately protected by counterparties (Organisation for Economic Co-operation and Development 2015). Perceptions of inadequate privacy or insufficient cybersecurity thus involve an externality, because the investment decisions of individual agents will affect overall trust in the economy's data security. By reducing trust and thus the willingness of users to share their data, one data set being mishandled may cause more harm to the system than the sum of the direct harm caused to each of the data subjects.

133 ACCC Final Report at 5.

134 *Id.*

135 Shoshana Zuboff, *The Coup We Are Not Talking About*, N.Y. Times (Jan. 29, 2021), https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html [https://perma.cc/BB8F-8BUX].

136 Gary T. Marx, *The Iron Fist and the Velvet Glove: Totalitarian Potentials Within Democratic Structures*, *in* The Social Fabric 102 (James E. Short, Jr., ed., 1986), https://web.mit.edu/gtmarx/www/iron.html [https://perma.cc/48ZL-GR7S].

137 For the fading divide between state and private sector and cooperation in information sharing, *see* Frank Pasquale, The Black Box Society 43–51 (2015).

138 One example is Tencent Holdings Ltd. launching with the Ministry of Public Security a pilot digital identification system. Alyssa Abkowitz, *The Internet Tightens: Popular Chinese WeChat App to Become Official ID*, Wall St. J. (Dec. 31, 2017), https://www.wsj.com/articles/internet-tightens-popular-chinese-wechat-app-to-become-official-id-1514541980.

139 Louise Matsakis, *Does TikTok Really Pose a Risk to US National Security?*, Wired (July 17, 2020), https://www.wired.com/story/tiktok-ban-us-national-security-risk/ [https://perma.cc/4M2F-5VPN].

140 Carpenter v. United States, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018).

141 *Carpenter*, 138 S. Ct. at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

142 *Carpenter*, 138 S. Ct. at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

143 Rani Molla, *Law Enforcement Is Now Buying Cellphone Location Data from Marketers*, Vox (Feb. 7, 2020), https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration; Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020); Christopher Mims, *Your Location Data Is Being Sold—Often Without Your Knowledge*, Wall St. J. (Mar. 4, 2018), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.

144 Mims, *supra* note 131.

145 *Carpenter*, 138 S. Ct. at 2218.

146 In 2021, "including both smart and feature phones, the current number of mobile phone users is 4.88 billion, which makes 62.24% of people in the world a cell phone owner." *How Many Smartphones Are in the World?*, BankMyCell, https://www.bankmycell.com/blog/how-many-phones-are-in-the-world (last visited Mar. 13, 2021) [https://perma.cc/Z8EF-FL4Y].

147 *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, Wash. Post (Oct. 30, 2013), https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.xhtml [https://perma.cc/CL46-3Y4C].

148 Press Release, WikiLeaks, Vault 7: CIA Hacking Tools Revealed (Mar. 7, 2017),

https://wikileaks.org/ciav7p1/ [https://perma.cc/K4SA-KDDQ].

149 Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 Harv. L. Rev. 497, 541 (2019).

150 Harrison Testimony, *supra* note 22.

151 *Hearing on Stacking the Tech: Has Google Harmed Competition in Online Advertising? Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. (Sept. 15, 2020) (Testimony of Adam Heimlich, CEO, Chalice Custom Algorithms), https://www.judiciary.senate.gov/meetings/stacking-the-tech-has-google-harmed-competition-in-online-advertising.

# 11
# Signs of Hope

Even when privacy, consumer protection, and competition policies are aligned and the surveillance economy is disconnected, privacy and competition will sometimes conflict. Policymakers would have to balance privacy's data minimization principles with competition's data-mobility policies. The Holy Grail is to have our cake (protecting our privacy) and eat it (obtaining the innovation and healthy competition from sharing that non-rivalrous data with others). So, the policymakers' mantra is to *promote competition while protecting privacy*.[1]

One possible way to do that is if personally identifiable information can be removed from the records in such a way to minimize the risk of disclosing any particular person's identity and the information about them. We will examine the de-identification of personal data as a possible way forward. While privacy scholars and computer scientists have expressed their doubts, given the risks of re-identification, we will consider whether recent legislation might increase the demand for better ways to anonymize personal data.

Many policymakers are keen to address the privacy and competition issues involving data-opolies. So, we will conclude with another sign of hope—possible change from within the data-opolies themselves.

## A. De-identification as the Holy Grail—Can We Benefit from the Non-rivalrous Quality of Personal Data without Sacrificing Privacy?

Some might ask, can't we do both? Can we promote competition through the free flow of personal data while adequately safeguarding our privacy, such as requiring the personal data to be aggregated or anonymized?[2] Two IMF officials note this win-win scenario where competition increases, but not at the price of our privacy:

> Can technologies such as anonymization provide a win-win by enabling the benefits of data access while maintaining adequate privacy? In several applications, data analytics can provide valuable insights without data being individually identifiable. Consider training artificial intelligence to drive an automated car, to recognize images of specific objects, to give a medical diagnosis based on an x-ray or blood test, or to study the effects of new pharmaceuticals based on anonymized data. All these applications rely on huge amounts of data to train the algorithms, but do not require that the data be linked to an individual.[3]

Identified data is "unambiguously associated with a specific person."[4] A good example is a driver's license, where the driver's birth date, photo, and other information are linked to the driver's name. One key issue is whether the personal data can be successfully anonymized ("data de-identification"). The California Privacy Rights Act of 2020, for example, has defined data as "deidentified" when the information

cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business that possesses the information:

> (A) takes reasonable measures to ensure that the information cannot be associated with a consumer or household;
> (B) publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision; and
> (C) contractually obligates any recipients of the information to comply with all provisions of this subdivision.[5]

In defining de-identified data, the legislature is primarily concerned with re-identification, where our privacy would be harmed. How can data, once de-identified, remain so without the risk of later being associated with a particular person or household? The OECD identifies the following approaches to de-identify data:

- Pseudonymised data, in which aliases are used in place of personal identifiers; aliases can only be reversed by the party that assigned them.
- Unlinked pseudonymised data, in which all identifiers are erased or substituted by aliases for which the assignment function is erased or irreversible, so that the linkage cannot be re-established by anyone.
- Anonymised data, which is unlinked and altered (e.g. attributes' values are randomised or generalised) in such a way that there is a reasonable level of confidence that a person cannot be identified.
- Aggregated data, which does not contain individual-level entries and is combined from information about enough different persons that individual-level attributes are not identifiable.[6]

One fundamental problem is that "the release of statistical data inevitably reveals some information about individual data subjects."[7] Suppose your alma mater discloses an aggregated anonymized dataset of alumni giving. Although the privacy risk of your being identified in this dataset is relatively small, the more the dataset is dissected and analyzed, the greater the potential privacy risk.[8]

Reconciling privacy and competition is even tougher for granular data. Although one can de-identify granular data, it is often easy to re-identify that data using other data sources.[9] Suppose a credit card company removes your name, address, and additional identifying information from its monthly credit card records. Suppose one accesses other databases that identify you (say, your geolocation data). In that case, one can quickly match your location to particular credit card transactions, such as when you bought gas last month at specific stations. With that information, one can now link your identity to your credit card purchases. Even if the geolocation data were de-identified, one could assume that the places where people spent most nights were their residences and re-identify them from other publicly available data.

One famous example involved the Massachusetts governor's personal medical records. To improve medical care and reduce health costs, Massachusetts in the late 1990s allowed researchers to access de-identified records summarizing information about all hospital visits made by state employees.[10] The governor assured them that in removing from the records their names, addresses, Social Security numbers, and other identifying information, their privacy was secured. It wasn't:

> Viewing this as a challenge, Professor Latanya Sweeney, then a graduate student at MIT, set out to identify Governor Weld's record in the dataset. She obtained demographic information about Governor Weld, including his ZIP code and date of birth, by requesting a copy of voter registration records made available to the public for a small fee. Finding just one record in the anonymized medical claims dataset that matched Governor Weld's gender, ZIP code, and date of birth enabled her to mail the Governor a copy of his personal medical records.[11]

Consequently, to successfully de-identify the data, one might have to strip away much information, and the data loses its value. As one computer scientist told me, "I can de-identify your face, but you'll look like a ghost."

Computer and privacy experts and policymakers, as of 2021, recognize that the current de-identification techniques do not remove all risks of re-identification for granular data; no standard or process currently exists to successfully ensure permanent de-identification, anonymization, and pseudonymization of personal information.[12] Moreover, the concern is that it will be easier to re-identify the individual, as (a) more datasets become available, (b) an individual's information is used more times in multiple analyses, and (c) data analytical techniques advance.[13] Thus, the research question remains: "Are there effective information disclosure controls, methods for de-identifying data, and means for assessing these de-identification methods?"[14]

One area of potential promise is the increase in demand for innovations and protocols to de-identify data. As privacy scholar Paul Ohm notes, technologies will not likely protect privacy 100% while enabling organizations to extract 100% of the data's value.[15] De-identification technologies might allow firms to extract perhaps a little more value from slightly less aggregated data without a significant decline in privacy.

Firms and scholars are experimenting with "differential privacy" tools, where researchers can have access to large datasets while reducing the risk of re-identification to an acceptable level. Differential privacy "protects an individual's information essentially as if her information were not used in the analysis at all, in the sense that the outcome of a differentially private algorithm is approximately the same whether the individual's information was used or not."[16] One method is adding random "noise" to the data.

Ideally, the difference between the results when a person's data is included in the analysis and the results when her information was excluded would be zero. In reality, the difference between the two is a positive number, called the privacy

loss parameter ε, which "measures the effect of each individual's information on the output of the analysis."[17] So, the privacy loss parameter ε can be "viewed as a measure of the additional privacy risk an individual could incur beyond the risk incurred in the opt-out scenario." The smaller the value of ε, the lesser the privacy risk of re-identification.

To illustrate, suppose you work at Facebook, and the company asks you to participate in a survey. One hesitancy is that even though the survey is supposed to be anonymous, Facebook could re-identify you from its questions about your age, gender, race, rank, and tenure with the company. Suppose the company promised to use these differential privacy tools in conducting the survey. Facebook promised not to use the data for other analyses and told you that random amounts of "noise" would be added to the data so that the privacy loss parameter ε would be quite low (say 0.02). Suppose you also know that around 80% of the employees would take the survey. Under the differential privacy tools, even if Facebook knew that you participated in the survey, it is improbable that Facebook could make any additional inferences about your responses than if you were among the employees who opted not to take the survey (the 20%). So suppose approximately 51% of the surveyed employees described Facebook as having a positive impact on the world, about 4% said it had no impact, and about 45% said Facebook had a negative impact. Using these differential privacy tools, the company could not identify which option you chose.

Nonetheless, differential privacy raises the trade-off between privacy and accuracy. To increase privacy, one might need to add more noise to the data, which reduces accuracy. Adding less noise to the data increases accuracy but reduces privacy.[18]

Thus, for small datasets, for datasets with many dimensions, or when the dimensions have large domains, one might have to add much noise, thereby reducing accuracy.[19] This was an issue with the 2020 U.S. census data. To preserve individuals' privacy, the U.S. Census Bureau said it would implement differential privacy tools. But many "organizations, data users, researchers, and demographers have expressed concern about the accuracy of the data produced under the DP algorithm and the usefulness of these releases for creating public policy, monitoring population structures and distribution, and expanding scientific understandings of ongoing demographic changes in this country."[20]

Researchers are now studying ways to improve the differential privacy tools and ways to obtain more value from the data, while preserving privacy.[21] Privacy

laws can increase the demand for these privacy technologies. If data is successfully "deidentified," then the GDPR and California Privacy Rights Act do not apply. Firms can freely collect, use, retain, sell, or disclose the de-identified information.[22] But to qualify as "deidentified" data, the firm must implement reasonable technical safeguards and business processes that significantly reduce the risk of re-identification. The GDPR, for example, requires firms to continually assess whether the data can be re-identified using the available technologies.[23] Suppose the law bans behavioral advertising and allows users to opt out of profiling. In that case, firms will have less incentive to hoard personal data and be more inclined to reduce their compliance costs under the jurisdiction's privacy laws. Suppose firms can avoid spending hundreds of thousands, if not millions, of dollars, complying with the privacy laws[24] by successfully anonymizing the personal data, and reap greater profits in doing so. In that case, they will have greater incentives to find ways to de-identify data.

Demand for de-identification technologies can also come from rivals seeking access to the data. The current legal framework encourages data-hoarding, which deprives rivals of scale, increases entry barriers, and widens the data-opolies' competitive advantage. Since data-opolies have the incentive to hoard data, rivals must persuade policymakers to impose data openness policies, which require the data-opoly to share the personal data with them. While the data-sharing might increase competition, it also increases the privacy risks. To mitigate the privacy risks, the data must be de-identified. But rivals must also convince policymakers that the data, once de-identified, cannot be re-identified. That gives rivals the incentive to find ways to successfully de-identify data and still glean insights from the data.

DuckDuckGo and Microsoft, for example, recognize that significant network effects are working against their search engines. (DuckDuckGo accesses organic search results and advertisements through negotiated agreements with Microsoft.) Without accessing many quality search queries (especially novel "tail" queries) and seeing where users click, their algorithms will not improve in quality relative to Google. As we saw in Chapter 1, this learning-by-doing network effect reinforces the leading search engine's advantage. As more people "google," the better the search results, the more likely they will stick with Google. With network effects (and Google's exclusionary practices) working against them, Microsoft and DuckDuckGo urged the U.K. competition authority in 2020 to require Google to share its click and query data. But the rivals

recognized that privacy concerns were a key obstacle in accessing the data. So, to alleviate privacy concerns, the search engine DuckDuckGo submitted that "APIs already exist to provide search results and that since the data is presented in a non-user identifiable manner, privacy and consumer protections, including compliance with GDPR, are preserved."[25] Likewise, the proposed Digital Markets Act would require the dominant search engine, namely Google, to

> provide to any third party providers of online search engines, upon their request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data.[26]

Thus, policymakers are willing to allow rivals to access the dominant search engine's query, click, click back, and generalized location data, if it will not jeopardize our privacy.[27]

When data is necessary to compete (whether to train algorithms, improve services, and gain insights), rivals will likely impress policymakers to require data-opolies to turn over personal data. But in recognizing the privacy risks of re-identifying granular data, rivals likely will invest in protocols and technologies to effectively de-identify the data, perhaps not at its granular level, but at a more aggregated level, where the data is still useful for their purposes and the privacy risks are minimized.

Consequently, one way to harmonize privacy's data minimization policies with competition's data openness policies is to allow firms to collect data that is necessary to provide the services or products (but not for profiling and behavioral advertising purposes), and then let (or require) firms to share aggregated de-identified data with researchers, universities, rivals, and government agencies when it would benefit society (such as fostering insights on health and safety) without increasing the privacy risk beyond a specific threshold.

In the advertising sector, we saw how data could help with verification, measurement, and attribution. So, one way to harmonize the privacy and competition levers, as the U.K.'s competition authority is considering, is by "shifting the matching between exposure and conversion events to the device, and only sending anonymous and or aggregate attribution data to advertisers, rather than relying on individual-level tracking."[28]

Once the privacy, consumer protection, and competition levers are correctly calibrated, the demand for de-identification protocols and techniques will likely increase. Although we may never reach the Holy Grail of successfully de-identifying granular data, improvements in the privacy differential tools can help many more entities derive slightly more value from the data while still safeguarding privacy, thereby promoting healthy competition, closing the AI divide, and fostering innovation.

## B. Signs of Hope within the Data-opolies

Our discussion has focused mainly on the government as the agents of change, bolstered by the market participants who are currently beaten down by the data-opolies. But what about change arising from within the data-opolies?

Money can blind many of us to our employers' unethical behavior.[29] So we should not expect the data-opolies' employees to support political candidates whose policies threaten their firms' monopoly. After all, the greater the monopoly profits, the greater the share that the employees might receive. According to one pay-scale website, a higher-level principal engineer at Google was estimated to make in 2021 on average about $1,107,572 per year,[30] which is more than Amazon or Apple senior software engineers ($671,564 and $681,000, respectively),[31] but slightly less than a senior Facebook software engineer ($1.36 million).[32] If they personally profit from their employer's monopoly, one would not expect the employees to support politicians who vow to strengthen the antitrust laws, and certainly not politicians who promise to break up their employer.

But Google's, Amazon's, Facebook's, and Apple's employees financially supported in the 2020 presidential primaries two progressive Democratic candidates, Bernie Sanders and Elizabeth Warren, who promised to break them up.[33]

Facebook employees donated $37,726 to Donald Trump in contrast to $244,771 to Bernie Sanders and $91,411 to Elizabeth Warren.[34]

Google same story. The top individual recipients, besides Joe Biden ($4,368,768), were Bernie Sanders ($979,651) and Elizabeth Warren ($701,646). Donald Trump, in contrast, received only $102,444.[35]

Likewise, for Amazon, the top individual recipients in the 2020 elections were Joe Biden ($2,277,466) and Bernie Sanders ($808,469). Donald Trump, in contrast, received $268,964, slightly more than Elizabeth Warren ($248,061).[36]

The top individual recipients from Apple employees, besides Joe Biden ($1,885,635), were Bernie Sanders ($494,953) and Elizabeth Warren ($290,427). Donald Trump, in contrast, received $108,565.[37]

One might argue that Donald Trump was tougher on antitrust. The Obama administration gave Big Tech a free pass (outside of collusion).[38] Most notably, the FTC in 2013 overruled its legal staff's recommendation to sue Google for its anticompetitive practices.[39] But during the presidential primaries, it was uncertain that the Trump administration would sue Google and Facebook. Antitrust enforcement during the Trump administration was often uneven and controversial.[40] Moreover, for the past 40 years, Republican administrations, unlike the Eisenhower and Nixon administrations, were tolerant of monopolies and their abuses. The Department of Justice, for example, brought only four monopolization cases during the entire 20-year period of the Reagan, Bush Sr., and George W. Bush administrations.[41]

So, what is going on here? It is unlikely that so many GAFA employees suffer from Stockholm Syndrome in identifying with their oppressors' goals.

Most of us desire purposeful work. One recent survey found a high correlation between well-being and purposeful work: "Whereas only 6% of those who have low levels of purpose in their work have high levels of overall wellbeing, fully 59% of those with high purpose in work have high wellbeing."[42] As Facebook's early investor and adviser, Roger McNamee, observed, "From its earliest days, Facebook was a company of people with good intentions."[43] Chris Hughes, one of Facebook's co-founders, authored a widely read 2019 op-ed, *It's Time to Break Up Facebook*, which helped launch the FTC and states' monopolization inquiry.[44]

Leading up to the mob attack on the Capitol in January 2021, Facebook's social network was seeing an increase in hate speech and call for violence. As *The Wall Street Journal* reported, Facebook's Chief Technology Officer Mike Schroepfer told employees –

> "Hang in there everyone," . . . asking for patience while the company figured out how best "to allow for peaceful discussion and organizing but not calls for violence."[45]

But Facebook employees dissented –

> "All due respect, but haven't we had enough time to figure out how to manage discourse without enabling violence?" responded one employee, one of many unhappy responses that together gathered hundreds of likes from colleagues. "We've been fueling this fire for a long time and we shouldn't be surprised that it's now out of control."[46]

In Facebook's semiannual "Pulse Survey," taken by over 49,000 employees in October 2020, many Facebook employees were losing faith in their employer:

> Only 51% of respondents said they believed that Facebook was having a positive impact on the world, down 23 percentage points from the company's last survey in May [2020] and down 5.5 percentage points from the same period last year [2019]. In response to a question about the company's leadership, only 56% of employees had a favorable response, compared to 76% in May [2020] and more than 60% last year [2019].[47]

Employees, as the internal Facebook documents reflect, are questioning the ethics of their employer's actions.

It is hard to feel good when working for an employer that bullies and destroys smaller rivals, merchants, app developers, and websites. It is hard to defend an employer's social media products, when foreign despots are weaponizing them to destabilize democracies. And in the end, it is hard to defend using one's talents to nudge individuals to click more ads or buy more stuff.

Few would want to live in this dystopia. As the famous electric shock experiments by Stanley Milgram show, dissent is a powerful mechanism to stop unethical behavior.[48] Thus, the data-opolies' employees, many of whom financially supported progressive candidates, may desire change for the betterment of their employer and society.

Most of us prefer using our talents for the betterment of others. We want to create, as Harvard Business School Professor Michael Porter calls, shared value. Our employer provides "economic value in a way that also creates value for society by addressing its needs and challenges."[49] We would prefer to compete in markets where the rules of the game are clear and fair and apply to all. We want to preserve opportunities for our children for meaningful, purposeful work.

Ultimately, after I presented a draft of this book, one thoughtful professor at UC Berkeley replied, it is easier to change a business model. That is especially true of a behavioral advertising-driven business model that primarily benefits a few companies, and is built on exploiting individuals, their privacy, and their autonomy. Most people perceive behavioral advertising as more harmful than beneficial. And they are right. So, why continue to support a business model that

has been weaponized to target vulnerable populations, helps engineer elections through micro-targeted political ads, sows discord, creates fight clubs, and is predicted to undermine democracies when other less harmful business models exist and have worked for years? Surveillance capitalism simply perpetuates an undemocratic class system, where a few profit at the expense of many.

As Microsoft's president warned, "Advanced technology no longer stands apart from society; it is becoming deeply infused in our personal and professional lives."[50] Walking down the street or attending a rally will increasingly subject us to more intrusive surveillance, like facial recognition technology,[51] which could be used by the government, marketers, or others in this largely unregulated, free-for-all. For glimpses of this world, we can look at China's advancements in algorithmic surveillance. Each citizen receives a "citizen score," designed to incentivize "good" behavior.[52] So your score "could be higher if you buy items the regime likes—like diapers—and lower if you buy ones it doesn't, like video games or alcohol."[53] Your political activities could also heavily affect your score: "Posting political opinions without prior permission or even posting true news that the Chinese government dislikes could decrease your rank." And your score is affected by what your friends do, such as "publish opinions without prior permission, or report accurate but embarrassing news."[54] Lest we think that scoring is limited to China, scoring is already occurring in Western democracies.[55]

With the incentives to profit from manipulating our behavior diminished, the data-opolies, websites and apps can re-channel their energies to what made their products and services original and innovative. Google's co-founders rightfully perceived the corrupting influence of behavioral advertising. But they knew that in this unregulated arms race, if their search engine did not profit from advertising, a rival would. The best anecdote to the Panopticon World is not in regulating data-opolies with more behavioral dictates. As long as behavioral advertising persists, so too will the toxic competition. The opportunity costs are enormous. Trust in digital markets will continue to decline, as will the potential value from sharing data. To reorient competition from its toxic form to something nobler, we need to change the current incentives.

Once we dismantle the Panopticon where almost every aspect of our lives—where we are, with whom we spend our time, how we spend that time, and whether we are in a romantic relationship—is tracked, predicted, and manipulated, we can harness the value from data to promote an inclusive

economy, that protects our autonomy, well-being, and democracy. In short, a nobler form of competition that brings out our best rather than preying on our worst.

---

1 *See, e.g.*, Digital Competition Expert Panel, Unlocking Digital Competition at 57 (2019) (also known as the Furman Report), https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel [https://perma.cc/VK9M-3GV8] [hereinafter Furman Report] ("Secure access to non-personal and anonymized data: tackling the data barrier to entry for smaller and newer firms, while protecting privacy.").

2 Furman Report at 74.

3 Yan Carrière-Swallow & Vikram Haksar, *The Economics and Implications of Data: An Integrated Perspective*, International Monetary Fund Policy Paper No. 19/16 (Sept. 2019) at 15, https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596.

4 Background Note by the Secretariat, Consumer Data Rights and Competition at ¶ 24, p. 10, OECD Doc. DAF/COMP(2020)1 (Apr. 29, 2020), https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf [https://perma.cc/SQ48-WEPD] [hereinafter OECD Consumer Data Rights and Competition].

5 California Privacy Rights Act of 2020 § 1798.140(m) [hereinafter CPRA].

6 OECD, Consumer Data Rights and Competition at ¶ 24, p. 10.

7 Alexandra Wood et al., *Differential Privacy: A Primer for a Non-Technical Audience*, 21 Vand. J. Ent. & Tech. L. 209, 230 (2018) (quoting Fed. Comm. on Statistical Methodology, Report on Statistical Disclosure Limitation Methodology (Office of Mgmt. & Budget: Statistical Policy, Working Paper No. 22, 2005), https://www.hhs.gov/sites/default/files/spwp22.pdf).

8 Wood et al., *supra* note 7, at 228 provide the following example of the problem of composition:

In March, Alice publishes an article based on the information in this database and writes that "the current freshman class at Private University is made up of 3,005 students, 202 of whom are from families earning over $350,000 per year." Alice reasons that, because she published an aggregate statistic taken from over 3,005 people, no individual's personal information will be exposed. The following month, Bob publishes a separate article containing these statistics: "201 students in Private University's freshman class of 3,004 have household incomes exceeding $350,000 per year." Neither Alice nor Bob is aware that they have both published similar information.

A clever student Eve reads both of these articles and makes an observation. From the published information, Eve concludes that between March and April one freshman withdrew from Private University and that the student's parents earn over $350,000 per year. Eve asks around and is able to determine that a student named John dropped out around the end of March. Eve then informs her classmates that John's family probably earns over $350,000 per year.

John hears about this and is upset that his former classmates learned about his family's financial status. He complains to the university, and Alice and Bob are asked to explain. In their defense, both Alice and Bob argue that they published only information that had been aggregated over a large population and does not identify any individuals.

Example 5 illustrates how, in combination, the results of multiple analyses using information about the same people may enable one to draw conclusions about individuals in the data. Alice and Bob each published information that, in isolation, seems innocuous. However, when combined, the information they published compromised John's privacy. This type of privacy breach is difficult for Alice or Bob to prevent individually, as neither knows what information others have already revealed or will reveal in future.

9 Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1751 (2010) (noting that the "utility and privacy of data are linked, and so long as data is useful, even in the slightest, then it is also potentially reidentifiable"); Shoshana Zuboff, Surveillance Capitalism 245 (2019) (noting that "with as little as three bits of data easily culled from the public record—birth date, zip code, and sex—reidentification science has demonstrated its ability to de-anonymize meta-data with 'disturbing ease' "); Brief of Amicus Curiae Center on Privacy & Technology at Georgetown Law in Support of Appellants' Petition for Rehearing En Banc, Leaders of a Beautiful Struggle v Baltimore Police Department, No. 20-1495, 2020 WL 7024181 (4th Cir. Nov. 27, 2020), at 6–7 (citing experiments demonstrating "how seemingly 'anonymous' data can be used to ascertain an individual's identity").

10 Wood et al., *supra* note 7, at 221-22.

11 *Id.* at 222 (noting that "risks remain even if additional pieces of information, such as those that were leveraged in Professor Sweeney's attack (gender, date of birth, and ZIP code),

are removed from a dataset prior to release").

12 OECD Consumer Data Rights and Competition, *supra* note 4, at ¶ 25; Wood et al., *supra* note 7, at 250.

13 Australian Competition and Consumer Commission, Digital Platforms Inquiry—Final Report at 36, 411 (2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report [https://perma.cc/M36S-YQJ4]; Bhaskar Chakravorti, *Why It's So Hard for Users to Control Their Data*, Harv. Bus. Rev. (Jan. 30, 2020), https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data [https://perma.cc/MT22-LN46]; Wood et al., *supra* note 7, at 212.

14 Nat'l Sci. & Tech. Council, National Privacy Research Strategy 17 (2016), https://www.nitrd.gov/pubs/NationalPrivacyResearchStrategy.pdf [https://perma.cc/ZU6E-JT9U].

15 Ohm, *supra* note 9, at 1744.

16 Wood et al., *supra* note 7, at 212. In other words, what can be learned about that person "from a differentially private computation is essentially limited to what could be learned about him from everyone else's data without his own data being included in the computation." *Id.* at 227.

17 *Id.* at 235.

18 *Id*. at 234.

19 Hyukki Lee & Yon Dohn Chung, *Differentially Private Release of Medical Microdata: An Efficient and Practical Approach for Preserving Informative Attribute Values*, 20 BMC Med. Informatics & Decision Making 1 (2020), https://doi.org/10.1186/s12911-020-01171-5.

20 Alexis R. Santos-Lozada, Jeffrey T. Howard, & Ashton M. Verdery, *How Differential Privacy Will Affect Our Understanding of Health Disparities in the United States*, 117 Proc. Nat'l Acad. Sci. 13405 (2020), https://doi.org/10.1073/pnas.2003714117 (finding that the implementation of differential privacy would "produce dramatic changes in population counts for racial/ethnic minorities in small areas and less urban settings, significantly altering knowledge about health disparities in mortality").

21 Wood et al., *supra* note 7, at 255.

22 GDPR Recital 26, https://gdpr-info.eu/recitals/no-26/ (stating that the data protection principles should "not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" and the GDPR does not "concern the processing of such anonymous information, including for statistical or research purposes"); CPRA § 1798.145(a)(6).

23 GDPR Recital 26 (requiring an assessment of all the means reasonably likely to be used either by the controller or by another person to identify the natural person directly or indirectly, including "the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments").

24 Nick Eckert, *What Are the Real Costs of GDPR Compliance?*, PrivIQ (Jan. 30, 2019),

https://priviq.com/blog/what-are-the-real-costs-of-gdpr-compliance/ [https://perma.cc/J3A3-4RQY].

25 CMA Final Report at ¶ 8.38.

26 European Commission, Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) Art. 6(1)(j) (Dec. 15, 2020), https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf [https://perma.cc/G87S-Q88U].

27 CMA Final Report at ¶ 8.38.

28 , Online Platforms & Digital Advertising: Market Study Interim Report Appendix L at ¶ 95 (2019), https://assets.publishing.service.gov.uk/media/5df9efa2ed915d093f742872/Appendix_L_Pote

29 *See* Max H. Bazerman & Ann E. Tenbrunsel, Blind Spots: Why We Fail to Do What's Right and What to Do About It 81–83 (2011) (discussing how financial incentives can motivate ethical blindness and how the behavioral ethics literature questions the objectivity of auditors, managers and lawyers, who have a significant pecuniary interest in the transaction or outcome); Scott Killingsworth, *"C" Is for Crucible: Behavioral Ethics, Culture, and the Board's Role in C-Suite Compliance, in* Culture, Compliance, and the C-Suite: How Executives, Boards, and Policymakers Can Better Safeguard Against Misconduct at the Top (Michael D. Greenberg, ed., 2013), http://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF316/RAND_CF316. [https://perma.cc/L4AM-GP7V].

30 *Google Level L8: Principal Engineer*, Levels.FYI, https://www.levels.fyi/company/Google/salaries/Software-Engineer/L8/ (last visited Mar. 14, 2021) [https://perma.cc/HTT7-5MLG].

31 *Apple Level ICT6: Principal Software Engineer*, Levels.FYI, https://www.levels.fyi/company/Apple/salaries/Software-Engineer/ICT6/ (last visited Mar. 14, 2021) [https://perma.cc/BP59-8R5R]. *Amazon Level L7: Principal SDE*, Levels.FYI, https://www.levels.fyi/company/Amazon/salaries/Software-Engineer/Principal-SDE/ (last visited Mar. 14, 2021) [https://perma.cc/23TQ-WTLL].

32 *Facebook Level E8: Software Engineer*, Levels.FYI, https://www.levels.fyi/company/Facebook/salaries/Software-Engineer/E8/ (last visited Mar. 14, 2021) [https://perma.cc/LY3R-28GN].

33 Elizabeth Warren, *Here's How We Can Break Up Big Tech*, Medium (Mar. 8, 2019), https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c [https://perma.cc/H5VG-VXG3]; Bernie Sanders, Issues: Corporate Accountability and Democracy, https://berniesanders.com/issues/corporate-accountability-and-democracy/.

34 Overall, 92.28% of Facebook employees' contributions in the 2020 election cycle went to Democrats (with $1,583,067 to Joe Biden). Facebook Inc., Open Secrets, https://www.opensecrets.org/orgs/facebook-inc/recipients?id=D000033563 (last visited Mar. 14, 2021) [https://perma.cc/GJH8-TSUK].

35 Overall 94.8% of Google employees' contributions went to Democrats. Alphabet Inc., Open Secrets, https://www.opensecrets.org/orgs/alphabet-inc/recipients?id=D000067823 (last visited Mar. 14, 2021) [https://perma.cc/U97R-4BUZ].

36 Overall 86.19% of Amazon employees' contributions went to Democrats. *Amazon.com*, Open Secrets, https://www.opensecrets.org/orgs/amazon-com/recipients?id=D000023883 (last visited Mar. 14, 2021) [https://perma.cc/Q35Q-3Z7Z].

37 Overall 95.44% of Apple's employees' contributions went to Democrats. Apple Inc., Open Secrets, https://www.opensecrets.org/orgs/apple-inc/recipients?id=D000021754 (last visited Mar. 14, 2021) [https://perma.cc/N2J6-ZRBE].

38 Leah Nylen, *The Government's Lawyers Saw A Google Monopoly Coming. Their Bosses Refused to Sue*, Politico (Mar. 16, 2021), https://www.politico.com/news/2021/03/16/google-files-mobile-search-market-475576

39 Brody Mullins, Rolfe Winkler, & Brent Kendall, *Inside the U.S. Antitrust Probe of Google*, Wall St. J. (Mar. 19, 2015), https://www.wsj.com/articles/inside-the-u-s-antitrust-probe-of-google-1426793274.

40 For a critical assessment, *see* Chris Sagers, *The Utter Failure of the Trump Administration's Antitrust Chief*, Slate (Aug. 10, 2020), https://slate.com/business/2020/08/antitrust-doj-delrahim-trump.html [https://perma.cc/SM2M-WU5B]. For a defense, *see* Roger Alford, *Regarding Those Marijuana Mergers: A Response to Accusers Who Question the DOJ*, Just Security (July 13, 2020), https://www.justsecurity.org/71295/regarding-those-marijuana-mergers-a-response-to-accusers-who-question-the-doj/ [https://perma.cc/KPN9-3NT3].

41 U.S. Dep't of Justice, Antitrust Division Workload Statistics FY 1980–1989, https://www.justice.gov/atr/antitrust-division-workload-statistics-fy-1980-1989 [https://perma.cc/DB74-GZSK]; U.S. Dep't of Justice, Antitrust Division Workload Statistics FY 1990–1999, https://www.justice.gov/sites/default/files/atr/legacy/2009/06/09/246419.pdf [https://perma.cc/A37H-K5WV]; U.S. Dep't of Justice, Antitrust Division Workload Statistics FY 2000–2009, https://www.justice.gov/sites/default/files/atr/legacy/2012/04/04/281484.pdf [https://perma.cc/NXF6-7DBL].

42 Bates College & Gallup, Forging Pathways to Purposeful Work, The Role of Higher Education 6 (2019), https://www.bates.edu/purpose/files/2019/05/Bates_PurposefulWork_FINAL_REPORT.pdf [https://perma.cc/N9QU-DJTF].

43 Roger McNamee, Zucked: Waking Up to the Facebook Catastrophe 16–17 (2019).

44 Chris Hughes, *It's Time to Break Up Facebook*, N.Y. Times (May 9, 2019), https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html [https://perma.cc/4ABN-LN7M].

45 Jeff Horwitz & Deepa Seetharaman, *Facebook Turned on Trump After Warnings That 'Business as Usual Isn't Working'*, Wall St. J. (Jan. 13, 2021), https://www.wsj.com/articles/facebook-turned-on-trump-after-warnings-that-business-as-usual-isnt-working-11610578907.

46 *Id*.

47 Ryan Mac & Craig Silverman, *Plunging Morale and Self-Congratulations: Inside Facebook the Day Before the Presidential Election*, BuzzFeed News (Nov. 3, 2020), https://www.buzzfeednews.com/article/ryanmac/inside-facebook-24-hours-before-election-

day https://perma.cc/GHW9-ESA8].

48 Stanley Milgram, *The Perils of Obedience*, Harper's Mag. (Dec. 1973), at 77.

49 Harvard Bus. School, Inst. for Strategy & Competitiveness, Creating Shared Value, https://www.isc.hbs.edu/creating-shared-value/Pages/default.aspx (last visited Mar. 14, 2021) [https://perma.cc/TZ68-9H89].

50 Brad Smith, *Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility*, Microsoft on the Issues (July 13, 2018), https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/ [https://perma.cc/RG23-492U].

51 *Id.*

52 Anna Mitchell & Larry Diamond, *China's Surveillance State Should Scare Everyone*, Atlantic (Feb. 2, 2018), https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/ [https://perma.cc/488M-549V].

53 Amy Hawkins, *Chinese Citizens Want the Government to Rank Them*, Foreign Policy (May 24, 2017), https://foreignpolicy.com/2017/05/24/chinese-citizens-want-the-government-to-rank-them/ [https://perma.cc/D636-5GWX].

54 Rick Falkvinge, *In China, Your Credit Score Is Now Affected by Your Political Opinions—And Your Friends' Political Opinions*, Privacy News Online (Oct. 3, 2015), https://www.privateinternetaccess.com/blog/in-china-your-credit-score-is-now-affected-by-your-political-opinions-and-your-friends-political-opinions/ [https://perma.cc/PEV8-QRHR].

55 Frank Pasquale, The Black Box Society 26–28 (2015).

# Index

*For the benefit of digital users, indexed terms that span two pages (e.g., 52–53) may, on occasion, appear on only one of those pages.*

Tables and figures are indicated by *t* and *f* following the page number.