





## Also by Cory Doctorow

### LITTLE BROTHER

*Little Brother*

*Homeland*

*Lawful Interceptions*

*Attack Surface*

*Spill*

### MARTIN HENCH

*Red Team Blues*

*The Bezzle*

*Picks and Shovels*

### FICTION

*Down and Out in the Magic Kingdom*

*Eastern Standard Tribe*

*Someone Comes to Town, Someone Leaves Town*

*With a Little Help*

*Makers*

*For the Win*

*The Rapture of the Nerds*

*Pirate Cinema*

*Walkaway*

*The Lost Cause*

*A Place So Foreign and Eight More*

*Overclocked*

*The Great Big Beautiful Tomorrow*

*Radicalized*

### GRAPHIC NOVELS

*Cory Doctorow's Futuristic Tales of the Here and Now*

*In Real Life*

### NONFICTION

*The Complete Idiot's Guide to Publishing Science Fiction*

*Essential Blogging*

*Content*

*Ebooks*

*Context*

*All Complex Ecosystems Have Parasites*

*Information Doesn't Want to Be Free*

*Chokepoint Capitalism*

*The Internet Con*

# Enshittification



# Enshittification

Why Everything Suddenly Got Worse  
and What to Do About It

**Cory Doctorow**



MCD | Farrar, Straus and Giroux | New York

MCD

Farrar, Straus and Giroux  
120 Broadway, New York 10271

EU Representative: Macmillan Publishers Ireland Ltd, 1st Floor, The Liffey Trust  
Centre, 117–126 Sheriff Street Upper, Dublin 1, DO1 YC43

Copyright © 2025 by Cory Doctorow  
All rights reserved  
Printed in the United States of America  
First edition, 2025

Frontispiece art by No Ideas

Library of Congress Cataloging-in-Publication Data  
ISBN: 978-0-374-61932-9

*Designed by Gretchen Achilles*

The publisher of this book does not authorize the use or reproduction of any part of this book in any manner for the purpose of training artificial intelligence technologies or systems. The publisher of this book expressly reserves this book from the Text and Data Mining exception in accordance with Article 4(3) of the European Union Digital Single Market Directive 2019/790.

Our books may be purchased in bulk for specialty retail/wholesale, literacy, corporate/premium, educational, and subscription box use. Please contact [MacmillanSpecialMarkets@macmillan.com](mailto:MacmillanSpecialMarkets@macmillan.com).

[www.mcdbooks.com](http://www.mcdbooks.com) • [www.fsgbooks.com](http://www.fsgbooks.com)  
Follow us on social media at [@mcdbooks](https://twitter.com/mcdbooks) and [@fsgbooks](https://twitter.com/fsgbooks)

10 9 8 7 6 5 4 3 2 1

*To my comrades, past, present, and future.  
It has been an honor.*



I will never forgive them for what they did to the computer.

—ED ZITRON



# Contents

Introduction	3
<b>Part One: The Natural History</b>	<b>7</b>
Case Study: Facebook	11
Case Study: Amazon	20
Case Study: iPhone	29
Case Study: Twitter	37
<b>Part Two: The Pathology</b>	<b>53</b>
<b>Part Three: The Epidemiology</b>	<b>69</b>
The End of Competition	71
The Death of Competition Kills Regulation, Too	106
“With an App”	111
It’s Not Wage Theft If We Do It with an App: Uber’s Algorithmic Wage Discrimination	114
Reverse-Centaurs and Chickenization	120
Twiddling	127
The End of Self-Help	133
The End of Labor Power	155
Tech Rights Are Worker Rights: Para and Tuyul Apps	159

The Google Walkouts, Tech Solidarity, and Tech Unions	168
Rent Seeking and Technofeudalism	194
<b>Part Four: The Cure</b>	<b>213</b>
Antitrust Is Back, Baby	227
Antitrust Under Trump	240
Bringing Back Regulation	248
Privacy First	254
The EU's Digital Markets Act and Digital Services Act	259
Administrability	268
Bringing Back Self-Help	281
The Strange Tale of Beeper Mini	291
Repealing the Law of "Felony Contempt of Business Model"	299
Restoring Labor	307
There's Bad News and There's Good News	319
Conclusion: Is Enshittification Just Capitalism?	331
Acknowledgments	335

# **Enshittification**



# Introduction

It's not just you. The internet is getting worse, fast. The services we rely on, that we once loved? They're all turning into piles of shit, all at once. Worse, the digital is merging with the physical, which means that the same forces that are wrecking our platforms are also wrecking our homes and our cars, the places where we work and shop. The world is increasingly made up of computers we put our bodies into, and computers we put into our bodies. And these computers *suck*.

This is infuriating. It's frustrating. And, depending on how important those services are to you, it's *terrifying*.

I've been an internet activist for a quarter of a century, working with the Electronic Frontier Foundation, a digital human rights group that more or less invented the whole idea of digital human rights. I've been a United Nations observer and helped draft internet treaties; I've lobbied legislatures and agencies in the United States, Canada, Europe, and the United Kingdom. I've been through street protests and virtual blackouts.

I've never seen anything like this.

In 2022, after decades of striving to get people fired up about the esoteric world of internet policy, I coined a term to describe the sudden-onset platform collapse going on all around us: *en-shittification*. To my bittersweet satisfaction, that word is doing big numbers. In fact, it has achieved escape velocity.

It's a funny, naughty word, and it's funny and naughty to say,

and I'm proud of that. But that's not why the American Dialect Society named it its word of the year in 2023, nor why Australia's *Macquarie Dictionary* named it its word of the year for 2024, nor why millions of people have used it to describe the inescapable online dumpster fire that's roasting them alive.

The reason for *enshittification*'s popularity is that it embodies a theory that explains the accelerating decay of the things that matter to us, explaining why this is happening *and* what we should do about it.

Because *enshittification* isn't just a way to say "Something got worse."\* It's an analysis that explains the *way* an online service gets worse, *how* that worsening unfolds, and the *contagion* that's causing everything to get worse, all at once.

You see, this moment we're living through, this Great Enshittening? It's not a mystery. It's not the Great Forces of History bearing down on our moment, decreeing that we must all suffer through the end of services that once met our needs. It's a material phenomenon, much like a disease.

Like a disease, it has *symptoms*, a *mechanism*, and an *epidemiology*. The first part of this book will explain these components of enshittification.

But the point of this analysis isn't to merely give you a more technically informed way to feel demoralized and furious about the state of the digital world—I wrote this book to propose a *cure*. That's the second part of the book.

This era, the Enshittocene, is the result of specific policy decisions, made by named individuals. Once we identify those decisions and those individuals, we can *act*. We can reverse the decisions. We can name the individuals. We can even es-

\* Though it's fine with me if you want to use it that way! One of the glories of English is its malleability. English words mean whatever English speakers say they mean. Go nuts. You have my blessing.

imate what size pitchfork they wear. Or at the very least, we can make sure that they are never again trusted with the power to make policy decisions for the rest of us.

We can make a new, good internet, one that's fit for human thriving. We can create the digital nervous system we need to connect and coordinate us through a twenty-first century haunted by climate collapse, genocide, authoritarianism, and economic chaos.

We can create enshittification-resistant infrastructure for a new, good world.



## Part One

# The Natural History

Enshittification infects a specific kind of digital business: *platforms*.

The term *platform* gets thrown about a lot. Formally, a platform is a business that operates a *two-sided market*, that is, a system that connects *business customers* and *end users*.

In its purest form, a platform's value comes from the people and companies that use it, not from anything it brings to the table. The more people there are selling things on an e-commerce platform, the more value that platform holds for shoppers. Likewise, the more buyers there are on a platform, the more value it holds for sellers.

Think of eBay and Amazon, which connect buyers and sellers. Or Uber and Thumbtack, which connect workers and customers. Or Google, which connects publishers and advertisers to searchers. Or Facebook, which does the same but for people who want to socialize rather than search.

The platform has emerged as the endemic form of online enterprise, which is weird, because another word for *platform* is *middleman*.

If you're old enough to remember the early excitement about the coming digital age, you'll recall how enthusiastic we were about the prospect of *disintermediation*—that is, cutting out the middleman.

It's not that middlemen (also called *intermediaries*, which is where we get *disintermediation* from) are intrinsically evil. Take books (like this one!): I have worked in printing, bookselling,

publishing, and pre-press, and obviously, I also write books. Even though I am knowledgeable and skilled in many of the arts needed to bring this book to you, I voluntarily and enthusiastically work with publishers like Farrar, Straus and Giroux, because they can accomplish this work better than I can, because they offer a fair deal, and because doing so lets me prioritize writing books, which I enjoy *much* more than doing that other stuff.

Intermediaries are part of the solution to the age-old problem of connecting people with one another—but they become part of the problem when they grow so powerful that they can act as gatekeepers who can usurp the relationship between the two sides of their markets.\*

That’s why the early days of the internet were so concerned with disintermediation. We had a sense that our intermediaries had gotten too big for their britches: we were tired of a few big retailers deciding what we could buy, a dozen big publishers and studios deciding what we could read and watch, and half a dozen big labels deciding what music we heard. We’d heard the horror stories of how these big intermediaries treated their suppliers—be they small businesses, creative workers, or manufacturers—and we yearned for a way to cut out the middleman and do business directly with the people who made and did the things we loved, or at least the things we needed.

There was a time when disintermediation seemed to be living up to its promise. Small businesses popped up to supply us with online goods and services, and while some of them were founded explicitly as fast-growing startups with global ambitions, some of the most successful disintermediators—like Craigslist—were basically hobbies that accidentally turned into hugely disruptive

\* For more on this, see *Chokepoint Capitalism: How Big Tech and Big Content Captured Creative Labor Markets and How We’ll Win Them Back*, a book from Beacon Press that I coauthored with Rebecca Giblin in 2022.

businesses, serving as a vessel that people with something to offer and people seeking out those offers could fill up.

But the internet's early blush of disintermediation faded quickly. Waves of mergers and acquisitions consolidated the internet into "five giant websites, each filled with screenshots of the other four."<sup>\*</sup> Meanwhile, the *non*-tech intermediaries were *also* consolidating: most of the key sectors of the global economy shrank to five or fewer firms, and the most pronounced consolidation took place with intermediary sectors like shipping and finance. The entertainment industry, too. Remember the early-2000s dream of disrupting the *dozen* major publishers? Today, there are *five* major publishers, *four* major studios, *three* major labels, *two* companies that dominate apps, and a *single* company that dominates ebooks and audiobooks.

We're a quarter century into the digital-forward, internet-fueled twenty-first century, and the power of intermediaries has never been greater. The internet *could* disintermediate our world, enable person-to-person relations, and relegate intermediaries to *helping* buyers and sellers, rather than exploiting them.

But it hasn't.

But it's worse: this isn't merely the age of the abusive outsized platform; it's the age of the *sick, collapsing* abusive outsized platform.

It's the Enshittocene.

When doctors observe patients who are sick with a novel pathogen, their first order of business is creating a *natural history* of the disease. This natural history is an ordered catalog of the disease's progress: What symptoms do patients exhibit, and in which order?

Here's the natural history of enshittification:

<sup>\*</sup> In the memorable phrasing of the New Zealand software developer Tom Eastman.

1. First, platforms are good to their users.
2. Then they abuse their users to make things better for their business customers.
3. Next, they abuse those business customers to claw back all the value for themselves.
4. Finally, they have become a giant pile of shit.

This pattern is everywhere. Once you learn about it, you'll start seeing it, too. In the coming pages, I'll do a few case studies of once-beloved services.

These case studies are not intended to be exhaustive; rather, they're a representative sample. You could fill several more books with breakdowns of companies like Uber, Valve, and Fitbit, but it would get repetitive!

# Case Study: Facebook

## Stage One: Good to Users

Facebook is the perfect place to start. Facebook is a service that Mark Zuckerberg started in his dorm room so that he and his creepy pals could nonconsensually rate the fuckability of their fellow Harvard undergrads.\*

It was Zuck's users who figured out how to make something great out of this inauspicious beginning. They filled up the vessel with themselves and with connections to one another, forging bonds. It was a compelling experience, so much so that many people called it addictive.

But Zuck was determined to bring Facebook back to its origins: a service that treated people as means, not ends—as something for the platform's managers to toy with and, ultimately, abuse.

When Facebook started, it was available only to American college kids. They *loved* it, and investors saw potential: with all these users piling it, there would be innumerable opportunities to sell things to them. Hell, you could sell users to one another. Investors poured money into the business. In 2006, Facebook decided to spend some of its investors' cash to expand to the general population, so it dropped the requirement for users to

\* True story.

sign up with the .edu email addresses that only American college students, faculty, and personnel can get.

Back in 2006, Facebook made a simple and compelling pitch to those new users it was hoping to lure onto the platform:

Sure, we understand that most of you already have a social media service that you enjoy using called MySpace. But has it occurred to you that MySpace is owned by an evil, crapulent, senescent Australian billionaire named Rupert Murdoch, and he spies on you with every hour that God sends?

Come to Facebook, where we will *never* spy on you.\*

All we ask of you is that you create a Facebook account and then “articulate your social graph” by telling us which other users you want to connect to you. Then, we will create an automated custom feed, consisting solely of the things that the people you follow have posted for consumption by their followers.†

This is a pretty good deal. You aren’t imagining it: Facebook was fun and useful and valuable, once upon a time.

That was stage one: Facebook had a surplus (its investors’ cash), and it allocated that surplus to its end users by subsidizing a feed of things that users wanted to see, rather than things that businesses would pay to show them.

To sweeten the deal, Facebook gave MySpace refugees a way to eat their cake and have it, too: a bot. Once you joined Face-

\* Yes, really. For more, see Dina Srinivasan’s classic article “The Antitrust Case Against Facebook: A Monopolist’s Journey Towards Pervasive Surveillance in Spite of Consumers’ Preference for Privacy,” *Berkeley Business Law Journal* 16, no. 1 (2019).

† Ibid., *supra*, re: This is a sarcastic paraphrase and not a direct quote.

book, you could give that bot your MySpace login and password, and then, several times a day, the bot would log in to MySpace on your behalf, scraping all the messages your friends there had left for you and pasting them into your Facebook inbox. You could reply to those, and the bot would push them back out to MySpace on your behalf. That way, you didn't have to choose between Facebook's superior user experience and the friends you left behind on MySpace.\*

So users piled in, and they proceeded to lock themselves into Facebook's platform. There are lots of ways for digital businesses to lock in their users, but with social media, they don't even have to try.

Most online businesses enjoy high *network effects*. This is the economist's term for a product or service that gets more valuable as it attracts more users. You joined Facebook because the people who were already there made it valuable to you, and once you were there, you made Facebook more valuable to the people who wanted to hang out with you.

But Facebook doesn't just benefit from large network effects; it also relies on high switching costs.

*Switching costs* is another useful piece of economics jargon. Switching costs are everything you have to give up when you switch from one product or service to another.

In the case of Facebook, the switching costs of leaving Facebook include the company of everyone you hang out with there, because they'll still be on Facebook and you won't be.

Now, hypothetically, you can avoid this switching cost. If you can convince all the people you like on Facebook to quit at the

\* Try to do this to Facebook today, and it'll nuke you till you glow. See the discussion of "felony contempt of business model" on page 145.

same time as you and transition to a new social network where you can all reestablish your links, you can leave Facebook *and* keep your friends.

Here's where the *collective action problem* comes in. That's our third and final piece of economics jargon: the collective action problem is the incredibly difficult business of getting other people to do what you want them to do, when you want them to do it.

You experience the collective action problem on a small scale all the time. You know that group chat with half a dozen friends in it? Remember how hard it was to decide what movie or bar to go to, or which board game you should all play? Even when you all agree that you want to do *something* together, it's hard to agree *what to do* and *when to do it*. That's the collective action problem.

Adding people to the group makes the collective action problem exponentially more problematic. Once you're established in a Facebook community with a couple hundred friends, you have to convince them all to leave at the same time as you, and go to the same place as you.

But all those friends have their own groups of people they can't afford to leave. Maybe they're in a support group for people with a rare disease. Maybe they use Facebook to organize their kid's Little League carpool with the other parents. Or maybe that's how they stay in touch with the people they left behind when they emigrated. Maybe it's where their customers are.

To get your friends to switch away from Facebook, you not only must convince them that it's time to go and that you've got the right place for them to go next—you *also* have to convince them to talk all those other people into leaving, too; or you have to convince them to endure the switching costs of leaving their own groups behind.

So Facebook users can't help but take one another hostage,

and Facebook grew progressively more cognizant of this fact. Once it sensed that a critical mass of its users were locked in to its platform, it was time for stage two.

## Stage Two: Good to Business Customers

Facebook understood that it could make money from two groups of business customers: advertisers and publishers. There was only one problem: to make the service valuable to them, Facebook would have to reduce the value enjoyed by its users.

So Facebook started to claw back the surplus from those end users and began doling it out to advertisers and publishers. Facebook approached its advertisers and made a pitch: “Hey, do you remember when we told these rubes that we wouldn’t ever spy on them? We were lying. We spy on them from asshole to appetite. If you give us a remarkably reasonable sum of money, we will use that surveillance data to do extraordinarily precisely targeted advertising on your behalf. What’s more, we are such upright, good-natured slobs that we have filled a whole building with engineers who labor day and night to fight ad fraud. If you give us a dollar to show an ad to a specific kind of person, you can be *sure* that ad is going to be shown to the right person.”\*

Then, Facebook approached publishers and made a different pitch: “Hey, do you remember when we told these rubes that we would only show them the things they asked to see? That was a total lie. If you post short excerpts from your own website content to your Facebook account, complete with a link back to that website, we will nonconsensually cram those excerpts into the

\* Once again, not an actual quote, but rather a hyperbolic, rhetorical interpretation of the corporate messaging.

eyeballs of users who never asked to see them. You will get a free traffic funnel that you can monetize as you see fit.”\*

So the publishers and the advertisers piled in, too, and they became dependent on the users—the users who were sticking around because they were dependent on one another, the users who took one another hostage—which meant the publishers and advertisers were now held hostage, too.

Now it was time for stage three of enshittification: putting the screws to the business customers.

### Stage Three: A Giant Pile of Shit

For advertisers, this took the form of rising prices and plummeting ad fidelity, along with skyrocketing ad fraud. Gradually, Facebook ramped up the price of targeting an ad to its users, but it also took less care to show ads to the users advertisers had selected.†

Meanwhile, ad fraud was going *wild*. Advertisers were paying billions for ads that *no one* ever saw. In 2018, Procter & Gamble zeroed out its \$200 million annual “programmatically advertising”‡ budget and saw *no* decline in sales.§ It seems all of those ads were either:

- a. Being shown to random people rather than the people P&G was paying to target; or
- b. Not being shown to *anyone*.

\* Also not a quote!

† Srinivasan, “The Antitrust Case Against Facebook.”

‡ The tech industry’s euphemism for *surveillance advertising*.

§ Lauren Johnson, “When Procter & Gamble Cut \$200 Million in Digital Ad Spend, It Increased Its Reach 10%,” *Adweek*, March 1, 2018.

It wasn't any better for publishers. Gradually, Facebook's content recommendation algorithm started to require longer and longer excerpts in order for posts to qualify for being shoved into strangers' feeds. The system *also* started downranking shorter excerpts in *subscribers'* feeds, meaning that publishers had to push longer and longer excerpts onto Facebook's platform in order to be seen at all. The longer a post was, the more substitutive it was for the whole article.

Eventually, publishers were corralled into publishing their whole articles on Facebook, and then, to add insult to injury, Facebook started to suppress posts that linked away from its site, on the grounds that such links might be "malicious." Worse, even whole articles with no links were often suppressed, even for followers, and publishers had to pay to "boost" their content in order to have it shown to the people who'd explicitly asked to see it.

At this point, the publishers had been converted to commodity back-end suppliers to Facebook, and their main path to monetization was Facebook's own rigged ad marketplace.

Meanwhile, for users, things kept getting even worse. Facebook dialed down the quantum of content from the people you chose to follow and wanted to hear from to a mingy, homeopathic residue, leaving behind a newsfeed void that the algorithm could fill with content people paid to put there: ads and boosted content.

This is stage three of enshittification: Facebook has now withdrawn *all* available surplus, leaving behind the bare minimum it calculates to be sufficient to keep users glued to one another, and publishers and advertisers glued to the users. Every available penny of surplus has been clawed back and given to Facebook's shareholders and executives.

But this is a very brittle equilibrium. The difference between the user who says, "Goddamn I hate this place, but I can't stop

logging in to it,” and the user who says, “*Goddamn* I hate this place, and I’m never coming back” is *razor*-thin.

All it takes is one whistleblower, one Cambridge Analytica-style privacy scandal, one livestreamed mass shooting, and users bolt for the exits.

Every time that happens, Facebook learns that network effects are double-edged swords. The users who can’t leave because they can’t bear to part with their friends have no reason to stay after those friends depart. Once the exodus starts, it tends to accelerate.

Investors certainly understand this. Any bobble in Facebook’s growth—let alone a contraction in Facebook’s user numbers—triggers shareholder panics. In the first quarter of 2022, Facebook posted lower-than-projected US user growth, and the stock market responded with a mass sell-off, dumping \$250 billion worth of Facebook shares in twenty-four hours, at the time the largest decline in any corporate valuation in the history of the human race.\*

When their company’s fortunes turn uncertain, tech leaders panic. Being techies, they have a technical name for this panic: they call it *pivoting*.

Facebook’s pivot was decidedly weird. Mark Zuckerberg addressed the world and said, “Look, I know I’ve spent the past decade insisting that the future would consist solely of you arguing with your racist uncle using a primitive text interface of my own devising. But I have had a revelation. It turns out that the future *really* will involve me converting you and everyone you love into a legless, sexless, low-polygon, heavily surveilled cartoon character in a virtual world called the Metaverse, which we ripped off from a twenty-five-year-old dystopian, satirical cyberpunk novel.”

\* You love to see it.

That's *end-stage* enshittification, the stage at which a platform turns into a pile of shit. Facebook isn't the first platform to reach this stage, but it has managed an improbably prolonged period of shambling continuation, long past the date when we should have put it into the ground.

That's what distinguishes enshittification from "tech companies turning awful and going out of business." All our tech businesses are turning awful, all at once, and they're not dying. We remain trapped in their rotting carcasses, unable to escape.

I'll explain why that is in Part Three, and in Part Four, I'll explain what to do about it.

# Case Study: Amazon

In Jeff Bezos's original business plan for Amazon, the company was called Relentless. Critics say that this is a reference to Bezos's cutthroat competitive instincts, but Bezos always insisted that it was a reference to his company's relentless commitment to customer service.

How did Amazon go from a logistics company that got packages to you quickly and efficiently to a behemoth of digital content defined by the Prime experience (which has much less to do with free shipping now and more with everything else)?

## Stage One: Good to Users

Like Facebook, Amazon started with a large surplus that it was able to allocate to its customers, and allocate it did. The company raised a fortune from early investors, and then a larger fortune by listing on the stock market. Then it used that fortune to subsidize many goods, selling them below cost. It also subsidized shipping and offered a generous, no-questions-asked, postage-paid returns policy.

As with Facebook, this offer tempted millions of users to pile onto the platform. Unlike Facebook users, however, Amazon users didn't automatically lock themselves in with the collec-

tive action problem. It doesn't matter to your neighbor whether you shop at Amazon or not. Your purchase of ebooks or audiobooks on Amazon doesn't make those books more valuable to other readers. Your Prime membership doesn't make their Prime membership harder to give up.

But that Prime membership *does* go a long way to locking you in to Amazon. Paying for shipping a year in advance is a powerful incentive for you to do your shopping on Amazon. Indeed, the overwhelming majority of Prime subscribers begin their e-commerce searches on Amazon and, if they find what they're looking for, don't comparison shop for a better deal.

You can think of Prime as a form of soft lock-in, Amazon binding you to its platform with a silken ribbon. But Amazon's also got some iron chains in its toolbox. All the audiobooks and movies, and most of the ebooks and e-magazines, you buy from Amazon are *permanently* locked to Amazon's platform.

That's because these products are sold with digital rights management (DRM), a form of encryption designed to force you to view or listen to these digital products using apps that Amazon controls. Break up with Amazon and delete your apps, and you will lose all the media you've ever bought from the platform. For a certain kind of reader, listener, or movie buff, this is a very high switching cost indeed.\*

Amazon has one more trick up its sleeve: after years of selling goods below cost, it has completed the work that Walmart started, eliminating swaths of small, independent brick-and-mortar businesses. Its online predatory pricing tactics have done the same for much of the e-commerce world.†

\* For more on this, see "The End of Self-Help," page 133.

† For more on this, see "The End of Competition," page 71.

That means that shopping anywhere other than Amazon has gotten substantially more inconvenient.

These tactics—Prime, DRM, and predatory pricing—make it very hard *not* to shop at Amazon. With users locked in, to proceed with the enshittification playbook, Amazon needed to get its business customers locked in, too.

## Stage Two: Good to Business Customers

Amazon was initially very good to those business customers. Amazon paid full price for their goods, then sold them below cost to its customers. It subsidized returns and customer service, too. It ran a clean search engine, which put the best matches for shoppers' queries at the top of the page, creating a path to glory merchants could walk merely by selling quality goods at fair prices.

Then, once those merchants were locked in, Amazon put the screws to them—just as Facebook put the screws to the publishers and advertisers.

Amazon brags about this technique, which it calls “the flywheel.” It brings in users with low prices and a large selection. This attracts merchants who are eager to sell to those users. The merchants' dependence on those customers allows Amazon to extract higher discounts from those merchants, and that brings in more users, which makes the platform even more indispensable for merchants, allowing the company to require even deeper discounts—and around and around the flywheel spins.

Let's take a step back before we get hurt. This flywheel is the direct product of a radical legal theory that has had the world in its grip since the late 1970s. From the 1890s until the Carter administration, corporate power was blunted by antitrust law, which treated large corporations as threats *simply because they*

were large. Once a company is too big to fail, it becomes too big to jail, and then it becomes too big to care. Antitrust law was designed to fight that apathy and force companies to care.

A rival—and frankly terrible—theory of antitrust law says that the only time a government should intervene against a monopolist is when it is *sure* that the monopolist is using its scale to raise prices or lower quality. This is the “consumer welfare standard theory,” and its premise is that when we find monopolies in the wild, they are almost certainly large and powerful thanks to the quality of their offerings. Anytime you find that people all buy the same goods from the same store, you should assume that this is the very best store, selling the very best goods. It would be perverse (goes the theory) for the government to harass companies for being so excellent that everyone loves them.

It was under this theory that Jimmy Carter started to remove a few of the Jenga blocks from the antitrust system. Then Ronald Reagan came along and tore them out by the fistful. (Most of the right-wing policies for which we remember Ronald Reagan started under Carter, who was hoping to woo conservative voters. He failed.) Every president since—Republican or Democrat—followed Reagan’s example, up to (but not including) Joe Biden.

The Amazon flywheel is designed to fit neatly into the consumer welfare framework. It proclaims itself to be an enemy to merchants *on behalf of* consumers. The flywheel is all about lowering prices, and the consumer welfare standard theory prizes low prices above all else.

### Stage Three: A Giant Pile of Shit

Amazon has a myriad of tactics at its disposal for shifting value from business customers to itself, some of which also involve

shifting value away from end users, no matter what the cute fly-wheel pitch says.

Amazon uses its overview of merchants' sales, as well as its ability to observe the return addresses on direct shipments from merchants' contracting factories, to cream off its merchants' bestselling items and clone them, relegating the original seller to page umpty-million of its search results.

Amazon also crushes its merchants under a mountain of junk fees that are pitched as optional but are actually effectively mandatory. Take Prime: a merchant has to give up a huge share of each sale to be included in Prime, and merchants that don't use Prime are pushed so far down in the search results that they might as well cease to exist.

Same with Fulfillment by Amazon, a "service" in which a merchant sends its items to an Amazon warehouse to be packed and delivered with Amazon's own inventory. This is far more expensive than comparable (or superior) shipping services from rival logistics companies, and a merchant that ships through one of those rivals is, again, relegated even farther down the search rankings.

All told, Amazon makes so much money charging merchants to deliver the wares they sell through the platform that Amazon's own shipping is fully subsidized. In other words, Amazon gouges its merchants so much that it pays *nothing* to ship its own goods, which compete directly with those merchants' goods.\*

Here's where Amazon's attacks on its merchants' bottom lines turn into higher prices for its customers. A merchant that

\* "At this point, the price Amazon charges these third party sellers has grown to nearly 50% of its revenue. It is this money, estimated at \$123 billion in total last year, that pays for 'free' shipping, as well as its video service, its music service, Twitch, and everything else that comes bundled with Prime." Matt Stoller, "The FTC Sues to Break Up Amazon over an Economy-Wide 'Hidden Tax,'" *BIG* (Substack), September 27, 2023.

pays Amazon through the nose needs to make up the money *somewhere*. Hypothetically, merchants could eat Amazon's fees themselves—in other words, if Amazon wants a 10 percent fee on an item with a 20 percent margin, the seller could split the difference, and settle for a 10 percent profit.

But Amazon's fee isn't 10 percent. Add all the junk fees together, and an Amazon seller is being screwed out of 45 to 51 cents on every dollar it earns on the platform. Even if a merchant *wanted* to absorb the "Amazon tax" on your behalf, it couldn't. Merchants just don't make 51 percent margins.

So merchants *must* jack up prices, which they do. *A lot*. Now, you may have noticed that Amazon's prices aren't any higher than the prices that you pay elsewhere. There's a good reason for that: when merchants raise their prices on Amazon, they are *required* to raise their prices everywhere else, even on their own direct-sales stores. This arrangement is called *most-favored-nation status*, and it's key to the US Federal Trade Commission's antitrust lawsuit against Amazon.

Let the implications of *most-favored nation* settle in for a moment. If Amazon is taxing merchants 45 to 51 cents on every dollar they make, and if merchants are hiking their prices everywhere their goods are sold, then it follows that you're paying the Amazon tax *no matter where you shop*. Amazon has made prices go up at Target. At Walmart. At the corner mom-and-pop hardware store. At the manufacturer's own website.

On average, the first result in an Amazon search is 29 percent more expensive than the best result for your search. Click any of the top four links on the top of your screen, and you'll pay an average of 25 percent more than you would for your best match. On average, that best match is located *seventeen* places down in an Amazon search result. Then there's Amazon's "search" product.

The quotation marks around *search* are there for purposes of expressing withering sarcasm, because Amazon’s “search” product isn’t about search at all. Amazon makes \$38 billion every year charging merchants for search placement. When you search for a product on Amazon, the top results aren’t the best matches—they’re the matches that pay the highest bribes to Amazon to be at the top of the list.

The researchers Rory Van Loo and Nikita Aggarwal call this “Amazon’s pricing paradox.”\* Amazon gets to insist that it has the lowest prices in the business, but no one can find those prices. Instead, we all pay a massive Amazon tax every time we shop there, *and* the merchants we buy from are paying an Amazon tax, too.

That means that, on average, the stuff at the top of an Amazon search results page is *bad*. It’s low-quality, high-priced junk. Even when you’re buying a known quantity, like a specific brand of AA batteries, the top item will usually be more expensive than the items lower down on the page—the ones without the splashy banners advertising “Our Pick” or “Top Choice.” The Amazon smile logo gets a lot more sinister when it appears next to a top search result that costs 29 percent more than the best match for your query, thanks to Amazon’s \$38-billion-a-year paid search placement.

Not that you can find lower prices through anything as simple as sorting your search results by price. The merchants that dominate the search listings will play games with quantity to have the result with the lowest price, even if the price *per unit* is much higher. For example, a four-pack of AAs priced at \$3.99 is more expensive per battery than a sixteen-pack priced at \$10

\* Rory Van Loo and Nikita Aggarwal, “Amazon’s Pricing Paradox,” *Harvard Journal of Law & Technology* 37, no. 1 (Fall 2023).

(i.e., \$1.00 versus \$0.63), but sort-by-lowest-price will bury the better deal on the third or fourth page of results.

This is only the beginning. Amazon has clawed back value from buyers and sellers in so many, many more ways. It underinvests in anti-fraud, so the top-scoring items with the highest user ratings are often terrible but are garlanded with (paid) rave reviews. Merchants with high-quality offerings are faced with two bad options: either they sink to the bottom of the rankings, or they cheat, too. If they *do* cheat, they'll have to raise the prices of their merchandise in order to pay for the specialized fraud-as-a-service scum who gin up all those fake reviews. Then, if they get caught, they'll be banished from Amazon and either go bust or have to start all over again under a new business name.

But for Amazon, all of this is fine. This is how its system works, its flywheel. Amazon makes money when you are satisfied, and it makes money when you're furious. The costs are borne by sellers, and by you. Why *would* the company invest in fighting fraud under those circumstances?

That's also why Amazon puts so little effort into policing rotten sellers—and why so many of the “brands” on Amazon are consonant-heavy nonsense strings, seemingly generated at random by fly-by-nights that pop up and disappear and then pop up again under a new random name.

This is end-stage enshittification. Amazon locked in its customers and then squeezeed, counting on a few good, desperate sellers to keep the system goin'. Then, it clawed value away from its good sellers, leaving behind bad sellers that are a further source of misery for us.

Now Amazon is in the terminal stage of enshittification. We're all still stuck to the platform, but we get less and less value out of it. And because we're all still there on Amazon, buying Prime

and starting (and ending) our purchase planning with Amazon's enshittified search results, the merchants who rely on selling to us are stuck there, too, earning less and less from every sale.

The platform has turned into a pile of shit, and we're at the bottom of it.

# Case Study: iPhone

## Stage One: Good to Users

It wasn't merely Steve Jobs's legendary "reality distortion field." The iPhone really *was* a revolutionary product. It built on the elegance of the iPod, a device that "just worked." Plug a new iPod into your computer, and in a few seconds all the music on your laptop would be mirrored into a pocket-sized gadget, along with your playlists and ratings. The iPhone extended that easy synchronization to email, calendars, and a host of other utility features that were easier to use and more powerful than those of its rivals, like BlackBerry and Android.

The iPhone kept itself so slick and functional by operating as a "walled garden." Although it was a full-featured computer, capable of running *any* software, Apple made it so that you could run only the programs it authorized. At first, these were the apps that shipped with the phone, but a year later, Apple opened its App Store, a "curated marketplace" of apps that the company had vetted for safety and quality.

Apple touted this as a service to its end users. The company expended considerable resources ensuring that every app you downloaded, paid or free, "just worked."

That was stage one. The company had a surplus—the sums it chose to spend on product quality and maintenance, rather than

on, say, share buybacks or dividends—and it allocated that surplus to users.

Then, some of that surplus was shifted to its business customers—the app vendors.

Apple has always stressed the superiority of its closed, curated, managed service over Google's Android, whose app store is said to have looser rules for inclusion and to be more dangerous than Apple's peaceful Eden. To make things worse, owners of Android devices can choose to directly install apps, without ever touching an app store—that means that, on their intimate pocket computers, they can run code that has never been vetted by a multibillion-dollar tech company's security experts.

Apple has also touted the superiority of an economy grounded in good, old-fashioned money, contrasting this with Google's ad-centric Android. Both Google and Apple charge you for the service you get, but (Apple claims) Apple puts the price tag on the front of its product, while Google charges you by siphoning off a constant stream of personal data used to feed a vast surveillance advertising empire. Apple said it was a hardware company, swapping material objects for cash, not a surveillance company that made its profits by selling its customers.

Apple's defenders claim that this makes Apple a better bargain—for its users, and for society. Because Apple gets paid in dollars, rather than eyeballs, it has an incentive to satisfy you. If you're paying Apple, Apple wants to keep you happy, by showing you the things that you want to see as quickly and efficiently as possible.

Not so the "surveillance capitalists" like Google: the longer you linger with their products, the more chances they have to show you an ad, and every time they show you an ad, they make more money. So these "bad" capitalists try to hook you by

“hacking your dopamine loops” to keep you angry and clicking and fighting, leading to a host of evils, from anorexia in teens to right-wing extremist militias.

Thus, in the “surveillance capitalism” hypothesis, the “good” capitalism of Apple—the kind where money is exchanged for goods—has no need for surveillance.

This is obviously a self-serving narrative, but this much was true: the iPhone was substantially less surveillant than Android, and the locked-down nature of the iPhone platform meant that there were fewer hacks and fewer scandals about data-stealing apps.

In other words, Apple had a surplus, and it allocated that surplus to its end users. The company devoted substantial engineering to producing a smoothly operating platform, and it devoted even more work to vetting apps.

But the flip side of that was lock-in. Unlike Android phones—which are typically designed to allow users to make use of alternative app stores and even install different operating systems—iPhones use software and hardware locks to prevent users from modifying Apple’s rules.

This is a system that works well, but fails badly. So long as Apple remains a benevolent dictator, your iPhone is a walled garden that protects you from the bad guys who want to attack you. But if Apple turns on you, that walled garden becomes a prison, one that pens you in and makes you easy pickings.

Apple’s total control over the iPhone meant that the more you used your phone, the more hooks Apple could sink into you, raising the switching costs of leaving the platform. The things you created—message histories, notes, calendar entries—were shackled to the platform, as was the media you bought: books, videos, and music.

Apple—not you—gets to decide whether you can install an app to make it easier to slurp all that data out of your iPhone and transmit it to an Android or Windows device.

## Stage Two: Good to Business Customers

Apple completed its lock-in by bringing in the business customers. For these business customers, Apple offered a sweet deal indeed: “Develop iPhone apps and sell them through our store. We’ll collect a one-time fee when you sell the app, and you’ll pocket the rest, plus the lifetime revenues from your customers’ in-app spending.” That was the time of “There’s an app for that,” when independent software vendors and iPhone customers met one another’s needs.

App makers showed up, and the network effect wrought its magic: every new app was a potential new reason to buy an iPhone; every iPhone sold was another potential customer for a new app. Every one of these apps increased Apple’s lock on its users, and the network effect only multiplied—users checked in, but they couldn’t easily check out.

For all that Apple presented itself as the surveillance-free alternative to Android (just as Facebook had once presented itself as the surveillance-free successor to MySpace), some aspects of the iPhone’s design made it an even more potent commercial surveillance tool than any Android device.

The same lock-in that prevented users from modifying their iPhones in ways that potentially exposed them to danger *also* prevented users from modifying their iPhones to *defend* themselves against danger.

That meant that once an app made it through the App Store

vetting process, users were defenseless against it. Apps from major companies like Facebook (as well as innumerable bottom-feeding fly-by-night outfits) gathered data on iPhone users and funneled it into the commercial surveillance vortex, where it was sold, given away, stolen, published, and weaponized.

Users could not install privacy blockers, spoofing tools, or any other utility that would let them push back against this abuse. Only Apple could do that—and it didn't. As far as Apple was concerned, only the company could decide which privacy protections you deserved. By allowing for *some* surveillance on iOS, Apple could lure in more business customers. So iOS users had to tolerate whatever surveillance Apple judged to be tolerable.

At first, anyway.

But in 2021, Apple took action on surveillance in the App Store: the company announced a one-click opt-out from app-based surveillance. Once users checked the “don't spy on me” box, *all* the third-party apps on their phones were prevented from gathering information on them. This was a massive blow to the commercial surveillance industry. Facebook warned investors that the move would cost the company at least *\$10 billion in the first year*.

There's a reason Apple's crackdown on commercial surveillance was so hard on Facebook (and other surveillance-oriented app companies): everyone hates commercial surveillance, sure, but Apple customers bought a product that was specifically marketed as a way to avoid it.

Once Apple offered iPhone owners a single button that they could click to block surveillance, *96 percent* of iPhone owners clicked it. Presumably, the other 4 percent were drunk, or Facebook employees, or drunk Facebook employees.

### Stage Three: A Giant Pile of Shit

But enshittification never sleeps: right around the time that Apple was running a global ad campaign touting its commitment to privacy, it was *also* rolling out a secret surveillance system for iPhones, iPads, and other iOS devices. Apple now gathers the very same data that Facebook once gathered on its customers, and for the same purpose: to fuel Apple's own surveillance advertising business.

The argument that “if you're not paying for the product, you're the product” is herein revealed as bunk. Companies don't treat you well because they're “good” capitalists, and they don't abuse you because they're “bad” capitalists. Respect for your privacy isn't a rebate you get for every \$1,000 you spend on an iPhone. Companies abuse you *if they can get away with it*.

That's the crux of enshittification. Apple didn't treat its customers well because it loved them. It treated them well to lure them into its walled garden, which was then revealed to be a prison.

Likewise, Apple didn't offer the companies that filled its App Store that onetime charge for initial sales because it was a “good” company. Getting app vendors into the App Store kicked off the network effect: more apps, more users; more users, more apps. And that gave Apple the power to change the deal later.

And *boy*, did Apple change the deal. The processing fee for money exchanged in an app or on the App Store doubled, to 30 percent, and Apple switched to charging that fee on *every* dollar the app made, *forever*.\*

At the same time, Apple rolled out draconian policies that

\* See Elliott Ash, Daniel L. Chen, and Suresh Naidu, “Ideas Have Consequences: The Impact of Law and Economics on American Justice,” NBER Working Paper 29788 (February 2022).

punished any app vendor that encouraged its customers to make payments via a website, where the payment processing fee could be reduced by more than 90 percent, to the industry standard of 2 to 5 percent. Even *mentioning* that there was a way to save money by paying on the web was grounds for removal from the App Store.

This is the Amazon playbook: pile the junk fees onto your business customers, then use your lock-in to punish them for doing anything to avoid those fees. Naturally, merchants had to raise their prices—few products, even digital ones, have 30 percent margins. But these prices went up on every mobile platform, because Apple’s “competitor,” Google’s Android, had exactly the same fees and policies, though Android used subtler tactics to lock app vendors in to its store, like contracts that banned phone manufacturers (like Samsung) and carriers (like Verizon) from preinstalling third-party app stores. Antitrust investigations in the United States and the European Union have concluded that Google uses these strong-arm tactics to keep customers locked in to the Google Play app store, every bit as much as Apple does with its App Store.

Stage three of enshittification heaves into sight at this point. Apple can pick winners and losers, for example, by exempting Uber from its 30 percent app tax, while charging smaller competitors the full amount. Like Amazon, Apple can clone its best customers’ businesses and directly compete with them.

When Apple sells you an audiobook via its Apple Books app (which comes preinstalled on your iPhone), it doesn’t charge *itself* a 30 percent fee for every book sold. But other companies *do* pay the fee, which is onerous indeed, since the wholesale discount for audiobooks is only 20 percent.

That means that when Apple sells you a Penguin Random House audiobook for \$25, it sends \$20 to Penguin Random House and keeps \$5 for itself. But if an indie audiobook store like (the

excellent) Libro.fm sells you that audiobook through Apple's platform, it pays Penguin Random House \$20 and owes Apple a further \$7.50. In other words, if Libro.fm tries to sell audiobooks through an iPhone app, it loses money on every sale.

Of course, this doesn't apply to everyone: Uber and Lyft are exempt from these fees. Enshittifiers stick together.

## Case Study: Twitter

When Twitter started, its most obvious characteristic was its brevity. Users were limited to sending messages no longer than 140 characters, brief enough to fit into the short message service (SMS) system, the standard text-messaging system used by mobile phones around the world. (See page 293 for more on SMS.)

But for business customers—developers looking to integrate with Twitter—the length constraint for messages was secondary. The most interesting thing about Twitter was its API (or rather, that Twitter *was* an API).

That’s one of those computer-industry acronyms that doesn’t really stand for anything. It originally stood for “application programming interface,” and later “advanced programming interface,” but really, *API* just stands for “API”—a subtle, *sui generis* way of talking about a feature of a digital system that has no adequate equivalent in the nondigital world.

An API, broadly speaking, is any way that one program can exchange data with another program and/or receive data and/or instructions from another program.

For example, you might get emails with calendar invitations in them. Clicking on these invitations automatically adds them to your personal calendar. This is possible because there’s a formal standard for calendar invites, decided by a committee at the Internet Engineering Task Force. Anyone who consults this standard

can use it to make a compatible calendar, or to generate invitations that work with such a calendar.

## Stage One: Good to Users

But an API can also be informal and improvisational. Hashtags are a kind of API: a developer who scrapes Twitter can use hashtags to figure out what each post is about. APIs can also be added by third parties: a developer who scrapes Twitter and categorizes posts by hashtag can then set up a more formal way for others to pull those out of their own database, without doing all that messy scraping.

At its outset, Twitter was, in fact, an API. The core of Twitter was a database of users' posts that users themselves had no way to access. In order to post or read tweets, users had to make use of a program that used the Twitter API to access the database, pulling out the relevant entries and presenting them in a human-readable form.

Twitter made one of those API-accessing programs, but it also allowed anyone else to make such programs, and they all accessed the *same* API.

It's hard to overstate how revolutionary this was: normally, companies give themselves privileged access to their own infrastructure. The API they expose to third parties is a weak, thin version of the private tool.

But not Twitter: it gave first-class access to all comers, and developers threw their resources into the project of building all kinds of ways of accessing Twitter. Some of these may be familiar to you, like TweetDeck, which Twitter eventually acquired and brought in-house. Others were strictly “programmatic”—tools that made it easier for other developers to do cool things with

Twitter, like operate bots that answered queries, told jokes, or automated public safety announcements.

Twitter also paid close attention to its users. Users invented “retweeting” by typing *RT* and copying and pasting someone else’s tweet into the composition box. Twitter noticed this and automated the process, creating a one-click system for retweeting anything on the system.

Many of Twitter’s core features were developed in this way, including “quote tweeting,” typing some commentary on a tweet, then pasting in its link and the #QT tag. (Twitter now automates this process as well.)

Developers call this “paving the desire paths.” That’s a reference to a design principle from physical spaces like parks and campuses. Landscape architects look for places where people have worn the grass thin by cutting across lawns and fields (desire paths) and formalize them by leveling them and paving them or putting down gravel, wood chips, or some other material.

Taken together, these two policies—first-class access to the Twitter API and integration of users’ own innovations—constitute a system of generous value sharing with both business customers (who could create a variety of tools for themselves and for users) and users (whose workarounds were observed and turned into official features).

People loved using Twitter. It was playful. It was fun. It was a party that the whole world was invited to.

## **Stage Two: Good to Business Customers**

But from the start, Twitter also made compromises. When Twitter added advertisements to its service in 2008, it made the decision to open local sales offices in countries around the world,

including nations like Türkiye, where governments could be relied upon to make censorship and surveillance demands.

This was a way of shifting surplus from users to business customers. Turkish advertisers didn't *need* to do business with a Turkish Twitter office, but opening offices in-country made that more convenient for Twitter's business customers. However, it also put Twitter employees and bank accounts within reach of Türkiye's authoritarian government, which used that reach to compel Twitter to do things that were harmful to its users, like revealing information about the identities of dissidents and removing their speech. (Despite this, Twitter continued to operate at a loss.)

Twitter also engaged in other forms of stage-two enshittification, notably in the staffing of its content moderation division. Content moderation on giant platforms like Twitter is always going to be a difficult proposition, but the more a company spends on moderators, the more moderation it can do. As Twitter's user base and volume of posts grew, the company *did* enlarge its moderation team, but not at a rate to match its overall growth. That meant that the ratio of moderators to activity worsened over time.

Of course, all of this was characteristic of Twitter 1.0, the private company that was later taken public through an IPO and governed by a shareholder-voted board of directors. This arrangement was far from ideal, but compared to what happened next, it was practically Eden.

In 2022, Elon Musk assumed ownership of Twitter. Musk had to borrow \$22.4 billion to fund the acquisition. That vast debt exerts enormous pressure on Musk to extract money from Twitter. Remember, shareholders *prefer* to get paid by the companies they invest in, but their ability to compel the companies they invest in to pay them is limited to voting for company directors who'll appoint CEOs who'll agree to give the company's money to its investors, rather than spending it on product maintenance and

development, wages for staff, improved infrastructure, or executive bonuses. But creditors who hold a company's debt are *entitled* to regular payments on that debt, and if the company stiffes them, they can ask a court to force the company to cough up, and if the company doesn't have enough money and can't borrow or raise it, they can force the company into bankruptcy.

By taking on tens of billions of dollars in debt, Musk was setting the company up for a world of hurt. Twitter (or, for some reason, X) will need to come up with *large* sums of money every year to service its debts, or its creditors can kill the company.

(Of course, if they do that, they will wipe out any chance of getting paid back. Forcing the company into bankruptcy would likely mean a fire sale of Twitter to someone else, with a share of the proceeds going to the creditors. By contrast, if they let Musk stiff them, they at least have the hope of getting paid in the future if he turns the company around—or if he makes it structurally important to a future federal government, as Musk was actively trying to do with the second Trump administration as of early 2025.)

There's not much to be gained by trying to read the minds of tech CEOs to determine which of their espoused views are sincerely held and what they're merely saying to win points with some group of users, customers, lawmakers, investors, or peers. And honestly, it doesn't matter whether Musk's strident pronouncements about gender politics, "wokeness," and other subjects are his true feelings, transient blurts, or acts of calculated image-crafting.

### Stage Three: A Giant Pile of Shit

Rather than playing Twitter Kremlinology, let's instead look at how Musk's handling of Twitter post-acquisition is an example

of how an enshittification speedrun can boomerang on the enshittifier—and how those bad choices can nevertheless inflict serious harms on users.

Musk's tenure at Twitter's helm is best understood as a rapid, indiscriminate, and clumsy series of value transfers from end users to Twitter (which is to say Musk, his investors, and his creditors).

At the outset, Musk shed the vast majority of Twitter's content moderation team. These workers were charged with maintaining an environment that was both hospitable to users and "brand-safe."

This is an absurdly difficult balancing act. Life is not brand-safe, and many of the least brand-safe parts of our lives matter the most to us. When platforms seek to ensure that their advertisers' materials only run alongside uplifting user content, they have to suppress or block users' posts about their sex lives, their political fears, or the disasters they're in the midst of.

While users don't necessarily want the platforms to block their own frustrated or angry posts, they also don't want to be abused, dogpiled, or doxed. They don't want their feeds filled with unsolicited gore, sexually explicit content, or extremist hatred.

So moderators have to figure out how to trade off the interests of advertisers against the sensitivities of users.

On top of that, moderators are charged with weeding out bad ads—frauds and scams, paid disinformation, and ads for illegal products—as well as weeding out bad non-advertising content like spam, scams, and *unpaid* (but coordinated) disinformation.

No platform does this well. Pre-Musk, Twitter was somewhere in the middle of the pack, having made its share of high-profile gaffes and missteps, but also routinely blocking millions of posts of the sort that it intended to block, consistent with its own decisions about the interests of users and advertisers.

Getting rid of the moderators made Twitter instantly, permanently, significantly worse for both users *and* advertisers. Users were—and are—inundated with ads for scams, counterfeits, and hoaxes. Advertisers find their messages attached to posts featuring gore, Holocaust denial, and pornography.

Everybody loses.

Including Twitter. This is where things get weird. For all that Facebook has strip-mined its service, sucking out the value that its business customers and end users created, it did so gradually. Facebook remained (very) profitable, even through its missteps.

But under Musk, Twitter speedran the enshittification curve, and it removed value so quickly that it sparked a mass exodus of advertisers and a collapse in revenue that more than offset any savings from firing the workers who maintained quality under the old guard.

Again, I'm not going to try to peer into Musk's state of mind here. He frequently claimed that his actions were in service to his appreciation of free speech, and at one point publicly swore at a roomful of executives of companies that advertised with Twitter who'd gathered for a *New York Times* summit, telling them that he didn't want their money if it was contingent on a well-moderated Twitter. In the profane onstage rant, Musk personally singled out Disney CEO Bob Iger, telling him "Fuck you" and "Go fuck yourself."

This is, at the very least, evidence that the subject of free expression rouses strong views in Musk. Nevertheless, his record on free speech and moderation has been poor. He's booted journalists who criticize him, caved to censorship requests from oppressive governments with poor human rights records, and pursued a vendetta against an account that published public records about the movement of Musk's private jet. In the first days of the second Trump administration, he suspended users who

identified government contractors whom Musk hired on behalf of the so-called Department of Government Efficiency (DOGE) and gave unsupervised access to sensitive government payment systems.

One of Musk's first official acts was to sell "verification"—that is, blue tick marks—to all comers. These blue ticks were initially created by (old) Twitter as a way of helping users spot fake accounts. Twitter users who had a high public profile and were worried about being impersonated on the platform could apply for a blue tick, which was awarded after a dedicated Twitter team took some steps to verify the account's authenticity.

This was a far-from-perfect process. Twitter's standards for notability were opaque and unevenly applied. Behind the scenes, Twitter's verification process was a sloppy mess.

In 2011, I myself was impersonated on Twitter by a user who created a fake account to attack others as me and to post false information about me. I wrote to the company and was told that it would take action against the impersonator only if I applied for verification, and that doing so entailed *faxing* the company a copy of my driver's license, because "email isn't secure."

When I told the people at Twitter that I couldn't send them a fax because my time machine was broken, they had a ready answer: yes, many users don't have fax access, but here's a free email-to-fax service run by some parties unknown. Just email your driver's license scan to this address and *they'll* fax it to us.

I was living in Europe at the time, so I wrote to a friend at Twitter and pointed out that this was *radioactively* illegal under the EU's General Data Protection Regulation. A few weeks later, Twitter changed its policy and let me send in a scan of my driver's license by email. Shortly thereafter, I got my blue tick and the impersonation account was deleted.

But under Musk, this verification process was swept away entirely. Users could receive a blue tick by paying a monthly fee, which rose steeply for businesses such as publishers. After a grace period, all the “legacy” blue ticks were deleted.

Again, this was a measure that clawed away value from business customers *and* end users. Business customers had to pay a monthly fee to fight impersonation. End users found themselves deceived by pranksters and fraudsters who bought blue ticks to lend verisimilitude to their deception.

Musk continued to turn the screws. Users who didn’t pay for blue ticks had their posts suppressed on the platform—meaning that their posts were less likely to be seen by other users who followed them, or to be recommended to strangers—while users who paid were prioritized and had their posts shoved into other users’ feeds across the platform.

This was a godsend for fraudsters, griefers, and other bad actors, who could put shock images or fraudulent solicitations at the top of millions of strangers’ feeds.

But for legitimate business customers, having to pay a fee to reach the people who’d asked to hear from them was a double insult. On the one hand, Musk had been vocally contemptuous of the press, which muddied the waters as to whether the fees he demanded were a form of ritual humiliation or merely a way to ransom publishers’ subscribers to them. On the other hand, the proliferation of fraud and trolling among blue ticks meant that publishers who bought a blue tick actually made themselves look *less* reliable. (Musk eventually “solved” this by adding a feature that let users disguise the fact that they were paying him, which speaks volumes about the message that his new blue ticks sent.)

Users suffered as well: the quantum of content in their feed that they had asked to see, or that the algorithm predicted they

would enjoy, dwindled to a bare minimum. This left a void that could be filled with ads and artificially boosted posts from blue ticks (which, again, were likely to be ads, frauds, gore, or porn).

Musk's leadership since has continued in this vein. While the public attention focuses on the flashy changes, such as renaming the company the letter X, the most consequential changes have to do with making things worse for users, while keeping users locked in to the platform. (After all, if users are still locked in to the platform, they'll keep at least some advertisers stuck to it as well.)

For example, in 2022, Musk suspended some high-profile Twitter users and stated that this reflected a new policy prohibiting users from listing their accounts on rival platforms (like Mastodon, Bluesky, and Threads) in their bios, usernames, or posts.

This step coincided with measures that blocked many business customers from using Twitter's API, and made API usage far more expensive for those who were still able to use it. Remember, Twitter started out as an API-first company, designed to be built upon, tinkered with, improved, and extended by a constellation of complementary companies, tinkerers, and users.

Together, this ban on publishing off-Twitter "forwarding addresses," coupled with severe API restrictions, killed off the burgeoning ecosystem of automated tools to help users migrate off Twitter. These tools (such as Twitodon and Fedifinder) requested your Twitter login, then used the API to pull down a list of all the accounts you followed and added them to the people you followed on Mastodon.

If all of that sounds confusingly technical, let me describe the process from *your* point of view. Say you get tired of Twitter, so you set up an account on Mastodon, a Twitter-like service that is built on open-source software and has lots of different servers

you can sign up with, run by individuals, companies, co-ops, and nonprofits.

So now you have a Mastodon account *and* a Twitter account. You log in to a migration tool and tell it how to find your old Twitter account and your new Mastodon account, and click “Go.” A few minutes later, your Mastodon account has been updated to follow everyone you know on Twitter who has also set up a Mastodon account.

When Musk targeted this practice, he made it clear that he viewed his path to profitability as depending on making it hard for users to leave.

In the years since, Musk has introduced a series of “anti-features” that give users and/or business customers plenty of reasons to quit. For example, in 2023, Musk abruptly altered the way that link previews worked; tweets that contained web links would automatically feature an image but no header or text snippet from the linked page.

Headers and snippets helped users make better estimates of whether they wanted to follow a link before clicking it. But they were even more important for publishers, a key constituency of Twitter’s business customers, whom Musk hoped he could coerce into paying high monthly “validation” fees. By stripping headers out of link previews, Musk drastically reduced the likelihood that users would click on the links, resulting in a near-total collapse of readership coming from Twitter posts. Publishers that had spent years cultivating a large Twitter subscriber base in order to drive traffic to their sites took a huge monetary loss from this decision.

Around the same time, Twitter also rolled out extremely long posts, with extensive formatting options. Musk then told publishers who were worried about collapsing Twitter traffic that they should reproduce the contents of their websites in very long tweets. Of course, this would mean eschewing the subscription

and advertising revenue publishers got on their own sites. (Musk offered them a share of the revenue from the content on the site, contingent on their paying for validation and calculated using a complex and opaque formula.)

Again, this is the same tactic that Facebook tried, but Facebook did it by degrees . . . and did it *first*. When Musk tried it, publishers were already familiar with this snare, and they declined to stick their feet in it.

Eventually, Musk had to back off: later in 2023, he announced that he would add blue ticks to “prominent” accounts that had enough followers. These were typically accounts that had been “verified” under the old Twitter management. A very small number of these verified users had chosen to pay to keep the status under Musk, and, after months of moribund sales, Musk suddenly and nonconsensually gave these users a tick mark that had come to mean “I am someone who tolerates—or even likes—Musk’s unhinged management of Twitter and/or his personal views on race, immigration, gender, and workers’ rights. I am voluntarily giving money to the Hitler-salute guy, every month.”

This was yet another impetuous, irrational policy U-turn for Musk. His initial gambit had failed: he didn’t get hundreds of thousands of internationally notable people to pay for blue ticks, thus creating a penumbra of desirability around his flagship product that would lure in millions of everyday people to splurge on blue ticks of their own.

Without the cohort of notable and verified pre-Musk blue-tick users, the blue ticks became associated with spam, porn, trolling, and fraud, which made them especially unattractive for everyday users *and* the influencers who Musk hoped would bring in business.

Musk’s restoration of (unpaid) blue ticks to the original cohort

now takes on a desperate air—like he’s hoping that he can dilute the cesspool that most people associate with blue ticks until they become a credible product. At the time of this writing, this gambit is failing, and I am reasonably certain that it will continue to be failing by the time you read this, notwithstanding Musk’s increasingly alarming early-2025 role as shadow president of the United States.

But there is one respect in which Twitter is thriving: it complements Musk’s financial influence by giving him a huge megaphone. In combination, Musk’s money and his platform have allowed him to establish himself as a kingmaker, “first bro” to Trump and key political ally for far-right figures around the world, whose ideology universally involves wrecking things, safe in the knowledge that the people who care about these things can’t escape.

I could go on for pages more about the various enshittificatory gambits that Musk has assayed on Twitter, but that would be beside the point.

I don’t recite Musk’s fumbles to make the point that he is stupid and incompetent (though, for the record, I think he is both very stupid and very incompetent). Rather, this is all to build up to the following:

People still use Twitter.

Hundreds of millions of people are wading through the enshittification, which rises every day, and continuing to use the service. All kinds of people continue to use it: The marginalized groups that have endured racist, gendered, homophobic, and transphobic hate campaigns are still there. So are the journalists whom Musk denigrates with every opportunity, and whose work he has gone to great lengths to devalue. So, too, are the performers who espouse progressive values antithetical to those that Musk promotes on the platform. Even people on Mastodon or

Bluesky are usually maintaining their Twitter accounts. Same for the millions of users who were bootstrapped onto Meta's Twitter clone, Threads. People who deplore Musk's politics, his reckless and unlawful seizure of entire US agencies, his firehose of lies, and his support for neo-Nazi parties all over the world are still using Twitter.

As of this writing, I'm still on Twitter.

Why are we still there?

Switching costs. Collective action problems.

Think of the parallels to the offline world: Why do marginalized groups stay in regions where they are openly despised and subject to harassment and discrimination? Because if you have to live with continuous harassment and discrimination, you absolutely rely on your community for your sanity.

The only thing worse than being a member of an oppressed minority is being an *isolated* member of an oppressed minority.

A community—or, for a creative worker, an audience—is a vital lifeline, but it's also an anchor. It's impossible to overstate how hard it is to coordinate an exodus of people, even people who love and rely on one another, even when things are terrible.

I call this the *Fiddler on the Roof* problem. In the musical, we meet a group of Ukrainian Jews living in a shtetl called Anatevka. Anatevka isn't a very nice place to live. It's poor, it's primitive, and, of course, it's subject to the czar's Cossacks, who ride through the frame every fifteen minutes or so and kick six kinds of shit out of the Anatevkans.

So why do the Anatevkans stay put? We learn the answer to that in the melancholy final scene. The czar has finally pulled the plug on Anatevka by ordering a purge of all the Jews. As the villagers make ready for their departures, they have one final farewell:

LAZAR: Tevye! Tevye, I'm on my way.

TEVYE: Where are you going?

LAZAR: Chicago, in America.

TEVYE: Chicago, America? We are going to New York, America.

LAZAR: We'll be neighbors. My wife, Fruma Sarah, may she rest in peace, has a brother there.

TEVYE: That's nice.

LAZAR: I hate him, but a relative is a relative.

It's quite a tearjerker! We have spent the past three hours coming to understand just how much these people rely on one another to get through their brutal, impoverished daily lives. Now we must reckon with the fact that they are going on to a new stage of their lives—one that will be every bit as brutal and impoverished, with the difference that they won't have one another to help.

That's why people are still on Twitter. It's not that they like the service—it's that they like *one another*. And leaving one another is especially hard in moments when things are especially terrible—say, when Elon Musk and Donald Trump are dismantling whole swaths of the US government in a blatantly undemocratic way. Those moments of existential terror are exactly when you need your community the most.

Enshittification—deliberately worsening a service—is only possible when people value that service to begin with. Enshittification is a game of seeking an equilibrium between how much people like the thing that locks them to the service (often, that's other people) and how much they hate the management of that service.

Twitter is a cautionary tale. It tells us that the “market forces”

that we'd expect to kill off services that turn into piles of shit have been neutralized. We are living in an age of zombie platforms: platforms that shamble on long after they should have been double-tapped and stuffed in a shallow grave.

The force that animates those zombies is desperation: not the desperation of the platforms' owners; rather, the desperation of the platforms' users and business customers, who can't live without one another and don't know how to leave without losing one another.

I have some ideas about that, which I'll get to in Part Three's "The End of Self-Help."

**Part Two**

# **The Pathology**



By now, you should be familiar with the *symptoms* of enshittification.

The next step is to examine the body corporate, and establish what *internal processes* cause these symptoms. This is the pathology of enshittification.

This is an urgent question. We are living through a Great Enshittening. Somehow, humans have unleashed the Enshittocene, in which all of our artifacts and hyperobjects are turning into piles of shit. What is it about this moment that allowed this contagion to spread so fast and so far?

Some will tell you that this is just the end of the zero interest rate policy (ZIRP), which followed on from the Great Financial Crisis of 2008, when central bankers around the world cut interest rates to zero (at times even tipping them into negative territory). The end of the era of “free money.”

When the prime rate goes to zero, it becomes very cheap for companies and their investors to borrow, and so, the theory goes, they have a lot of money to throw around on goodies like ad-free search or social media that shows you the things you want to see instead of the things that make money for the platform. When central banks raised interest rates, companies were no longer able to spread that free money around, so they flipped a switch and went from giving goodies to end users and business customers to bleeding them dry.

Another theory: Once, the great tech platforms were run by their heroic founders, who were men of vision. Whatever their merits or flaws, these founders believed in their companies' mission, and frequently (if not universally) made decisions that traded off their shareholders' short-term interests for the quality of the company, which would stand as their lasting legacy. However—goes the tale—these founders were but mortals, and eventually, the pressures of leadership grew too onerous and they stepped aside. The trusted lieutenants who moved into the CEO's office weren't visionaries; they were bean counters, elected by the board to serve the shareholders above all else.

A final theory: Mercury has entered into retrograde, and so everything has gone to shit.

I think all three of these theories are wrong.

On ZIRP: Yes, it's true that companies have less free money to hand around than they did a few years ago, and doubtless that plays into their calculations about whether and how hard to enshittify their products and services. But ZIRP ended in 2022, and that was *years* into the enshittification pandemic. Facebook started enshittifying a decade ago. Uber and Amazon started going rotten at least five years ago. ZIRP may be accelerating the enshittification of some companies, but it's not *causing* it.

What about those heroic founders? Again, the evidence doesn't support the claim. First, some of these companies are still run by their founders. Take Meta: Not only is Zuckerberg still running that company, he also still controls a majority of the voting shares. (Meta, like Google and some other tech giants, has a two-tier share structure in which only some shares get a vote on the company's management, and these shares are disproportionately held by the company's founders.) Zuck's not just the CEO of Meta; he's its ruler for life. Even more damning: Google actu-

ally got markedly *worse* when cofounder Sergey Brin returned to oversee the daily management of the company in 2023 during its AI “pivot.” So no, I don’t think this is about a change in leadership.

That just leaves Mercury in retrograde, something I just can’t bring myself to take seriously. After all, I’m a Cancer, and as everyone knows, Cancers don’t believe in astrology.

So what explains the Great Enshittening?

Here’s where the pandemic metaphor helps us again. When a whole population starts to change in the same way at the same time, it’s a sign that something *external* and *systemic* is underway. Rather than looking for the origins of enshittification inside the companies, we should look at the world the companies operate in.

One way to start is to ask, “Why *don’t* companies enshittify?” After all, companies would like to charge as much as possible for goods and services while spending as little as possible on . . . anything. They would like to pay the lowest-possible wages, offer the lowest-possible quality, and sell at the highest price they can name.

When you put it that way, the answer is obvious: Companies can’t enshittify to their heart’s content because it wouldn’t work. Workers would quit over low pay. Suppliers would stop shipping product over unpaid invoices. Customers would balk at high prices.

In other words, companies don’t enshittify when they *can’t* enshittify.

Which means that companies start to enshittify when they *can*.

In other words, anytime you see good products produced ethically and offered at fair prices, it’s because the world from which those products emerged punishes cheating: low quality,

poor labor practices, and high prices all cost the company more than it stands to make from indulging them.

So let's talk about what stops companies from enshittifying.

There are two forces that act on every company in every industry: *competition* (markets) and *regulation* (governments).

## The Discipline of Competition

On average, a company that operates in a competitive market will make better products, at better prices, under better conditions, because failing to do so will cause its customers, workers, and suppliers to go elsewhere. If a company ignores this possibility, then, on average, it will fare poorly. If it continues to ignore this lesson, then it will likely fail altogether.

## The Discipline of Regulation

Likewise for regulation. When a company understands that cheating its customers, suppliers, workers, or community will result in fines that exceed the savings from cheating, the company will cheat less. Companies that continue to cheat will see more and more of their income diverted to fines and court costs, and, if they don't learn their lesson, they, too, will likely fail. Even if the fines don't kill them, the regulator might, imposing a corporate death penalty that sees the company's charter revoked, its assets seized, and even its executives imprisoned.

Every company, irrespective of sector, can be disciplined by competition and regulation.

But two other sources of discipline exist that are unique to tech: *self-help* and *tech workers*.

## The Discipline of Self-Help\*

Let's start with self-help. Digital computers are marvelously flexible in a way that non-computer scientists seldom grasp. Technically speaking, every computer you use is a "Turing-complete, universal von Neumann machine." This is mid-century computer science jargon that I could spend a whole book explaining. (The giveaway is the names of those two wartime computer scientists Alan Turing and John von Neumann.) But the bottom line is this: *Every computer we know how to make is capable of running every computer program we know how to write.*

That is, computers are universal. There is no known practical way to make a computer that only runs the programs its manufacturer approves of. If there were, we'd make computers that were incapable of running ransomware and spyware and other malware.

The implications of this universality are really the story of the past forty years. For one thing, the fact that every computer can run every program means that there's a nearly infinite coalition of industries that benefit from (and invest in) faster and better computers. The faster, cheaper chips that make your phone do more also go into your car and your thermostat and your medical implant.

This also means that every kind of *thing* we use is increasingly computerized. Chips are so cheap, so plentiful, and so flexible that we stick them into everything we use.

That digital flexibility is key to enshittification. The core mechanic of enshittification is a continuous series of adjustments to the "business logic" of a service—how much it charges, how

\* If you're not an economist, the term *self-help* might make you think of juice cleanses and daily affirmations, but in econospeak, self-help is a policy that allows people or companies to fix their problems by themselves, rather than appealing to a regulator, an enforcer, or a third party. Think of it as the economic equivalent of Florida's "stand your ground" law.

much it pays, how it ranks search results, and so on. That's how companies can start charging for things they once let you do for free, and how they can apply those charges selectively to different users and business customers, at different times.

But, as with network effects, the flexibility of digital tools is a double-edged sword. The fact that every computer can run every valid program means that every enshittificatory gambit has a potential disenshittificatory countermove.

That means that every time HP raises the price of ink, it invites third parties to reverse engineer its printer cartridges and make a compatible cartridge. These third-party ink cartridges don't just threaten HP's current practice of gouging you on ink; they potentially sever the relationship between HP and its customers forever. Once you're buying your ink from a third party and enjoying the quality and value of its products, you might find yourself buying your next printer from that third party as well. That's what happened when Lexmark—then the printer division of IBM—tried to kill a Taiwanese toner-cartridge remanufacturer called Static Control Components. The courts refused to block Static Control's cartridges, and today Lexmark has been absorbed into Static Control.

While it's unlikely that HP is going to end up being bought out by a tiny Taiwanese toner-cartridge refiller, HP still has to worry that once you discover the existence of cheap, reliable third-party ink, you'll stop buying HP cartridges forever.

This carries over into every part of digital business. Imagine this: You're in a product meeting for a company's website. The head of the company's product group says, "All right, folks, here's something I've been noodling with. You know how our KPI\* is based

\* Key performance indicator—a benchmark used by companies to determine promotions and bonuses (or suspensions and firings).

on the gross revenue from ads on our website? Well, I've been doing some scenario projections, and I think that if we make our website's ads 20 percent more obnoxious, we can goose topline ad revenue by 2 percent. The bonuses from that will pay for all of us to take our families skiing in France this Christmas. Who's with me?"

At that point, someone in that meeting, someone who doesn't care *at all* about product quality or the well-being of the company's customers, will still stick their hand up and say, "All right, Elon, I love how you think, really, but here's something you haven't considered. If we make our web ads 20 percent more intrusive, 40 percent of our users are liable to go to a search engine and type, *How do I block ads?* When they do that, the revenue from those users won't rise by the 2 percent you're projecting. They won't even stay at the current baseline of 100 percent. Instead, the revenue from those users will fall to *zero, forever.*" After all, no user ever goes back to the search bar and types, *How do I start seeing ads again?*

The flexibility of computers makes them *interoperable* in a way that no other technology can match. Physical limitations make it hard to impossible to swap the engine block or transmission between two manufacturers' cars. Mixing and matching the attachments from your vacuum cleaner, food processor, or electric shaver requires access to a machine shop or a plastic molding setup. But once someone writes a program that connects two computer systems, anyone can install and run that program.

Sometimes, these programs are made with the cooperation of the original manufacturer. All kinds of companies make use of standards, like the standards for Wi-Fi, Bluetooth, and USB, and make gadgets, programs, and systems that can be mixed and matched with other vendors' products. As discussed above, companies offer APIs to invite third parties to interoperate with them.

But sometimes, interoperable programs are made against the wishes of the original manufacturer. A whole suite of

guerrilla tactics—bot building, scraping, reverse engineering, decompiling—can be deployed by would-be interoperators to unilaterally connect to another vendor's products.

You have used these products, possibly without knowing it. For example, if you've ever used Apple's iWork apps (Pages, Numbers, Keynote), you've benefited from this *adversarial interoperability*. Apple technologists made these apps by reverse engineering Microsoft Office (Word, Excel, PowerPoint) so that they could read and write its file formats. After a short but bitter fight, Microsoft surrendered and standardized its Office formats so that anyone could implement them. That's how you can paste data between Microsoft Office, Google Docs, iWork, and programs like LibreOffice (the program I used to write this book).\*

Adversarial interoperability is the key to self-help. The fact that enshittification can always be reversed with a disenshittifying counter-technology always acted as a brake on the worst impulses of tech companies. The threat of adversarial interoperability meant that even when companies didn't care about treating their customers fairly, they still had to *act* like they did, lest those customers avail themselves of a rival's interoperable product and sever the relationship between the enshittifying company and its customers . . . forever.

## The Discipline of Tech Workers

The tech labor market is unique. For many decades, tech workers have enjoyed a tremendous amount of labor power, despite working in a sector with extremely low union density.

\* I have a *lot* more to say about interoperability, especially adversarial interoperability. For more, check out my 2023 Verso book, *The Internet Con: How to Seize the Means of Computation*, now out in paperback.

Unions give workers power by solving their collective action problems. When workers bind together into a single bargaining unit, their bosses can't play them off against one another in order to erode their wages and working conditions.

But tech workers' power came from another source: scarcity. For most of modern history, the tech industry has demanded far more tech workers than the world could supply. This shortage could not be overcome, no matter how much work tech bosses offshored, no matter how many workers they brought in from overseas.

Tech workers understood that their bosses needed them more than they needed their bosses. They knew that they could quit anytime, walk across the street, and get a job that was just as good, or better, with a rival firm. (It helped that the center of the tech industry was Silicon Valley, because the California state constitution bans noncompete agreements.)

Tech workers knew this, and their bosses knew it. Tech workers knew their bosses knew it, and their bosses knew that their workers knew it.

Scarcity gave tech workers enormous bargaining power, so tech bosses got creative. Rather than motivating their workers by threatening them with replacement by more desperate workers willing to accept worse pay and conditions, tech bosses discovered a different, winning strategy: inculcating a sense of *mission* into tech workers.

The self-mythologizing of the tech sector was hugely beneficial to tech bosses. By framing every tech worker as a temporarily embarrassed entrepreneur, a founder-in-waiting who was only drawing a salary to pay the bills until they founded their own startup, tech bosses were able to convince tech workers that they weren't *workers* at all. Perhaps the bosses even believed this!

Tech bosses converted their workplaces into whimsical

“campuses” with gourmet cafeterias, luxury fitness centers, free dry cleaning and massages, and egg-freezing services so that tech workers could stay on the job through their fertile years without ever taking parental leave.

It worked.

So long as all this set dressing was accompanied by high-minded slogans—like Google’s “Don’t be evil” and Facebook’s “Connect every person in the world”—tech workers could tell themselves that they were pampered geniuses rather than patsies who’d been gulled into working like government mules.

There’s a name for this strategy, coined by the librarian-theorist Fobazi Ettarh: *vocational awe*. Ettarh uses this term to describe the weaponization of workers’ sense of duty, especially to the public those workers serve. For Ettarh, vocational awe is why teachers, nurses, hospice care workers, and, of course, librarians accept poor pay and conditions without rebelling. They feel a sense of duty to their students, patients, and patrons, and their bosses don’t, and everyone knows it. So long as workers believe that their boss would rather harm the people they love and care for rather than increase their pay, they are held hostage by their own sense of duty.

On the face of it, tech workers are odd candidates for vocational awe. After all, the popular conception of tech workers is as “shape rotators,” people who are primarily motivated by the interior pleasure of solving ferociously complex logic puzzles.

But for many tech workers, their journey started with a passionate love affair with digital technology and the people and systems they could access with digital networks. Historically, the tech industry boasted a large cohort of workers who saw themselves as part of a revolutionary movement, warrior-monks on a mission to bring about a better, brighter future. The founding ideas and ideals of the internet revolution made this mission real.

For example, the founding principle of the internet itself is the “end-to-end principle.” This is the idea that networks should be designed to transmit data from willing senders to willing receivers as efficiently and reliably as possible. This was quite a departure from the networks that preceded the internet, like AT&T’s “Bell System.”

In the Bell System, you could connect to me only at the sufferance of AT&T. AT&T decided which hardware we could use, thanks to a law that made it a literal crime to connect unauthorized equipment to the phone system. AT&T also decided what kinds of signals could run over its wires. That meant that everyone in America had to rent a phone from the Bell System, paying monthly fees that totaled up to hundreds or thousands of times the cost of the phones in their homes. New devices, from switchboards to answering machines to novelty phones to modems (*especially* modems), existed only at the sufferance of the Bell System, and on terms that did not threaten its bottom line.

The Bell System was largely stagnant. What passed for innovation at AT&T was touch-tone dialing. When the system added the odd digital service, it always came at a price. For example, when caller ID was added in 1988, Bell companies sold it at the monthly fee of \$6.50.

The end-to-end principle meant the end of rackets like this. A network designed to deliver data between willing senders and receivers as efficiently and reliably as possible can’t support a \$6.50-a-month caller ID system.

Think about it: Once I have a computer and you have a computer and they’re both connected to the internet, then anytime you want to send me something—an instant message, an email—the data about who it’s coming from is built into the system. If my email provider decides to charge me \$6.50 a month to see the “From:” line on your email before I open the message, I’ll just

switch email providers. The monthly cost to the Bell System of delivering caller ID to your phone was \$0 a month. The \$6.50 was pure profit—multiplied by hundreds of millions of Bell System subscribers. Nice work if you can get it.

But not so nice if you're someone who has lots of bright ideas about what you and everyone else can do together with your network-connected computers. If you're a bright young physicist at CERN in Geneva in 1989 and you're noodling around with an idea for a "World Wide Web," you need an end-to-end network to try it out. If you need permission from the world's various Bell Systems, including Swisscom, among the most hidebound and anal-retentive telephone companies in the world (a category with stiff competition!), you might as well give up and go back to physics.

For technologists who lived through the transition to the internet and its immediate aftermath, there was a legitimate, widespread, and justifiable sense of excitement. After decades of stultifying monopoly control, the field of networking—that is, of letting people all over the world interact with one another directly—was exploding. If you had a good idea, you could just *try it* and no AT&T executive in New Jersey could sic the phone cops on you. What a time to be alive!

The years that followed were profoundly exciting, and tech bosses turned that excitement to their end: *See this revolution underway? The accelerating doublings of computer power, of network speeds, of connected users and devices? You can help conjure up the world that's a-borning. You can take the hobby that has excited you through endless sleepless nights hunched over a keyboard and monitor, and turn it into a career—a vocation!*

It worked. Tech workers had vocational awe in spades, though they used other words to describe it. Memorably, Elon Musk called it being "extremely hardcore."

Tech workers, despite their enormous bargaining power, became *extremely* extremely hardcore. Sixty-hour weeks, eighty-hour weeks, hundred-hour weeks? Why not? Put a bed under your desk or in the rafters of the converted Presidio warehouse that's sheltering your startup. Use the company massage therapists, eat the company meals, get a shower and sauna in the company gym. Bring your laptop to the toilet! (Google holds a patent for a laptop-sanitizing, UV-lit shelf next to the handwashing sinks in the company bathrooms.) Working like this is addictive. Work that's this all-consuming feels heroic, and crowds out many of the big, existential questions. Anything you work this hard on feels *important*. Why would you pull those long hours otherwise?

But for tech bosses, there was a huge downside to manipulating workers into spending every waking hour at the office by instilling a sense of mission in them: *those workers felt a sense of mission*. When their bosses told them to enshittify the products they felt a sense of ownership over, having poured their heart and soul into them, they experienced a sense of betrayal and profound moral injury. *No, I won't enshittify the product I missed my mother's funeral and my kid's Little League games to ship on time. I'll quit before I do that—and the guy across the street will give me a job ten minutes later. Go fuck yourself, boss.*

So tech workers constituted a final bulwark against their bosses' enshittificatory impulses. Even as other constraints weakened, crumbled, and fell, tech workers valiantly held the line for their users.

For a while.



## Part Three

# The Epidemiology

Doctors study sick people; epidemiologists study disease itself. Epidemiologists seek to understand why and how a pathogen spreads, causing sickness. In this section, I'll explore the epidemiology of enshittification.

So what happened? One by one, each enshittification-constraining constraint was eroded until it dissolved, leaving the enshittificatory impulse unchecked, ushering in the Enshittocene.

Let's look at how competition, regulation, interoperability, and worker power all slipped away.



## The End of Competition

Competition was the first constraint to go.

Starting with the Carter administration, every US president from the 1970s until Joe Biden's election in 2020 embraced the once-fringe consumer welfare standard theory of antitrust law.

Essentially, Democrats and Republicans alike declined to enforce antitrust law as it had been originally conceived. Companies eventually realized that they were pushing on an open door when it came to forming and maintaining monopolies, and they embarked on an increasingly flagrant monopolization spree.

The most visible symptom of this trend of market concentration was an orgy of mergers and acquisitions. Major rivals married and remarried, forming bizarre group marriages and polycules. They turned on smaller companies and gobbled them in one bite. Whole sectors grew so inbred that they developed the corporate equivalent of a Habsburg jaw. The Reagan era saw a *quarter* of Fortune 500 companies being acquired by another company. Things only got worse from there.

Fifty years later, from eyeglasses to sea freight, glass bottles to payment processing, vitamin C to beer, most industries are now dominated by five or fewer global companies.

The mergers weren't optional. When smaller companies refused to sell to cartel members, the giants had free rein to flout competition law further and insulate themselves from competi-

tion, which would allow their customers to punish them where regulators wouldn't.

Predatory pricing was a favorite technique to keep an independent rival from gaining a foothold. Take the tale of Diapers.com, for instance, a casualty of Amazon's predation. Amazon didn't become the "everything store" by being the best at everything. After Amazon conquered a few key markets (first and most notably, books), it sought out rivals that had come to dominate other verticals that involved shipping things in square cardboard containers and made them offers they couldn't refuse. (Like most other tech monopolists, Amazon is much better at buying things than it is at making things. More on this later.)

Diapers.com was one of those early e-commerce leaders. (No points for correctly guessing what vertical it had come to rule over.) Moreover, Diapers.com was excited for its future and saw no reason to sell out to Amazon.

That wouldn't do. Amazon needed a surplus, so it tapped the capital markets for a war chest and then proceeded to set \$200 million on fire over a single month, selling diapers significantly below cost. In the end, Diapers.com went bust; Amazon picked it up for pennies on the dollar and then shut it down.

For Amazon, \$200 mil was a steal. Not only did it get to corner the diaper market, but it also sent a message to the world: *If Amazon makes you an offer, sell . . . or else.*

Amazon isn't the only company that claims to be an inventing-cool-products kind of business while actually operating as a buying-other-people's-products kind of business. Google is the poster child for this. Twenty-five years ago, Google conquered the global search market by making the greatest search engine the world had ever seen. The capital markets showered the company with cash, but try as they might, Google just couldn't replicate the feat.

Almost without exception, every success Google has had since Google Search was an acquisition, not an invention. Android and YouTube, of course, but also the company's whole advertising-technology (ad-tech) stack, its Google Docs and collaboration products, Google Maps, navigation and satellite images, server management, and customer service—all were other people's companies that Google bought, scaled up, and integrated into its sprawling empire.

To be sure, Google did a lot of work *operationalizing* these products, getting them to run reliably at the company's unimaginable scale. Operations work is important and skilled work, and turning a small successful project into a big, dependable product that hundreds of millions of people rely on is no mean feat.

But operations is not invention. Keeping something running isn't the same as making something no one has ever seen before—something that changes how people live their lives.

Google may be very good at operations, but it's objectively terrible at innovation. Almost without exception, the products Google invents in-house crash and burn—so many that there's a website called Killed by Google that lists hundreds of products that expired on Google's watch.

The one always-reliable Google product was Search. The company's flagship product captured 90 percent of the market, and held on to it. Google is literally synonymous with searching the web, as in the verb *to google*. Though Google didn't invent the idea, most people today probably couldn't name a single search engine that came before Google.

But while Google took over the search market by being better than everyone else, that's not how it retained its position.

As the world learned in 2023, when the US Department of Justice successfully sued Google over its anticompetitive behavior, Google spent tens of billions of dollars per year, year on

year, to ensure that every search box, on every platform, went to Google. Whether you were using a Samsung Galaxy or an Apple iPhone, whether you were searching on Chrome or Firefox, every search went to Google.

This is Google's version of Amazon's Diapers.com caper. The tens of billions of dollars that Google spent every year had a wider effect, far beyond the searches we did on our Samsungs and iPhones. By ensuring that there was no way for anyone to try a better search tool, Google signaled to investors and tech founders that there was no point in even *attempting* to make a search tool that worked better than Google's.

Google's calculus was simple: It could spend billions of dollars every year making sure that even someone who'd tried every other search engine would still prefer Google. Or it could spend a lot fewer billions of dollars making sure that no one ever tried a search engine other than Google. It chose the latter.

Now, spending money to make sure that no one tries your competitors' products is one of those things that existing anti-trust law actually prohibits—but it's also the kind of thing that became normalized thanks to antitrust enforcers routinely ignoring it. Google did this for years, mostly out in the open, and its executives seemed shocked and *affronted* when Biden's DOJ sued the company over it.

Google is maybe the ideal example of how the lack of competitive discipline leads to enshittification. Google may suck at making new things, but it's genuinely good at making other people's inventions work at scale, and for a long time the company bought out its rivals and used them to build a kind of comfortable prison for its users, adding new features that allowed you to do more with its services even as the service performed more invasive surveillance on you.

But as it became clearer that Google couldn't lose—once it

was obvious that neither giant rivals like Microsoft's Bing nor clearly superior startups like Neeva could dent its market share—Google's internal culture started to shift. Top management changed over from technical experts to businesspeople (Sundar Pichai, Google's CEO, is ex-McKinsey). Then those changes rippled through Google's organizational structure, something we see clearly documented in the exhibits in the DOJ's Google lawsuit.

Many Google-watchers have gone spelunking through those once-internal documents and come up with a vivid picture of how the worst people at Google started winning arguments over the company's direction once the company's anticompetitive domination drove complacency.

The best account of Google's internal power struggles comes from Ed Zitron, a PR specialist whose newsletter, *Where's Your Ed At?*, is an indispensable chronicle of the internet's decay. (Zitron calls the tech giants' collective businesses "the rot economy," a term I love.) In a particularly incandescent newsletter installment, Zitron chronicles the rise of Prabhakar Raghavan, Google's head of ads, who was able to sideline Ben Gomes, Google's head of search, at a key juncture. Raghavan hatched a plan to increase the number of search queries we all ran. (The more you search, the more ads Google can show you and the more money it makes.) That plan is shrouded in a lot of business-speak, but it cashes out to this: by making search results worse, Google could force us to run multiple queries before we got the information we were seeking, and make more money by showing us more ads with every search-results page.

In the memos, Gomes—a two-decade veteran of the company—is palpably horrified by Raghavan's proposal to juice search queries by making the answers to each query worse. Gomes made his bones at Google by overseeing the scale-up of

Google Search to run reliably on ever-larger server arrays—in other words, Gomes played a significant role in developing Google’s two key competencies: search and scale. And yet the memos show how he is progressively sidelined by the company’s senior-most managers, who see no reason not to devalue the company’s flagship product to produce shareholder value.

There’s a sense in which this is an ordinary business ploy, no different from, say, a house-paint company that waters down its reliable longtime formula, forcing us to buy two cans of paint and apply two coats where one used to do.

But Google is not just a house-paint company. It’s *the* conduit to the world’s information. It’s right there in the company’s mission statement: “Google’s mission is to organize the world’s information and make it universally accessible and useful.” (This gets a lot less play than the now-retired “Don’t be evil,” but it’s a lot more ambitious and, ultimately, frightening.)

Google is also a company with a sizable cohort of workers who really *believe* in that mission. After all, those workers are also Google users. (So is almost everyone—that’s what a 90 per cent market share means.) And the better Google gets, the better their own lives are, too.

I used to spend a fair amount of time on Google “campuses,” speaking at the company’s conferences or doing a reading as part of the Authors@Google series. (Full disclosure: Google didn’t pay for those appearances, though sometimes there’d be an outside bookseller who’d sell my books to the Google employees who showed up.) I always made the same corny joke to whoever checked me in and showed me around: “Now that I’m inside Google, can you show me the computer where I get to search the *whole* internet?” The point was that Google let *everyone* search the whole internet, and the search engine that you and I used

from our computers at home or our phones on the road was the same one that every Google engineer used. Google's CEO, its founders, and the chair of its board had the same search results. Anything that made search results worse would make their lives immediately worse, too. The people I met at Google were nice, and they were nerds, so they laughed at my joke.

But it turns out that "I get good search results" wasn't the most important incentive for Google's managers. Once the fear of competition had been eliminated, making Google Search worse was a small price to pay for rising stock prices and massive buybacks. I haven't been back to Google since the pandemic, but I wonder if the "Can you show me the computer with the good search?" joke would get the same reaction today. It's hard to believe that Googlers themselves are stuck using the same crummy search as the rest of us.

I'm only half kidding here. In early 2024, I met one day with my novel editor, Patrick Nielsen Hayden, and his wife, Teresa. They are two of my oldest friends—I met Patrick on a dial-up bulletin board system when I was seventeen (!)—and they're also two of the most erudite autodidacts I've ever met, with an encyclopedic knowledge of many wide-ranging subjects, which is to say, I listen to them. Patrick and Teresa sang me the praises of Kagi.com, a small new search engine that requires a paid subscription. The way they described it reminded me of how we'd all talked about Google in 1998, when we discovered a search box that could reliably find you the things you wanted, as opposed to the dominant competitors like AltaVista, Lycos, and Yahoo!, where each query fetched a mountain of ads and spam with the odd useful link far down on the page.

I tried it out for less than a day—you get one hundred free searches—before I was sold. After years of rapidly declining

Google Search quality, using Kagi was almost *sorcerous*. I bought the family plan and texted my wife and kid back in Los Angeles with their own logins and passwords.

But this isn't merely an unpaid, unsolicited endorsement for Kagi.\* The point of this story came a month later, when Jason Koebler, ex–editor in chief of *VICE Motherboard* and cofounder of 404 Media, published a glowing review of Kagi. In that review, he revealed that Kagi was actually *primarily powered by Google*. Kagi was paying Google for access to its back-end servers and its database of web pages, but was applying a different ranking algorithm to the results.

In other words, Google's poor search quality is a *choice*. Anything Kagi's skeleton crew of engineers can dream up to tweak Google's search results is available to Google's army of PhDs. Google Search sucks because Google *wants* it to suck, because when we have to run multiple search queries, Google shows us more ads and makes more money.

But it's not just Google's end users who find ourselves with a worse experience thanks to the lack of competitive discipline. The advertisers who pay Google are also victims here.

During the Google/DOJ trial in October 2023, a lawyer named Megan Gray, formerly of the Federal Trade Commission, reported on a set of odd exhibits presented by the prosecution to those in the courtroom. According to Gray, Google's internal memos documented a system of “semantic matching” that caused ads to be triggered by the keywords the advertiser had chosen *and* similar keywords that Google added on its own.

Gray claims that Google used the semantic-matching technology to invisibly append brand names to queries—for exam-

\* Though it is both unpaid and an endorsement. The only contact I've had with the firm is a brief email exchange with the company founder when he wrote to thank me for publishing a blog post about my experience with the service.

ple, if you searched for *kids' snowpants*, the query might have the words *North Face* silently added to it for the purpose of showing you ads (as though the brand name *The North Face* were a synonym for *kids' snowpants*).

Why would Google do this? Because companies pay Google a *lot* of money to have their ads triggered when you search for a specific company name. And it's not just the company you're searching for that pays to show you those ads. If you search for *coke*, Coca-Cola has to outbid Pepsi and RC and any other soft-drink maker that might want to appear in the results.

For Google, these are extremely lucrative ads, and by semantically matching generic queries to brand names, Google can trigger large, automated payments by advertisers. Depending on your point of view, this is either merely very sleazy, or it's actual fraud. Say a *North Face* competitor promises to pay Google whatever it takes to have ads for its products show up over the query *kids' snowpants*. Google can use semantic matching to treat *kids' snowpants* (a very common query) as if it were *North Face kids' snowpants* (a far more rare, far more relevant query for a *North Face* competitor). Doing so lets Google charge that *North Face* competitor up the wazoo for something it never asked for, while telling it, "Google is only serving your ads to the audiences you've expressed an interest in and paid to reach."

Google later claimed that Gray had misinterpreted the exhibits displayed in court—but it declined to explain what she got wrong or to provide those exhibits for public scrutiny. (Google insisted on—and received—an unheard-of degree of secrecy during its trial, with most of the exhibits under seal and courtroom attendees banned from taking pictures or even typing notes on a computer or phone.)

So it's a bit of a "she said"/"Google said (and refused to explain itself any further)" situation, and it's entirely possible that Gray

got this wrong and Google was doing something perfectly innocent that it declined to explain for . . . reasons. But this semantic-matching business is just the tip of the ad-shenanigans iceberg.

When the majority of US states, led by Texas, formed a coalition and sued Google for antitrust violations in 2020, they, too, were able to demand access to the company's internal memos. These contained many bombshells, but none so consequential as Jedi Blue, the code name for a secret collusive agreement between Google and Facebook that rigged the ad market to raise the price of ads while delivering a lower share of the revenue to the publishers who ran those ads.

Google CEO Sundar Pichai, Facebook CEO Mark Zuckerberg, and Facebook COO Sheryl Sandberg had all personally signed off on Jedi Blue. Not only did this conspiracy rip off Google's and Facebook's business customers—advertisers and publishers alike—but it also blocked competitors from entering the market and offering a fairer deal to either publishers or advertisers.

All this bad behavior—deliberately worsening search results, rigging the ad markets—started once it became undeniable that Google didn't have to worry about losing market share to a competitor.

The secrecy of the Google antitrust trial made sure that the biggest antitrust trial in US history barely registered with the public. But a few memos *did* manage to escape the black hole of courtroom secrecy and make a splash.

None is more indicative of Google's path to enshittification than the notes for a presentation prepared by Google VP for Finance Michael Roszak. Roszak said that this presentation was prepared as part of a "course on communication" he taught, and that he was writing things he "didn't believe . . . full of hyperbole and exaggeration." I don't know Roszak, but I have no reason to doubt him. That said, the memo's contents describe the mindset

that overtakes a business relieved of any fear of competitors: that is, the enshittification mindset.

Roszak wrote: “Search advertising is one of the world’s greatest business models ever created . . . Illicit businesses (cigarettes or drugs) could rival these economics . . . We can mostly ignore the demand side . . . (users and queries) and only focus on the supply side of advertisers, ad formats and sales.” Roszak goes on to claim that Google is “able to ignore one of the fundamental laws of economics . . . supply and demand.” Take Roszak at his word and call this hyperbole—but hyperbole or not, Google is a company that sure acts as though it has transcended the “fundamental laws of economics.”

Google has two great frenemies in Big Tech. When it comes to advertising, Google and Meta rule the internet, and while they may nominally be competitors, they’re also business partners, cooking up sleazy deals like Jedi Blue, CEO to CEO. Google’s other frenemy is Apple, its competitor in the mobile phone duopoly. Apple makes a really big deal out of how it is Not Google, most visibly through a global outdoor advertising campaign touting the company’s commitment to privacy and contrasting that ethos with Google’s surveillance-happy business model.

But then, Apple’s single largest source of revenue is a check for more than \$20 billion that Google writes it every year to buy the default search box in Safari and on the iPhone. That \$20+ billion check is also Google’s single largest expenditure. This deal is brokered and agreed to by Apple CEO Tim Cook and Google CEO Sundar Pichai at an annual summit between the two leaders. For all Apple’s talk of its differentiation from Google and its “surveillance capitalism,” the company has entwined its flagship products with Google’s business in the most fundamental way.

Keep in mind what this deal means: Google (like other surveillance ad companies) maintains a deep, nonconsensual dossier

on the behaviors, social ties, purchases, economic status, employment history, and physical location of virtually every internet user.

The dossier Google maintains on you starts with your search history, one of the most sensitive and revealing sources of data about your innermost thoughts, fears, and intentions. Google is so addicted to this data that it secretly installed clandestine surveillance in Chrome that tracked your internet usage even when you were in “incognito mode.”

In making Google the default search for every iPhone, iPad, and iPod user as well as every user of Safari on a desktop, tablet, or phone, Apple is abetting Google in building and maintaining that dossier.

Which is not to say that Apple’s privacy commitment is all lip service—though it’s still not what it seems. As previously mentioned, in 2021, Apple rolled out a new version of iOS that came with a powerful new privacy option by which users could opt out of *all* commercial surveillance by *all* the apps they used by checking a single box. This had *huge* implications for services like Facebook. Months after the rollout, Mark Zuckerberg issued a warning to his shareholders to the effect that Apple’s new privacy tool would cost the company \$10 billion *in just one year*.

But this privacy story has a twist ending: even as Apple was blocking third parties from spying on its customers, even as it was putting up billboards all over the world trumpeting its corporate commitment to its customers’ privacy, Apple was *secretly spying on its users*. Updates to iOS instituted a system of totalizing commercial surveillance, collecting the very same data that Facebook and its imitators prized so highly and gathered so indiscriminately. Apple gathered that data on *all* its users, not just the less than 4 percent who didn’t check the privacy box. What’s more, it gathered that data for the same purpose Google did: to

feed an ad-targeting network that competed with the Google/Facebook duopoly.

This was a powerful rebuke to advocates of the idea that some companies practice “good” capitalism because they demand that you pay them, while other companies practice “bad” capitalism by spying on you and giving you services for free.

It turned out that “If you’re not paying for the product, you’re the product” was wishful thinking. It was truer to say, “Even if you pay for the product, you’re the product if the company can get away with treating you as the product.”

Take the media Apple sells you through Apple Music, Apple Books, and iTunes: these are all scrambled before they are sent to your phone. The only programs that can unscramble these files come from Apple, and Apple has designed those programs so that they delete the unscrambled version as soon as you’re done with it.

The fact that only Apple apps can unscramble Apple media, and that these apps don’t let you save the media in an unscrambled state, means that you *must* use Apple’s programs to play your Apple media. Naturally, these programs don’t run on Android, so switching from Apple to Android means throwing away all the media you’ve ever purchased.

Of course, you don’t *have* to buy your media from Apple; you could install another app and buy your books, TV shows, movies, and music through that app.

Or you could, *except* for Apple’s pesky App Store policies. Any app that gets accepted to the App Store has to exclusively process its payments through Apple’s system, and that system creams off a *30 percent* commission on every purchase. Thirty percent! For those of you who don’t have to process payments, this is *very* high.

Here’s some context: Most payments go through a cartel of

massive credit card companies (Visa, MasterCard, Amex, and sometimes Discover). These processors have a well-earned reputation as price-gouging scum—for one thing, they have raised the cost of payment processing by *40 percent* since the pandemic, even as their costs declined (and Visa is—as of the time of this writing—the target of a DOJ antitrust enforcement action for monopolizing payments).

The sky-high fees that the payment cartel charges? They come out to *between 2 and 5 percent*. That's *after* a 40 percent pandemic greedflation hike.

Apple charges *ten times as much*. The 30 percent App Tax doesn't just make it hard to do business via an app—for some media, the App Tax makes it *impossible* to run a competing business.

For example, the normal wholesale discount for audiobooks is 20 percent. If you make an audiobook app that allows customers to buy new titles within the app, you will lose money on every sale. (That's why great indie stores like Libro.fm expect customers to use their websites—which are far less prominent than, say, Audible's—to make purchases, though Apple's App Store rules mean that they can't actually *tell* users to buy books on the Libro .fm site or provide a link allowing them to do so.)

Naturally, Apple's own stores are exempt from the App Tax, which means its stores have more titles at lower prices than competing apps.

Media sales are just part of how Apple locks users in to the iOS platform. By bundling default email, calendar services, photos, and cloud services with its devices, Apple ensures that most of its users stand to lose an awful lot if they switch platforms. And since Apple has an absolute veto over which apps you can install on your device, it can block or degrade any app that makes it easy to change platforms and keep your data.

These high switching costs explain how Apple ended up

using its far-reaching platform control to both protect *and* abuse its customers . . . at the same time. When Apple protects you from Facebook spying, it makes the case for you to move into its walled garden and take up residence. Once you're in the walled garden and you've been gulled into putting down roots there, Apple can make life worse for you without worrying too much about losing your business.

Apple isn't the only company that claims to be better than its rivals because it charges money rather than spying on its customers. Apple's not even the only company that does so *while spying on its customers*.

Microsoft is the tech sector's *second* great monopolist—and it owes its existence to the attempt to rein in tech's *first* great monopolist: IBM, a company that was born in a period of lax antitrust, grew larger under robust antitrust, and then found itself in antitrust's crosshairs in the biggest tech antitrust case in history.

IBM was founded in 1911, and it always had a well-deserved reputation as a bully that played hardball with its competitors and pressed its advantage with its customers. Despite this, IBM enjoyed a legitimacy born of its status as a pioneering data-processing company, and also because of its deep ties to the US government and military. As the old saying went, “No one ever got fired for buying IBM.”

In other words, IBM would always have customers even if it delivered subpar products and charged a premium for them. That's what “No one ever got fired for buying IBM” means. It's just another way of saying “too big to care.” So IBM gouged its customers on some of its products, and used predatory pricing, long-term exclusivity contracts, and engineering tricks to prevent competitors from entering the market. The executives who wrote purchase orders for IBM products overpaid for inferior products, but they didn't get fired.

Many of IBM's biggest and most hard-done-by customers were governments and government agencies, including the military. The primacy of IBM in the provision of public services had an ironic and contradictory double effect.

On the one hand, bad experiences with governments that depended on IBM's low-quality offerings undoubtedly lent credence to the story that governments are intrinsically incompetent and that they should outsource all their services to the private sector. It's true: government tech deployment (from the \$2 trillion Joint Strike Fighter to the creaking systems used to hand out stimulus relief during the COVID-19 pandemic) often sucks—but generally the culprit is a government *contractor* from the private sector.

On the other hand, the fact that Uncle Sam (and all his nephews and nieces in statehouses and town halls) trusted IBM to run so many consequential government functions *also* served as a calling card for IBM, generating sales from blue-chip companies that treated IBM's government business as evidence of its reliability.

But by 1970, those government customers had had enough. The Antitrust Division of the US Department of Justice brought a monopolization case against IBM—a case that pitted the US government against its largest (and richest) technology partner.

For the next *twelve years*, IBM spent more on outside counsel to fight the DOJ than the DOJ spent on *all* the lawyers in the Antitrust Division. Every year, year after year, IBM outspent the US government, throwing so many lawyers at its case that the case remained stuck fast for more than a decade.

As expensive as the maneuver was, it was a canny one. IBM outlasted the DOJ, protracting the hostilities long enough to see Ronald Reagan ascend to the presidency. Reagan called off the DOJ, and IBM escaped justice.

But those twelve long years—called “Antitrust’s Vietnam” by Robert Bork, the standard-bearer for the pro-monopoly consumer welfare standard theory—took a toll on IBM’s culture. After more than a decade of having every memo, contract, and deal under the DOJ’s microscope, the IBM C-suite lost its swagger. The company’s executives developed a flinch response to things that would make the DOJ mad.

Which is why, when IBM decided to enter the personal computer market, it broke entirely with its old ways of doing business. Rather than custom-making all the parts in the PC (the “vertical integration” the company had taken so much DOJ heat for), it bought commodity parts on the open market. And when it came time to make an operating system for the PC, IBM didn’t ask its global army of skilled programmers to do the job. Instead, the company approached a couple of kids, Bill Gates and Paul Allen, and asked *them* to provide the OS.\*

Gates and Allen didn’t write the OS, either—they tricked another company into selling them its OS cheap, incorporated a new company called Micro-Soft, slapped the Micro-Soft name on their sucker’s product, and made billions from IBM. Both men became very rich, though Gates got *much* richer than Allen and, even so, schemed to rip off his business partner for a sizable share of his equity in Microsoft. (They ditched the hyphen and the capital S pretty early on.)

Microsoft owes its fortune to the DOJ, and not just because the Antitrust Division scared IBM so bad that it outsourced its operating system. When a company called Phoenix reverse engineered IBM’s read-only memory chip that sat at the computer’s core, IBM looked the other way. In an earlier era, IBM would

\* Tim Wu, “Tech Dominance and the Policeman at the Elbow,” in *After the Digital Tornado: Networks, Algorithms, Humanity*, ed. Kevin Werbach (Cambridge University Press, 2020), 81–99.

have unleashed its most rabid attack-lawyers on Phoenix, but in the wake of their antitrust adventure, IBM's execs had been conditioned not to take overtly anticompetitive actions. As a result, IBM got *competitors*. Companies like Dell, Gateway, and Compaq sprang into existence, building PCs around the Phoenix PC-clone ROM—and then they all bought operating systems from Microsoft.

Microsoft learned precisely the wrong lesson from all of this: that if it could form a large enough monopoly before the DOJ took notice, it could use its war chest to outlast the US government and live to fight another day. Which is exactly what happened. Microsoft used exclusivity deals with PC makers to ensure that there would never be any market oxygen for a rival OS. Why make another OS if every PC maker already has an exclusive contract with Microsoft?

If this sounds familiar, here's what you might be thinking of: Why make a search engine if every search box on every platform belongs to Google?

Then Microsoft tied applications—like Microsoft Office and Internet Explorer—to its operating system. Because Microsoft controlled the OS, it could let its own programs use features that its rivals couldn't access and sometimes didn't even know about. It also tweaked new releases of its OS to deliberately break popular apps that competed with Microsoft products. (The spreadsheet Lotus 1-2-3 was the number one competitor for Microsoft Excel, hence Microsoft's internal slogan "DOS isn't done until Lotus won't run.")

Microsoft owed its existence to IBM's forced conversion from cheating bully to accommodating partner, but the lesson it learned from the IBM affair was that cheating paid. Microsoft was charged with breaking the same laws as IBM, in the same ways, declaring war on the internet itself, creating a string of proprietary alterna-

tives to the public internet that leveraged Microsoft's control over its OS to attempt to dissuade Windows users from joining the real internet in favor of its enshittification-ready walled garden.

When that gambit failed, Microsoft took the war to the browser, sabotaging compatibility with a new, popular browser called Netscape, made by the first firm to successfully commercialize the web browser.

Microsoft succeeded in killing off Netscape by bundling its also-ran, low-quality browser, Internet Explorer, with its Windows operating system. The design of Internet Explorer sank deep hooks into the internals of Windows, making it nearly impossible to truly remove Explorer from your computer and degrading Netscape's operations by denying it access to the same deep OS internals.

History may not repeat, but it sure rhymes. The brazen assault on Netscape prompted Bill Clinton's DOJ to file suit against Microsoft, teeing up another IBM-style battle, this one over the soul of the web.

Like the IBM of 1970, the Microsoft of 1998 had a huge war chest, thanks to the monopoly profits it had extracted from its suppliers and customers. As with IBM's successful delaying tactic, Microsoft drew out its battle with the DOJ until a more favorable administration came into office: Reagan had saved IBM's bacon in 1982, and George W. Bush did the same for Microsoft in 2001.

The parallels don't end there. IBM was scarred by its twelve-year antitrust ordeal, its hostile reflexes so blunted by the DOJ's punishment that it *gave* Microsoft the whole operating system market for the next twenty years. In just the same way, Microsoft's DOJ misadventures shattered the company's nerve for risking the wrath of antitrust enforcers. The disruptive companies that came *after* Netscape were allowed to enter the market with-

out being dirty-tricked by Microsoft. The most notable beneficiary of the kinder, gentler Microsoft was, of course, Google.

The rise of Microsoft, the PC, and Google is a testament to the power of competition to foster innovation. The DOJ's interventions in the market may have been "unsuccessful"—in the sense that the DOJ didn't win the court case and thus wasn't able to force breakups of IBM and Microsoft—but as the saying goes, "The process is the punishment."

Years of bruising courtroom battles, of being haunted by the knowledge that any memo you write or conversation you have could be entered into evidence, of having your top executives deposed for hours on end all take a toll on the culture of the corporation. (Famously, Bill Gates flubbed his deposition so badly that it went VHS-viral, with bootleg tapes of the CEO losing his cool and coming across like a sullen, spoiled brat circulating widely among his peers and enemies—today, the video is online, and absolutely worth watching.) Top executives instinctively shun risky behavior and obsessively color within the lines.

But the lesson doesn't last. The conduct of Microsoft in the years that followed is proof that while even failed regulatory enforcement can produce a one-off reformation in a corporation's character, enduring change requires constant vigilance.

As Microsoft's antitrust lessons faded in its corporate memory, as key executives retired and were replaced by managers who never had to live through a full DOJ colonoscopy, the company reverted to its old ways.

There are many examples of enshittificatory backsliding by Microsoft in the twenty-first century—its video game business, its messaging platform, and more—but the most egregious example is Microsoft Office, the company's flagship productivity suite, composed of Microsoft Word, Excel, and PowerPoint (and, if you squint hard, Outlook).

Long after the Lotus/Excel fights, Office was key to preventing competitors from entering Microsoft's market. In the late 1990s, Office was the cornerstone of Microsoft's war on Apple's Macintosh operating system. Apple had about 5 percent of the desktop OS market, and Microsoft had the other 95 percent. Many users preferred MacOS to Windows, but they found themselves unable to use their Macs, thanks to defects in Microsoft's Macintosh version of Office.

Frankly, Mac Office stank. The files it generated often couldn't be reliably read by Office for Windows, and vice versa. Mac Office users who exchanged documents with their Windows-using colleagues often experienced file corruption as files moved from one OS to the other, a plague of lost text, images, and formatting.

Unless you worked in an all-Mac shop (a rarity even in the subfields that were Mac-dominated, like graphic design, video editing, and pre-press), you, a Mac user, had to routinely exchange files with colleagues who relied on Windows. And even if you worked in an all-Mac shop, your clients, customers, and suppliers probably used Windows. After all, Windows users outnumbered Mac users twenty to one.

The severe impediments that Mac users faced when collaborating with Windows users meant that Mac-curious Windows users rarely made the switch from Windows to Mac. Worse still, Mac users found themselves cornered into switching *to* Windows because their love for the Mac was no match for the hassle and expense of not being able to reliably exchange documents with the 95 percent of the computing world that used Windows.

This is the network effect in action.

For example, the more Uber drivers there are, the easier it is to get an Uber; when more people use Uber, more drivers join Uber. The fact that every rider defaults to Uber means that drivers are skeptical of Uber rivals, and the fact that drivers won't

install rivals' apps means that there's no reason for riders to try those rivals out. Sometimes, you get an also-ran like Lyft, but after an initial bloom, the segment has calcified into Uber and sometimes Lyft, without any market oxygen for new competitors, driver co-ops, or other alternatives.

Microsoft has always been very good at attaining scale through network effects, and then leveraging those network effects to keep its rivals out of the system. No one (except Microsoft insiders, who aren't talking—yet) can say for sure whether Microsoft deliberately introduced defects into the Mac version of Office in order to hurt the Mac, but that was certainly the effect.

Some economists—the “neoclassicals” who defend monopolies as “efficient”—point to network effects and declare that some monopolies aren't just efficient but also *inevitable*. Once Microsoft captured a critical mass of the Office productivity suite market, it ignited a self-renewing cycle in which more people used Office, which made it harder for everyone else to use anything else, so we all used Office, too, which made it even harder to be an Office refusenik.

But Microsoft lost the Office wars in the early 2000s, when Apple reverse engineered Microsoft Office and produced its *interoperable* alternatives: Pages, Numbers, and Keynote (the iWork Suite), which could perfectly read and write Word, Excel, and PowerPoint files.

Interoperability is a powerful counter to network effects. Once Apple released a program that could read and write the files generated by Windows users, then every file those Windows users generated became a reason to *buy a Mac*.

Apple's guerrilla interop flipped Microsoft's network effect on its head. Once you bought a Mac and installed iWork, the switching costs (which are, remember, everything you have to give up to switch from one service to another) fell dramatically. Sure, you

still had to shell out for a Mac, but you didn't have to kiss all your files—and your working relationship with your Windows-using collaborators—goodbye.

Microsoft didn't give up easily. In the years immediately following the release of iWork, Microsoft introduced a flurry of new “features” that broke compatibility with Apple's program. Apple countered by buying each new version of Office, handing it to a team that swiftly reverse engineered those new features and integrated them into iWork, and pushing out compatibility-restoring updates to Pages, Numbers, and Keynote.

In the end, Microsoft sued for peace. The Office file formats were standardized, giving rise to the world we live in today, where Microsoft Office, iWork, Google Docs, LibreOffice, and even the code in your browser all know how to read and write files that can be interchanged between environments.

But Microsoft wasn't done. In the years since, the company has aggressively pursued a “cloud” strategy, encouraging—and then coercing—its customers to move from software that they buy and install, to software that they *rent*, accessing Office and other Microsoft products inside a browser, rather than running it off their own hard drives.

While there's nothing intrinsically wrong with moving functionality from programs on your hard drive to programs that run on remote servers that you access with your browser, the fact that this gives the company that sells you your software the power to alter how it works—and what it costs—every time you use it is a powerful temptation to enshittify.

Cloud software can be wonderful. Rather than installing *another* app on your phone every time you need to do a little one-off task—say, reducing the size of a photo before submitting it to your school's yearbook—you can find a web-based tool that performs that job, use it once, and forget it.

But because cloud-based systems can be endlessly twiddled, they are often the source of pernicious mischief, especially among market-leading companies whose users are locked in and thus unlikely to bolt if the company uses its cloud software to attack its customers.

Take Adobe, the eight-hundred-pound gorilla of graphics software. Like every other tech giant, Adobe attained market share by devouring rivals in anticompetitive mergers, which continue to this day: in 2024, Adobe unsuccessfully attempted to convince regulators to let it buy up Figma, a major competitor whose products are heavily integrated into the workflow of millions of web designers.

For more than a decade, Adobe has aggressively pushed its users to switch from the boxed/downloaded versions of programs like Photoshop and Illustrator to cloud versions hosted on its Adobe Creative Cloud servers.

Again, there are undeniable advantages to being able to summon up an Adobe program you don't normally use for a one-off task, as when a heavy Photoshop user who needs to do a small spot of video editing needn't install Adobe Premiere and can instead pay to access it briefly for that one job.

But because Adobe enjoys so much market power, and can impose such high switching costs on users who have built up vast libraries of files encoded in Adobe's proprietary formats, the mere existence of all those knobs on the back end of Adobe Creative Cloud is a danger to the entire design industry.

Take Pantone colors. In 2022, Photoshop users were informed that they would henceforth need to pay a subscription fee for certain *colors* in their images, and if they didn't pay the fee, those colors would be replaced with plain black in every existing file they appeared in.

Screens and printers render colors in fundamentally different ways. There are some colors you can create by turning on the LEDs behind each pixel that you simply can't create by spraying ink on a page, and vice versa.

The colors you see on your screen are, at best, an approximation of the colors you'll see if you print whatever you're looking at. This isn't good enough for designers, who need precise control over the colors they print.

Designers also use special inks: inks that are embedded with metals, or that glow in the dark, or that are mixed from rare chemicals to give them a sheen or imbue them with Day-Glo pigments. There are even conductive inks that can be used to print circuits on paper!

These specialty inks are called *spot colors*. When a print job calls for a metallic ink, the printer gets a fifth—or sixth, or seventh—ink or toner cartridge that sprays the spot color onto the places where the designer wants that fancy effect.

The specific mixtures of different chemicals to produce every one of these spot colors have been compiled by a company called Pantone. Pantone's main product is a database of spot colors that's analogous to the paint chips you peruse at the hardware store.

When you go to Sherwin-Williams and ask for a gallon of Cyberspace paint (SW 7076), the technician mixes together various whites and grays to make a color that's somewhere between Network Gray (SW 7073) and Site White (SW 7070). The paint can is clamped into the paint-shaking machine, and a few minutes later you're ready to take your gallon of Cyberspace up to the register.

When a printshop gets an order for a spot of Pantone PMS 872 (Metallic Gold), the workers either fit their printer with a ready-made cartridge containing that color or mix a batch from ingredients they have on hand.

In this way, a designer can show a client a book of color chips, agree on a color that can't be reproduced on-screen or with the on-site printers, and send a file to a commercial print house or service bureau. When twenty thousand copies are delivered the following week, the color will look exactly the way the designer promised the client it would.

Pantone is *extremely* central to the lives of print designers, and Pantone knows it. Since time immemorial, Adobe has paid Pantone a handsome annual license fee so that designers who rely on Adobe products can get faithful color when their jobs go to print.

That ended in 2022, when Adobe suddenly announced that it had ceased paying the license fee on its customers' behalf and that henceforth those customers would have to pay the fee themselves, at a monthly charge of \$21.

That was bad enough, but it was just for openers. The main event was what would happen to all the images that Adobe customers had produced in the *decades* that Adobe had been making graphics programs. If you declined to pay the upcharge and then opened one of your images in Adobe Creative Cloud, any Pantone colors would be rendered as black pixels.

In other words, Adobe was stealing the colors out of your images. And because Adobe had long since abandoned the outright sale of its programs, the *only* way to open those images was to subscribe to Creative Cloud and then, separately, the \$21-a-month Pantone color package.

Almost without exception, the entire career output of two generations of print designers was threatened, and every one of them would have to pay monthly rent in order to access their own portfolios.

No one (apart from corporate insiders who haven't come

forward—yet) can say for sure what led to this surreal juncture. Perhaps Pantone demanded a fee hike and Adobe called its bluff, passing the charge on to its customers. Perhaps Adobe got tired of paying its annual fee and demanded a discount, only to have Pantone call *its* bluff.

In the end, it doesn't matter, especially not to the designers who were affected by the move. The point is that none of this could have happened were it not for Adobe's decision to migrate all of its software to the cloud and deny its customers their long-standing right to simply buy its programs and enjoy their perpetual use.

The fact that Adobe *could* revoke the features its customers relied on virtually ensured that it *would*. Eventually, either Adobe would have calculated that its customers were so locked in to its platform that it could delete an essential feature and then recategorize it an "upgrade," or some other monopolist—like Pantone, whose obscure "thin selection copyright" to its color book gives it a federally backed monopoly—would alight on this opportunity to squeeze Adobe's customers.

A company can yield to the temptation to do only those things that are *technically possible*. Likewise, before a corporation *can* be corralled into a course of action that is adverse to its users, that course of action must be *possible* for the corporation.

You can't be tempted or forced to do something impossible. The instant Adobe moved its software to the cloud and eliminated the non-subscription versions of its apps, it put a gun on the mantelpiece. It was only a matter of time until someone opened fire on Adobe's customers with that gun.

Tech companies are wildly reckless about adding capabilities for mischief to their products without taking into account the ways that *other* parties might abuse them. The most obvious

example of this is when tech companies gather and retain sensitive information about their users, only to have that information demanded by oppressive governments that wish their users harm.

But it doesn't stop at governments. When Amazon created its Kindle ebook platform, it included a facility that allowed it to reach into its customers' devices and delete or replace the books they had paid for. Two years later, the George Orwell estate demanded that Amazon use this facility to delete certain copies of *Nineteen Eighty-Four* from its customers' Kindles without telling them. (No, really.)\*

Microsoft once sold ebooks, too. In 2019, it decided that the business was too marginal to continue, so it shuttered its online bookstore, *and* it shut off its digital rights management server. It notified its customers that after April, their books would stop working and offered them a refund on those books.

I spent many years as a bookseller myself, and there was no force on earth that could have required me to break into the homes of the people I sold books to and take those books off their shelves. To do so would have been both outrageous *and* illegal, even if I left some cash on the dresser by way of a refund.

Once a company *can* enshittify its products, it will face the perennial temptation *to* enshittify those products (along with the pressure from investors, board members, and executives to do so). That enshittificatory impulse can come from an external actor, like the Orwell estate or Pantone, or it can come from within.

On June 5, 2024, every Adobe Creative Cloud customer in the world discovered that they had been locked out of the Adobe programs they used to earn their living. In order to regain access to those programs, customers had to click through a new set of

\* Amazon eventually admitted it, and settled a class-action suit.

terms and conditions, granting Adobe the right to use their creative works to train Adobe's AI.

Customers were outraged. The questions of whether AI “art” is good art, or ethical art, or even *legal* art are complicated and unsettled. But one thing was clear even before Adobe's surprise terms-of-service update: many creative workers—designers, illustrators, painters, filmmakers, and so on—are deeply mistrustful of AI art. That got even clearer after Adobe's update, when howls of protest went out across the internet, making international news.

Adobe was clearly taken aback by the reaction. After all, art-hosting platforms like DeviantArt and social media sites with large cohorts of illustrators like Tumblr had announced that they were going to train AI models with their users' creations and weathered the ensuing storms.

But while many DeviantArt and Tumblr users complained or even resigned over AI training, the outrage over Adobe's plans to feed their work to an AI was orders of magnitude more forceful. Creative workers don't relate to Adobe as a company that hosts their creations for public consumption. They see Adobe as a tool, an *essential* tool, and the terms-of-service change prompted a bucket-of-ice-water realization that Adobe was so unafraid of losing their business that it would cheerfully announce that it was going to data-mine every creative work made by every creative professional through their entire career, and if those workers didn't like it, they could pound sand.

Adobe miscalculated. At first, the company went silent, seemingly in hopes that the outrage would run out of steam. Instead, Adobe customers grew angrier, and the technical staff of large design firms started to seriously explore the cost of extracting all their data from Adobe's cloud and switching to obscure, tiny rivals of Adobe. Those companies' products might not be as slick

as Adobe's, and it might take a while for designers to acquire new muscle memory after years of using Photoshop and Illustrator, but if the alternative was Adobe using the files you paid it to host to create a product that was designed to eliminate the need for your services and put your designers out of work, extreme measures were warranted.

After three weeks of this, Adobe blinked. It announced that users had simply misunderstood, that the company would only be scanning users' files for child sex abuse material (more colloquially known as "child pornography"), and that it was very sorry that it had made its customers so mad by assuming that they would interpret the legal changes in a more favorable light.

As apologies went, it wasn't a good one, even by corporate standards. But the impulse to enshittify had been checked by sustained public outcry.

The ability of purveyors of cloud-based products to alter their terms, prices, and features at will enables one of the most beloved enshittification tactics of tech business leaders: bait and switch. If you operate a cloud-based app, you can monitor your customers' every click and keystroke to discover which features are most valuable to your deepest-pocketed users, and then you can remove that feature from the product's basic tier and reclassify it as an upcharged add-on.

The CEOs who do this got their MBAs at Darth Vader University, where the first lesson is "I'm altering the deal. Pray I don't alter it any further." It works with surprising consistency, and tech executives are so confident in the lessons of the Darth Vader MBA that they come over all affronted and hurt when their customers balk.

It wasn't just Adobe. In September 2023, Unity—the world's largest provider of video game development tools, used to model

and animate 3D objects, from heroes to monsters to treasure chests—announced that it was altering its pricing scheme. Beginning in January 2024, successful game developers would have to pay Unity a “runtime fee,” a set amount every time someone downloaded the developers’ games. (*Runtime fee* is a euphemism for *royalty*.)

Game developers are *very* locked in to Unity. Games take a long time to create, sometimes years, and game companies had bought Unity software and created vast quantities of Unity-based game assets based on financial projections that did *not* include splitting the margin from every sale with the company that provided them with the tools.

Game developers were, if anything, even angrier with Unity than designers were with Adobe. Unity president Marc Whitten didn’t help matters when he justified the move by saying that his company merely wanted “shared success” with its customers.

Game devs intuitively understood this to be nonsense. For one thing, that’s not how shared success works. The company that sells you the hammers and nails that you use to build your lemonade stand does not get a nickel every time someone buys a cup of lemonade.

But just as important, Unity was proposing only shared *success*, not shared *risk*. It wasn’t offering to reimburse customers whose games flopped—only to tax customers whose games did well.

Unity is an avatar of the attitudes that produce enshittification. At the time of the shared-success scandal, the company’s CEO was John Riccitiello, best known for calling his customers “fucking idiots” for refusing to employ deceptive tactics to trick gamers into paying for in-game upsells.

Like the designers who held Adobe’s feet to the fire, Unity’s

customers also refused to back down. Major game studios announced that they were moving to Unity's small, struggling competitors, giving them much-needed boosts. Unity's stock price plunged 60 percent. Riccitiello resigned. (Or "resigned"—it is an open secret in the games industry that the board made it clear that he could either walk out under his own power or be carried out on a stretcher.) So did Marc Whitten.

The company substantially revised—but did not undo—its shared-success scheme. Under the new terms, only the very largest and most successful game developers will have to pay ransom to Unity. Meanwhile, game developers have had a major wake-up call. Unity has gone from a no-brainer, the default option that every game studio would take as a given when embarking on a new project, to being a controversial choice that has to be justified every time it's made. (I discuss the Unity situation further on page 214.)

This is how it's supposed to work: it's the market discipline of competition acting on companies. Enshittification requires more than executives' idle speculation about how they would arrange things if they could force you to go along with them. Enshittification is what happens when the executives calculate that they *can* force you to go along with their schemes, and when they're *right* about that.

Which brings me back to Microsoft. Like Adobe, Microsoft has migrated its iconic, practically de rigueur flagship product, Microsoft Office, to the cloud. You can no longer buy Word, Excel, and PowerPoint. Instead, you *subscribe* to them.

This move has given Microsoft enormous leverage over Microsoft Office customers. Office365—Microsoft's name for its cloud Office—re-rigs the market for Office software. You *can* collaborate with an Office365 user even if you don't use Windows, but users who run browsers other than Chrome and Edge

(Microsoft's re-skinned version of Google Chrome) get error messages telling them that Office365's "functionality is limited" by those browsers. And of course, you can't log in to Office365 without creating a Microsoft account, which requires that you enter into a one-sided contractual arrangement with Microsoft whose terms you can't amend (but Microsoft can, anytime it wants).

Still, corporate IT workers love Microsoft ("No one ever got fired for buying Microsoft"), and so do their bosses, despite red flags so large they can be seen from space. For example, Microsoft offers bosses a "productivity" scoring tool that measures employees' activity—internet usage, typing, clicking, and so on—and produces a stack-ranked score of the best employees.

This is a very bad idea. As Goodhardt's law (named after the British economist Charles Goodhardt) has it, "When a measure becomes a target, it ceases to be a good measure." If you tell employees that their workplace esteem is contingent on moving a mouse a certain way or typing at a certain rate (and that they will receive promotions and raises accordingly), the least motivated, least honorable employees on the shop floor will master the process of wiggling their mice or typing on their keyboards in ways that please the algorithm, irrespective of whether that translates into getting their job done. Rinse and repeat, and you've got an office full of algorithm-pleasers, while everyone else who was so focused on getting their jobs done that they didn't bother to reverse engineer the ranking system has been fired.

But from a firm-wide perspective, there's an even worse aspect to Office365's bossware suite: if you opt in, Microsoft will harvest all the data about every employee and manager in your company and then tell you how your company ranks compared to your direct competitors and your sector as a whole.

It is *wild* to think that there are corporate executives in 2025

who fall for the ruse of “We will show you your competitors’ sensitive data” without realizing the obvious corollary: “We will show *your* sensitive data to your competitors.”

Obviously, there’s a rude awakening on those executives’ horizons, but when it comes, they will struggle to eradicate the many tentacles and taproots that Microsoft has planted in their organizations. Office365 and its associated cloud tools “work best” with Microsoft’s competitors to Slack (Teams), Zoom (Teams again), Authenticator (Microsoft Authenticator), and a wide range of other commonly used productivity tools. What’s more, these tools all “work best” with Microsoft’s cloud. It’s *technically* possible to use just a few of Microsoft’s products, but it takes a *lot* more work.

Microsoft bundles all kinds of these products with its core offering, which means that when your workplace develops the need for a new kind of software, chances are that you’re already paying Microsoft for it, which means there’s no reason to go out and try something else.

With so few ways to stumble on a stand-alone rival to one of Microsoft’s products, there’s very little reason to invest in such a product—just as there are very few ways to stumble onto an alternative to Google Search, thanks to the tens of billions of dollars Google pays every year to ensure that it’s the default search engine for every search box you encounter, ensuring in turn that only the most quixotic investors back rivals, no matter how much better their search results are.

Viewers of *Saturday Night Live* in the 1970s lived through one of the most extraordinary eras in TV comedy, the birthplace of many cultural touchstones that still circulate today. My favorite of these is Ernestine, a character that Lily Tomlin created for *Rowan & Martin’s Laugh-In*, then brought with her to *SNL*. On *SNL*, Ernestine starred in a series of parodical ads for AT&T, in

which she would nasally extol the dubious values of the Bell System. At the end of those ads, Ernestine would turn to the camera and deliver the campaign slogan: “We don’t care. We don’t have to. We’re the phone company.”

When one search engine can grab 90 percent of the market by buying up the defaults on every platform, it is indeed too big to care. “We don’t care. We don’t have to. We’re *Google*.”

# The Death of Competition Kills Regulation, Too

The death of competition likewise doomed regulation. Competition is an essential component of effective regulation, for two reasons: First, competition keeps the companies within a sector from all telling the same lie to its regulators. Second, competition erodes companies' profits and thus starves them of the capital they need to overpower or outmaneuver their regulators.

While not all regulation is wise or helpful, a world without regulation is a catastrophe. That's because, in a highly technological world, your ability to do well (or even to live out the day) requires that you correctly navigate innumerable highly technical questions that you can't possibly answer.

You need to know whether you can trust the software in your car's antilock braking system, whether you should heed your doctor's advice to get vaccinated, whether the joists over your head at home are sufficient to keep the ceiling from falling in and killing you, and whether your kids' schooling is adequate or likely to turn them into ignoramuses.

It's not that you lack the intellect and discernment to answer each of these questions. You're a smart cookie. Given enough time, you could get a PhD's worth of education in software engineering, cell biology, material science, structural engineering, and pedagogy; investigate each of the offerings before you

in each of these categories; and make an intelligent choice that reflects your priorities and the trade-offs you're willing to make.

The problem is that it would take you several lifetimes to acquire all that knowledge, and long before you could do so, you'd be killed by food poisoning because you guessed wrong about whether you could trust the hygiene policies at your local diner.

It would be nice if you could let markets take care of these questions for you, but many of the consequences of wrong answers don't manifest fast enough to steer your decision-making. Sure, if a private school turns one of your kids into an ignoramus, you can demand your money back and refuse to send your other kids to that school—but your kid is *still* an ignoramus. Likewise, you can punish a restaurant that gives you food poisoning by withholding your future custom, but if that's a *lethal* poisoning, the fact that you don't eat at that restaurant anymore isn't quite the moral victory you might be hoping for.

To navigate all of these technical minefields, you need the help of a third party. In a modern society, that third party is an expert regulator who investigates or anticipates problems in their area of expertise and then makes rules designed to solve these problems.

To make these rules, the regulator convenes a truth-seeking exercise, in which all affected parties submit evidence about what the best rule should be and then get a chance to read what everyone else wrote and rebut their claims. Sometimes, there are in-person hearings, or successive rounds of comment and counter-comment, but that's the basic shape of things.

Once all the evidence is in, the regulator—who is a neutral expert, required to recuse themselves if they have conflicts—makes a rule, citing the evidence on which the rule is based. This whole system is backstopped by courts, which can order the process to

begin anew if the new rule isn't supported by the evidence created while the regulator was developing the record.\*

This kind of adversarial process—something between a court case and scientific peer review—has a good track record of producing high-quality regulations. You can thank a process like this for the fact that you weren't killed today by critters in your tap water or a high-voltage shock from one of your home's electrical outlets.

One key advantage of the process is that it relies on competitors to counter one another's claims. The reinforced steel joist manufacturer that claims that only its products are suitable for use in high-rise apartment buildings will have to defend those claims against competitors who submit their own structural engineering and material science evidence. Regulators don't need to look for holes in the arguments advanced by interested parties; they only need to assess the quality of the criticisms raised by other commenters who submit to the docket.

This process isn't just a way to prevent corporate executives from cheating the public by knowingly overpromising about their own products or denigrating their rivals'; it's also a way to stop firms that have tricked *themselves* from fooling the rest of us, too. As with the scientific method, the safeguards of peer review help us catch grubby attempts at both deception and *self*-deception, because it's *very* easy to talk yourself into a sincere belief that you are right and everyone else is wrong.

This process works well on “disorganized” sectors composed

\* During the drafting of this book, the US Supreme Court upended much of this process in a case called *Loper Bright Enterprises v. Raimondo*, which ended a long-standing practice called *Chevron* deference (see page 237). The earlier *Chevron* case had established the power of expert agencies to make and promulgate rules. The *Loper Bright* decision is widely believed to be a disaster for high-quality rulemaking in the United States. (I hold this belief personally.) Notwithstanding the violence wrought by the Supreme Court on this system in the United States, the systems in the rest of the world's democracies hew more or less to lines similar to those drawn in the *Chevron* case.

of many firms that compete hard with one another. When hundreds of companies are all at one another's throats, they suffer from a collective action problem—the same force that keeps *users* from leaving services like Facebook.

Hundreds of companies find it impossible to agree on almost *anything*, including where to have a meeting in which they could discuss what line they are going to feed their regulator. They probably can't even agree on how to cater that meeting.

Hundreds of companies are a disorganized rabble. They can't come to accord, and even if they could, a truly competitive sector produces smaller profits for each company (since one of the best ways to compete is by lowering prices to attract new customers and raising wages to attract the best workers). That leaves very little surplus capital with which to pursue regulatory adventures.

But when a sector dwindles to five companies—or four, or three, or two, or just one\*—the collective action problem is annihilated by the inevitable coziness among the executives of the incestuous industries.

After all, the executives in an industry dominated by a handful of firms are apt to have worked at most or all of the companies in the sector. They know one another, came up together, and are part of one another's social milieu.

Not only do concentrated industries find it easier to converge on a set of policy priorities and maintain message disci-

\* EssilorLuxottica is the world's largest manufacturer of eyeglasses, having purchased or forced the sale or license for dozens of eyewear brands, including Alain Mikli, Armani Exchange, Arnette, Brooks Brothers, Bulgari, Burberry, Chanel, Coach, Costa Del Mar, Dolce&Gabbana, Emporio Armani, ESS, Giorgio Armani, Luxottica, Michael Kors, Miu Miu, Native Eyewear, Oakley, Oliver Peoples, Persol, Polo Ralph Lauren, Prada, Ralph Eyewear, Ralph Lauren, Ray-Ban, Scuderia Ferrari, Sferoflex, Starck Biotech Paris, Swarovski, Tiffany & Co., Tory Burch, Valentino, Versace, and Vogue Eyewear. EssilorLuxottica also owns a large plurality of eyeglass retailers (Sunglass Hut, Lens-Crafters, Glasses.com, etc.), as well as the largest eyewear insurer in the world (EyeMed Vision Care). It manufactures the majority of the world's corrective lenses. And it has raised the prices of glasses by more than 1,000 percent over the past decade.

pline while bargaining with their regulators, they also have a lot to bargain *with*. Concentrated sectors tend to have Mafia-style demarcations of turf. (Think of Pope Alexander VI dividing up the “New World” in 1494, of cable companies carving up the map of the United States into exclusive fiefdoms, or of Apple taking an annual \$20 billion-plus payment from Google in exchange for not making its own search engine.)

This prevents “wasteful competition” and allows these companies to amass gigantic war chests that they can mobilize to win their policy priorities.

A hundred companies are a mob, a rabble. Five companies are a cartel.

“Regulatory capture”—when a company suborns its regulator and teams up with it to screw over customers, rivals, and suppliers—starts with a regulator that is weaker than the company it is supposed to be watchdogging. The pro-monopoly policies of the past forty years have produced *gigantic* companies that find it easy to unite against their regulators, even as the deregulatory policies over the same period have starved regulators of the resources they need to fight back. The inevitable result is regulatory capture.

## “With an App”

Regulatory capture has two faces: On the one hand, a captured industry is able to flout regulations that are meant to prevent it from harming the public, its employees and other stakeholders, and the environment. On the other hand, regulatory capture creates a *coalition* between the regulated industry and its regulators. They form a team and work together to enforce rules against other industries, startups, foreign adversaries, and so on. Regulatory capture isn't the same as *underregulation*; rather, it is the combination of *underregulation* (for the industry that has effected the capture) and *overregulation* (against that industry's enemies).

In this chapter, I'll be discussing underregulation (the overregulation story comes later, in “The End of Self-Help,” page 133)—the ways in which tech companies violate our labor, our privacy, and our rights as consumers to harm the public and beef up their own bottom line.

The most common tactic used to flout regulation is to break the law with an app and then insist that the law hasn't been broken at all, because the crime was committed with an app.

Sometimes literally (as Uber does when it argues that it's not an employer because it directs its workers with an app) and sometimes figuratively. Tech-like apps can obfuscate what's really going on, sloshing a coat of complexity over a business that

allows its owners to claim that they're not breaking the law. ("It's not an illegal unregulated hotel, it's an Airbnb!")

Riley Quinn, showrunner for the excellent *Trashfuture* podcast, says that whenever you hear the word *fintech* (financial technology), you should mentally substitute *unregulated bank*.

App-based lending platforms ignore usury law and say it doesn't count because they do it with an app. Cryptocurrency hustlers illegally trade in unregistered securities and say it doesn't count because they do it with an app.

When Uber entered the taxi market without securing taxi licenses or extending the workforce protections required under law, it said the move didn't count because it did it with an app.

The McDonald's-backed company Plexure sells surveillance data on you to vendors, who use it to raise the price of items when they think you'll pay more. In its promotional materials, Plexure uses the example of charging extra for your breakfast sandwich on payday. It says that such practices are not a rip-off because they're done with an app.

RealPage gives "recommendations" to landlords about the minimum rents they should charge for all the apartments in your neighborhood, raising rents and worsening the housing crisis. The company says it's not price-fixing because it's done with an app.

On the subject of the housing crisis, Airbnb is racing to convert all the rental stock in your city into an unlicensed hotel room, but it says the conversion doesn't count because it's done with an app.

As you'll see later in this book (page 147), the legal regime for apps really *is* different from the rules governing web pages. Thanks to intellectual property laws that ban "circumvention,"

companies that embed undesirable anti-features in apps can use the law to destroy rivals that disenshittify their offerings.

In other words, tech companies don't stop with "It's not a crime if we do it with an app." They also say, "It's a crime if you fix our app to defend yourself from our crimes."

# It's Not Wage Theft If We Do It with an App: Uber's Algorithmic Wage Discrimination

Platforms mediate between business customers and end users. For Amazon, that's sellers and buyers. For Uber, the business customers are drivers and the end users are riders. Like any other company that relies on a digital system, Uber can twiddle the knobs in its servers to make things worse for customers (like charging you more during busy times). But of course, the platform can also twiddle the knobs for its business customers: the drivers.

Every time an Uber driver is offered a job, the wage for that job—dollars per mile and minute—is recalculated by an algorithm at Uber HQ. The goal of this algorithm is to lower the wage of Uber drivers. It works spookily well.

The legal scholar Veena Dubal coined the term *algorithmic wage discrimination* to describe Uber's labor-pricing tactic. Dubal came to understand algorithmic wage discrimination through her ethnographic work with rideshare drivers. She reports that drivers divide themselves into two groups: ants (who take every job the app offers) and pickers (who are selective, cherry-picking the jobs with the biggest upside). When Uber's algorithm offers a job to all the drivers in your neighborhood, it calculates a differ-

ent wage for each driver based on that driver's recent behavior. If the driver has recently been picky, the system will offer a higher wage than it will to a driver who has been more ant-like. Pickers who take the bait will then be offered slightly lower wages in the future. The increments and frequency of these pay cuts are randomized so that it's hard for drivers to recognize that they're being squeezed, and of course, if a driver balks at a job and gets a little picky, then the wage starts to titrate up again.

The Uber algorithm isn't doing anything particularly clever here: this isn't a mind-control ray that's bypassing the drivers' critical faculties and tricking them into giving up their other part-time jobs in favor of a lower-waged grind for Uber. The trick is *simple*, but it's performed *quickly* and *tirelessly*.

If algorithmic wage discrimination is ringing a bell for you, perhaps you're thinking of when Facebook tricked publishers into posting longer and longer excerpts from their websites to Facebook, culminating in the full substitution of Facebook for their own independent, stand-alone web presences.

Facebook did the same thing to publishers that Uber does to drivers. Most publishers who observed their posts garnering fewer reads on Facebook would poke around and find publishers that had solved this problem by being more generous with the length of the excerpts they posted to Facebook. But some publishers balked, worried that they'd be giving away the store if they posted longer teasers to Facebook. When that happened, Facebook's algorithm—which determined whether a publisher's subscribers would see the post, as well as whether it would be "recommended" in the feeds of users who *hadn't* subscribed to the publisher's account—would sometimes goose the publisher's numbers, showing an old post or two to *lots* of readers, some of whom would click through to the publisher's site. This was quite

a convincer. Publishers that worried about Facebook replacing their website now saw that Facebook was actually sending *tons* of traffic to the site, and they posted longer, more frequent excerpts to Facebook.

This is the same game that Uber plays with drivers, dribbling a few crumbs when a business customer—a driver this time, rather than a publisher—decides the juice isn't worth the squeeze.

Lots of platforms do this. In January 2023, *Forbes* reporter Emily Baker-White revealed the existence of TikTok's "heating tool," a secret back-end feature that TikTok strategists used to lure different kinds of creators onto the platform.

Facebook started off with a default feed composed of accounts that you followed and then added in the odd recommendation. By contrast, TikTok went out of the gate with an algorithmic feed, called the For You feed. By accessing commercial surveillance dossiers of new users and then surveilling them further as they used the app, TikTok's content recommendation algorithm was able to make *really* good guesses about which videos a user was likely to enjoy. TikTok *does* offer users the ability to follow other users on the platform, but the algorithmic feed is so central to how TikTok works that most users treat subscribing to an account as a way to hint to the algorithm that they want *more* things similar to the videos the account they subscribe to posts, not as a way of saying "Just show me what the people I follow are posting."

The social contract with TikTok, then, is that it will spy on you, but it will use that surveillance data to fill your feed with things whose existence you hadn't suspected but that you find endlessly fascinating.

The heating tool violates this contract. Sometimes a TikTok strategist will decide to woo a specific performer or kind of performer in a bid to get them to retool for TikTok. (TikTok's idiosyncratic format and conventions make it hard for creators to

make videos that work well on TikTok *and* on rival platforms, which means that TikTok has a mass of TikTok-first/TikTok-optimized performers.)

The strategist identifies an account they wish to entice, and then applies the heating tool to that account. The heating tool pushes that performer's content into millions of users' feeds, irrespective of whether the content recommendation system would have "organically" recommended it.

So, if TikTok decides there aren't enough sports bros making content for the platform, a strategist can pick a random bro and make him king for the day, shoving his latest video into tens of millions of users' feeds. The sports bro doesn't know this—he just knows that he's gone TikTok-viral, and whatever system he has for converting attention to money (supplements, sponsorship, etc.) is now ringing up gigantic profits. That sports bro declares himself to be the Louis Pasteur of TikTok. He trumpets his victory to other TikTok-curious sports bros and boasts of the unlimited riches waiting to be claimed by the bold sports bro who optimizes his video format for the platform.

I call this the "giant teddy bear gambit." When I was a kid, my family used to go to the Canadian National Exhibition, an annual fair with a traveling midway. The CNE opens in Toronto every summer around August 15 (my mother's birthday) and closes on Labour Day (when we would all march with my parents' unions in the Labour Day Parade, which ended inside the CNE, with free admission for all the marchers).

The midway is lined with carnies roping for various games of skill that *seem* like they should be easy but turn out to be nigh impossible to win, like tossing five balls into a peach basket. But if you go down to the CNE, on any given day you'll see some poor guy lugging around the kind of gigantic teddy bear you win only if you get all five balls in the basket.

Now, that guy didn't actually get five balls in the basket. To a first approximation, *no one* has ever gotten five balls in the basket. What's happened instead is that a carny has flagged down a likely looking mark early in the day and said, "Tell you what, sir, since I like your face, I'm gonna make you a deal. You get just *one* ball in the basket, and I'll give you one of these key chains. You get *two* key chains and I'll let you trade 'em in for this giant teddy bear." Of course, the carny's not in the business of giving away giant teddy bears, but he understands that by dooming that poor sap to lugging around a teddy bear as big as he is all day long, through the muggy heat of Toronto in August, he will create an advertisement for his unwinnable peach-basket ball game.

TikTok's heating tool is a way for TikTok strategists to hand out giant teddy bears—and to take them back again. After all, TikTok users will tolerate only a certain amount of artificially promoted, irrelevant nonsense in their feeds, so if a TikTok strategist is satisfied that there is a sufficiency of sports bros locked in to the platform, it can withdraw the heat from its chosen sports bro and apply it to some astrologer, making her not only a queen for a day but also a Judas goat for other astrologer-influencers.

The giant teddy bear gambit is one of the most powerful forms of twiddling. It allows Uber to keep its algorithmic wage discrimination machine humming smoothly. As Veena Dubal has documented, the forums frequented by Uber drivers are full of posts from drivers who are certain that they are "good at Uber," who boast of the giant salaries they bring home from driving. Dubal's ethnographic work includes heartbreaking interviews with drivers who drive until they can't keep their eyes open, sleep in their cars, get back on the road—and then blame themselves for the pittance they take home. They don't understand that their indiscriminate desire to please the algorithm by taking every ride that

comes their way is *actually* signaling that they are easy pickings and can be enticed into driving for sub-starvation wages.

Tech leaders point to this stuff and call it *innovation*. It's more accurate to call it *obfuscation*. Except for the level of indirection introduced by the presence of an app, the algorithmic wage discrimination gambit would trigger labor law enforcement.

The idea of titrating wages to employees' desperation is hardly novel. Bosses since time immemorial have exploited bargaining power over workers to depress their wages. If you're an employer and you know that all the other employers in your town are sexist jerks who won't hire women (or racist jerks who won't hire Black people), why not offer that perfect job candidate half the wage of her male (or white) colleagues?

But the opportunities for pre-digital era bosses to suppress workers' wages were few and far between, and comparatively crude. Wages were set when workers were hired, and adjusted only once or twice per year, thanks in large part to the impracticality of doing the paperwork to track a workforce's ever-changing salaries without computers.

The blackhearted coal bosses in old Tennessee Ernie Ford songs might have dreamed of changing coal miners' pay from instant to instant based on how desperate the miners were, but not even the greediest coal boss was willing to fill a warehouse with all the accountants in green eyeshades needed to make those adjustments in paper ledgers.

The point is that while algorithmic wage discrimination isn't an innovative new way of doing business—and like every other shell game is just a simple trick done quickly—the fact that it's done with an app lets the modern blackhearted coal bosses claim that they're not violating labor law.

## Reverse-Centaurs and Chickenization

In automation theory, workers are “centaurs” if they have some kind of tool that lets them do more than they could do on their own. For example, if your boss invests in bossware like Microsoft Office365 that counts your keystrokes and mouse movements and takes note of every link you click, then they are a centaur, accomplishing more than any human boss could, thanks to the software that automates nearly all of that work.

Not every centaur is as sinister as a boss who spies on you with cloud software. A farmer with a tractor is a centaur, and so is a cashier whose register automatically adds up the groceries and calculates your change.

There’s more than one way to partner a human with a machine. A *reverse-centaur* is a machine that uses a *human* to accomplish more than the machine could manage on its own.

Take Amazon delivery drivers: Amazon outsources much of its delivery to third parties it calls Delivery Service Partners (DSPs). DSPs are typically manic entrepreneur types, bamboozled by Amazon’s promises of “being your own boss” while “partnering” with one of the most powerful, most profitable companies in world history.

DSPs are responsible for buying a fleet of vans and kitting them out to Amazon’s exacting standards: not just an Amazon-branded paint job but also a bewildering array of sensors that

track the van through time and space, noting sudden maneuvers and recording traffic around the vehicle. The sensors go *inside* the van, too, where AI-equipped cameras constantly monitor the drivers, down to the motions of their *eyeballs and mouths*.

The drivers whose eyeballs are being so lovingly observed aren't Amazon employees: they're payrolled by the DSP. But in every regard save this one, Amazon is the boss. Amazon's software tells the drivers what route to drive, sets (impossible) quotas for deliveries, and demands the dismissal of drivers who don't live up to the standards it sets.

This is why the roads leading to Amazon depots are littered with sealed bottles of human urine. There is no way for drivers to meet quota and keep their jobs if they're stopping to pee, so, caught between a kidney stone and a hard place, they pee in bottles in the van, tightly screwing on the lids afterward (something you don't forget to do twice). Amazon doesn't like the bad press this generates, so it has ordered DSP operators to search returning vans for pee bottles, with punishments for drivers caught with evidence of having indulged the inescapable human need to eliminate their bodies' waste, forcing the drivers to huck them out the window on the way back to the depot.

In 2023, the UK prankster Oobah Butler harvested some of that urine, rebottled it, and offered it for sale on Amazon as Release Energy, a "bitter lemon drink."

Butler did the stunt for his documentary *The Great Amazon Heist*, which aired on the British public broadcaster Channel 4. In the special, Butler shows how his bottled piss snagged the favor of the Amazon recommendation algorithm, rising to become the top-selling "bitter lemon drink" on the platform.

This took quite a lot of doing on Amazon's part: Butler had listed Release Energy as a "refillable pump dispenser" (he didn't have the proper food and drink licensing paperwork needed

to list it as a beverage for human consumption), but Amazon thoughtfully shifted it into the “correct” category, and even more thoughtfully failed to ask for the paperwork showing that it was fit to drink.

Not all of Amazon’s attention was automated. Once the bottled driver piss hit the top of the Amazon sales chart, an Amazon rep actually phoned up Butler to pitch him on using Amazon for his shipping and fulfillment.

Butler never actually shipped a bottle of urine to a stranger. The only people who got a real bottle of Release Energy in the mail were Butler’s pals, who were in on the joke.

Amazon never figured out the gag—at least, not until the documentary aired. Then it wheeled out a poor PR droid named James Drummond to recite boilerplate about how Amazon has “industry-leading tools to prevent genuinely unsafe products being listed.”

When your drivers are pushed so hard by automation that they can’t even urinate, they aren’t centaurs, whose work is supercharged by high-tech tools. They are *reverse-centaurs*, humans who are used as inconvenient, fallible meat-puppets for a robot that demands superhuman feats of them, working them in ways the human body literally can’t withstand, until they are used up and discarded, and then replaced with other humans.

(A leaked 2021 Amazon internal research memo warned that the company was burning out warehouse workers so quickly that it was in danger of using up every single eligible worker in the United States.)

But Amazon isn’t merely in the business of turning its workers into reverse-centaurs. Before it does that, it *chickenizes* them.

In labor economics, *chickenization* refers to a set of particularly ghastly labor practices originating in the poultry industry (hence the name). Poultry packing—like so many other sectors—is a

cartel, with three companies dominating, each running in its own exclusive territory, meaning that farmers typically have no choice but to use the one packer available to them.

Like Uber drivers, chicken farmers are classed as entrepreneurs who work for themselves—and like Uber drivers, chicken farmers are monitored and controlled by their true employer to a degree that exceeds all but the most abusive workplaces. And, as with Uber, these chicken platform owners claim they're just brokers, not bosses, and have no obligations to the farmers who are their *de facto* employees.

To become a chicken farmer, you must first borrow a *lot* of money. Then you use that money to build a coop to the precise specifications of the poultry packer that buys your birds. The packer sells you the baby birds and tells you what kinds of lights you should expose them to, and for how long. It tells you what foods the birds will eat, and how much, and when. It tells you what medicines the birds will receive and at what dosage.

You raise these birds—which you had to buy at the rate that the poultry processor set—to the exacting specifications of that processor. Once the birds are ready for slaughter, you bring them to the processor, and only then does the processor tell you the one thing you were absolutely *not* allowed to know while you were putting in all that labor and expense: what you will be paid for your birds.

The processor, occupying a regional chokepoint through which every chicken farmer in its district must pass, knows exactly how little it can get away with paying each farmer, a sum carefully calculated to let the farmers roll over their loans and raise another batch of chickens, but never enough to escape from debt.

This is an enviable position—for the chicken processors. Sometimes they tinker with the formulas they use to maximize

chicken yield, varying diet, light, and medicines for one farmer (without telling the farmer whose livelihood they're toying with). If the experiment works, all the other farmers will be directed to adopt the new methods the next year. If it fails, the cost is borne by the farmer.

Farmers don't like this, of course, but what can they do? Farmers who complain are cut off from selling to the only chicken processor that is close enough to send their birds to. Worse than that: Jonathan Buttram, a chicken farmer, had the temerity to testify at a DOJ hearing in Alabama about the abuses of the system. Not only did the processor cut him off from the poultry industry, but also, according to Zephyr Teachout's 2020 book, *Break 'Em Up*, it chased him into his next career: fixing chicken coops. The processor let it be known that farmers who hired Buttram to work on their physical plant would be permanently blocked from selling their birds. Like Amazon spending \$200 million to drive Diapers.com out of business, this kind of bullying is a great investment: make an example out of the one holdout, and you scare everyone else so bad they never even *think* about stepping out of line.

That's chickenization: a system of total control over workers who have to borrow money to pay you for the privilege of working for you, and to whom you owe nothing. Those workers rely on you for everything, and they know that you can ruin their lives at the stroke of a pen and that, if you do, they have no recourse.

Amazon DSPs aren't just reverse-centaurs; they're *chickenized* reverse-centaurs. A DSP has to borrow money to buy Amazon vans that can't be readily repurposed for any other kind of service. They hire workers and buy Amazon uniforms to dress them in. They sign long-term leases on lots to park their vans in, and long-term maintenance contracts to keep those vans running.

Amazon tells these DSP owners that they're "entrepreneurs,"

but they have only one customer: Amazon. Amazon lures multiple naive victims into serving the same district in order to build the capacity to make good on its same-day/next-day delivery promises, then abruptly cuts off any excess once it figures out how many drivers it really needs to serve the demand.

But that's not the only reason a DSP can be stuck with a parking lot full of Amazon vans and no Amazon contract: in 2023, Amazon fired a DSP after its drivers formed a union. If those workers were employees, that would be illegal: American companies are prohibited from closing down a shop after its employees unionize, but Amazon claims that because it exerts its control over the drivers through an app and an intermediary, it can fire them at will.

Chickenization started in the poultry industry, but thanks to tech, it has spread like wildfire. Long before the COVID-19 lockdowns shifted many people to work-from-home jobs, tech helped some of the greediest, most predatory businesses establish a beachhead in their workers' own apartments.

Arise is a tech company that provides outsourced call center staff for some of the world's biggest companies, like Intuit, Disney, and Carnival Corporation, parent of Carnival Cruise Line. The company markets itself heavily to Black women, relying on an MLM-like strategy that encourages women to recruit their friends and family, and pays them a bonus when they do.

The workers who take calls for Disney aren't Disney employees. They're also not Arise employees. Arise classifies them as self-employed independent contractors, recruited to "be their own bosses." As independent contractors, Arise's workers have no employment rights—and, boy, did Arise know it.\*

\* Arise changed some of these practices in 2024, following multiple lawsuits and being barred from doing business in Minnesota and DC.

To work for Arise, you have to use your own (likely borrowed) money to outfit yourself with a high-end PC, a headset, and a broadband connection. But—according to a 2020 investigative series by ProPublica’s Ken Armstrong, Justin Elliott, and Ariana Tobin that sparked a successful suit by the DC attorney general—you also have to pay a “background check fee” and put down a deposit to train to work as a call center operative. If you pass the training course, you then have to pay a “service fee” to Arise twice a month—that’s right, you have to *pay* Arise for the right to work for Arise.

Once you’ve been certified to work for a given client, Arise and that client can (and do) constantly monitor your calls. Any “unprofessionalism” (including audible signs that you are working from home, like a passing siren, a neighbor’s leaf blower, or a crying child) can result in your status being revoked. When that happens, you don’t get a refund, naturally, on the substantial sums you’ve paid to train for that client.

Arise workers describe a nightmarish working life in which they must endure the (often racist and misogynist) abuse of callers, even as they frantically shush their children to tiptoe around the house while they work, lest they find themselves fired and have to forfeit their investments, while still having to pay off the loans they took out to pay for them.

But that’s not the worst of it! Arise requires its workers to sign contracts that include penalties for “early termination.” That’s right: you don’t just have to pay Arise for the privilege of working for it—you also have to pay it more if you quit.

## Twiddling

*Twiddling*—the process of changing the costs, prices, recommendation weights, and search rankings through automated or semi-automated means—is a key driver of enshittification. A business with a digital back end can endlessly twiddle all of these virtual knobs.

When platforms heat business customers, or shadow ban them, or raise the prices on customers based on surveillance data (like Uber raising the cost of a taxi for riders whose phones are about to run out of battery), or drive you to a more expensive match for your search, they alone know that they're doing it.

Black Facebook users don't have any way of knowing that they're being shown ads for more expensive financial products than white users with similar financial histories. Teenagers in Australia don't know that Facebook advertises the ability to target them when their surveillance profiles show signs that they are depressed.

Twiddling is a central characteristic of digital platforms. If, one winter day, an unscrupulous gas-station owner spies someone leaving a vehicle stranded in the snow and trudging toward his station, he'd still need an army of helpers to reprice all the snow chains before that stranded traveler can make it through the door.

But a digital business can change *everything*, all the time, instantly, based on automated processes that act on surveillance data and other information.

Tech suppliers are doing everything they can to bring twiddling to the “real” world. Take the increasingly popular electronic shelf labels popping up in grocery stores. These e-ink displays are networked and can adjust the price of everything in a given store, or in all the stores in a chain, at the click of a mouse. In Norway, where electronic shelf labels are popular, some merchants “adjust” prices more than two thousand times per day.

Twiddling is a system of pumps that digital platforms can use to move value from business customers to end users and back again, siphoning off a bit more for themselves every time, until all the surplus value has been harvested for executive bonuses, dividends, and stock buybacks—enshittification, in other words.

Twiddling is the *how* of enshittification. While we can all see enshittification from the *outside* as platforms are good to users, then to business customers, then to themselves, twiddling is the invisible thing that’s going on *inside* the companies.

Because twiddling takes place inside the corporate black box, it’s hard to get your head around it. That’s made especially complicated because the platforms lie like crazy about what they’re doing.

Take the ad-tech market, which is dominated by Google and Meta, which (you’ll recall) have a very cozy relationship with each other—so cozy that they actually formalized a secret, collusive arrangement to divide up the ad market among themselves.

Ad tech is a hellaciously complex beast. The antitrust scholar Dina Srinivasan, herself a veteran of the ad-tech industry, does a great explainer on the sector in which she points out that 15 percent of the money in the ad-tech market is simply unaccounted for. Literally, the system is so complicated that no one knows where the money is going!

With that said, here’s a simplified overview of how ad tech works: Advertisers create accounts on a demand-side platform

(DSP), where they specify what traits they'd like to target (“Please show our ads to eighteen-to-thirty-four-year-old man-children in the five boroughs of New York who own Xboxes and have searched for gonorrhea-related information in the past three weeks”) and what they'll pay to reach them.

Web publishers have accounts on a sell-side platform (SSP), where they specify what kinds of users are requesting pages from them (“I just got a click from a boomer in rural West Virginia who is signed up to a Medicare Advantage plan and recently searched for information on reverse mortgages”).

The SSP and DSP send all this information about what kinds of users are sought and what kinds of users' attention is available to a “marketplace” that conducts eyeblink-fast auctions where advertisers bid to buy slots on pages that are currently being assembled.

That long delay after you reach a web page but before it shows up in your browser? That's the “surveillance lag,” the delay while all those auctions are concluded. Web publishers design their pages so that nothing loads until the ads are ready; otherwise you might get the information you're looking for and close the tab before the ad is shown to you.

Meta and Google each operate a sell-side platform, a demand-side platform, and a marketplace, and each is periodically also an advertiser and a publisher. Each one has rigged its ad-tech stack so that publishers who use their SSP and advertisers who use their DSP are driven to use their marketplace, so everything happens under the same roof.

Here's an amazing fact: Historically, the intermediaries that served the print, display, radio, and TV ad industries accounted for about 15 percent of the total sums generated by advertising—that's all the ad agencies, media buyers, and other *Mad Men* middlemen of the golden age of advertising. Today's ad-tech duopoly captures *51 percent* of that total.

Google and Meta swear that they have increased their share of ad revenues by more than 300 percent because they're just so gosh-darned *good* at matching ads with audiences. After all, there are so many more ads being shown to so many more people than at any time in history! This is an extraordinary claim, but the evidence in support of it is decidedly subpar.

For starters, there's the widespread discontent among publishers and advertisers about the ad-tech system. Publishers are extremely vocal about the declining revenues they've experienced as ad tech consolidated. If ad tech is capturing a bigger slice of a *much* larger pie, the rest of that pie isn't going to publishers.

But advertisers aren't the ones reaping the benefits of the publishers' losses. Advertisers spend more on ads but get worse results from them. (Recall that when Procter & Gamble zeroed out its \$200 million surveillance advertising budget, it saw no change to its sales.)

There's a much simpler and more logical explanation for why the ad-tech sector is making so much more than its historical antecedents: Google and Meta are cheating. After all, they represent buyers *and* sellers in a marketplace that they control and where they compete with those buyers and those sellers. They claim that when they represent advertisers, they're trying to get their clients the best deal. They claim that when they represent publishers, they're trying to get *those* clients the best deal. But the numbers show that the only party getting a good deal is the ad-tech platforms.

Imagine that you and your spouse are seeking a divorce and that when you arrive at the courthouse, you discover that your lawyer is *also* representing your soon-to-be ex, and that *same* lawyer is *also* the judge. Then you peek at the lawyer's phone screen and discover that she's trying to *match with both of you on Tinder*.

Then that judge/lawyer/suitor bangs her gavel and declares that the divorce is final and that neither you nor your ex is going to get the house. *The house is going to the lawyer.*

The lawyer's insistence that the house is a fair payment for the excellent work she performed as counsel, opposing counsel, and judge is not very credible, and neither are Google's and Meta's stories about why they cream off the majority of the money in the advertising marketplace simply for brokering connections between publishers and advertisers.

Google and Meta are among the most profitable businesses in human history, a fact that some of their critics chalk up to their incredible technological prowess. After all, Google and Meta pitch advertisers on the persuasive possibilities of automated analysis of surveillance data: "We have spied on everyone you could possibly want to sell things to, and we can use 'Big Data' and 'AI' to craft pitches that are tailored to the psychological vulnerabilities of every internet user. This will allow *you* to sell anything to anyone. And that, my friend, is why you should pay such a large premium to advertise with Google and Meta."<sup>\*</sup>

But with most ads not being shown to *anyone*, and also with how often and shamelessly these companies lie about *everything*, perhaps we should entertain a more parsimonious explanation. Like everyone who ever claimed to have developed a mind-control system, Google and Meta are lying (to us and possibly to themselves). From Mesmer to Rasputin, from the CIA's MK-ULTRA to "neuro-linguistic programming" to the sad men who style themselves "pickup artists," everyone who has claimed or still claims to be able to bypass our rational faculties to control our behavior was and is a liar or a crank.

<sup>\*</sup> For avoidance of doubt, allow me to explicitly state that this is a sarcastic interpretation of the implicit message Google sent to its users, and not an actual quote. Govern yourself accordingly.

The Virginia Tech science and technology scholar Lee Vinsel has coined a very useful term for this situation: *criti-hype*. It refers to what happens when critics wave around the boosters' "picture of extraordinary change but focus instead on negative problems and risks." They take "press releases from startups and cover them with hellscapes."

Criti-hype is *still* hype. By credulously amplifying Meta's and Google's cod-psychology claims to have finally perfected mind control by computerizing warmed-over Skinnerian behavior modification techniques (many of which are caught up in the replication crisis that has rocked psychology), we help them sell ads to dopey executives.

After all, executives are the one group whom ad salespeople have always known how to persuade. The department store magnate John Wanamaker proved this when he quipped, "Half my advertising spend is wasted; the trouble is, I don't know which half." What a tribute to the silver-tongued advertising execs serving Wanamaker's that they convinced its owner that they were wasting *only* half his money!

Rather than criti-hyping Google's and Meta's claims to have perfected the cybernetic Rasputin, we can stick to the observable facts: these companies cheat like crazy, lie like crazy, and have a duopoly that they maintain by secretly colluding to structure the ad market. No mind control needed!\*

\* For more on this, see my short monograph *How to Destroy Surveillance Capitalism*, published in 2020 by Medium.

## The End of Self-Help

No one has ever figured out how to make a computer that only runs the programs that its manufacturer desires. As I noted on page 59, the modern computer is *universal* in a highly technical sense: the “Turing-complete, universal von Neumann machine” is a mid-century innovation, the product of a heavily funded Allied Army technical project that was, in its own way, even more seismic than the Manhattan Project.

*Turing-complete* refers to Alan Turing, the gay computer scientist who, during World War II, led a group of brilliant mathematicians (including a cadre of exiled Poles) and code breakers (including a motley assortment of crossword puzzle experts and other weirdos) at Bletchley Park, a secluded estate between Cambridge and Oxford, in an effort to break the Nazis’ Enigma cipher.\*

Across the ocean, John von Neumann (as in *universal von Neumann machine*) led a group of exiled Hungarians and colleagues from around the world at the Princeton Institute in devising a new physical architecture for a computing machine. The

\* Polish mathematicians were the trailblazers here, developing the electromechanical computers (*bombas*) needed to break the Nazis’ modified Enigma machines, used to encode and decode secret messages. Their work is less well known than Turing’s, but they deserve enormous credit for their contribution to the war effort. Turing, of course, was hounded to suicide by a British government that knew no bounds of decency when it came to persecuting homosexuality. Today, we rightly remember Turing as a hero—he even appears on a five-pound note—while the Polish code breakers his work was built on—Jerzy Różycki, Henryk Zygalski, and Marian Rejewski—are all but unknown (though they did get their own Polish postage stamps in 1983).

Princeton Institute attracted some of the world's brightest scientists, poets, historians, and other smarty-pants types, and their kids were pressed into work during summers, stuck in the Princeton Institute's basement, hand-winding wire around the ceramic memory cores that von Neumann's first computers employed.

Each of these efforts completed one piece of the theoretical puzzle needed to build the modern computer. The brightest minds on both sides of the Atlantic, working separately, conceived of something new under the sun: a system that could compute the output of any valid program. In some fundamental, technical sense, every computer has the same capability: the ability to run every formally correct program. Of course, modern computers can run these programs billions (and soon trillions) of times faster than those first computers, but if you gave one of those early computers an infinite amount of time and energy, it could run the same programs as our modern devices.

The discovery/invention of the universal computer profoundly changed the world, though it took a while for this to become noticeable. Early on, when computers were expensive and slow, it seemed like they were mostly useful for just a few things, like calculating ballistics charts or actuarial tables. But because computers are universal, each advance that reduced their cost and/or increased their power exposed a new suite of applications for them. Being able to compute more complicated programs in a reasonable amount of time meant that computers could be brought to bear on more problems (for example, weather prediction). And being able to compute older, less complex programs more cheaply meant that it was economical to run those programs in new ways (for example, to compute sports statistics).

This set up a virtuous cycle: R&D made computers cheaper and faster, and cheaper and faster computers were useful to

more industries, which justified more R&D to make computers cheaper and faster still.

From the end of World War II to now, we have seen a steady march of computers into more and more applications. Many older devices have quietly, profoundly changed: Cars have become computers in fancy cases. Same for TVs, thermostats, and watches. Printers—which once used electromechanical relays to direct a daisy wheel or a typeball to strike a ribbon over a sheet of paper—are now supercomputers, capable of vastly more computation than all the computers on earth at the end of World War II.

All of this is a by-product of computers' universality, which means that the R&D applied to improving computers on behalf of the video game industry also improves the computers used for cancer diagnosis and the computers used in fart machines soon to end up in the discount aisle at your local dollar store.

But universality is a double-edged sword. No one knows how to make a computer that's *almost* universal, that's "universal minus one." We can't make a computer that only runs programs that don't crash. We can't make a computer that only runs programs that aren't viruses. We can't make a computer that can't run ransomware. And more's the pity.

All this means that we *also* can't make a computer that only runs programs that are good for the manufacturer's bottom line. There's no way to make an HP printer—a computer in a fancy case with some bottles of ink wired into it—that's incapable of using third-party ink. There's no way to make an iPhone—a pocket-sized computer that will make phone calls for you if you insist—that only runs apps that you buy through Apple's App Store. There's no way to make a car—a computer that you put your body into and drive around at eighty miles per hour—that can't run a privacy blocker that keeps it from transmitting every

aspect of your driving (every time you touch a control, everywhere you go, even which songs you play on the stereo) to the automotive company, various data brokers, and your insurer.

Which is weird, because HP claims that its printers can only use its cartridges of \$10,000-a-gallon ink. Apple claims that its phones can only run the apps from its App Store, where it takes 15 to 30 percent out of every payment, to the tune of \$24 billion a year. And car manufacturers claim that the only way to operate their vehicles is by running the software that collects gigabytes of data every hour and exfiltrates them to a shadowy commercial surveillance industry.

Implicit in these claims is that there's no other way to do it—no way to make a printer that takes anyone's ink or a car that doesn't spy on you. What are we to make of industry claims to have made a *selectively universal computer*, which will only run the manufacturer's preferred programs?

It's quite simple, really. When the Big Tech companies say, "It's *impossible* to run code of your choosing on a computer we've sold you," what they're really saying is "It's *illegal* to run code of your choosing on that computer."

This is a far more controversial proposition, which is why they maintain the useful imprecision in regard to impossibility/illegality. But it's an important distinction, and one worth dwelling on.

Let's start with a definitive statement: Congress never passed a law that makes it illegal for you to install non-Apple-approved software on your iPhone. That would be an outrageous law, akin to one that required you to put Nike-approved laces in your Air Jordans. Those are your shoes, and it's none of Nike's business whose laces you wear. Even if they can show that some Air Jordan wearers are breaking their ankles due to poor lacing, even if they could prove that broken laces were causing drivers' feet to

slip off the brake pedals, killing the drivers and other unlucky road users, they still wouldn't be able to require you to use their laces. Those shoes are *yours*, and anything irresponsible you wanna do with them is a matter between you, the government, and anyone who gets caught in the crossfire. The manufacturers don't get a say.

The same goes for your printer, your phone, and your car. They're *your* property. Every first-year law student takes an Intro to Property Law course, where they'll be acquainted with the 1753 treatise *Blackstone on Property*, which defines *property* as "that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe."

If your printer is yours, if you have "sole and despotic dominion" over it, to the "total exclusion of the right of any other individual in the universe," then it is *certainly* none of HP's god-damned business whose ink you use. Hell, fill your printer with ditchwater if you want! Or vintage Veuve Clicquot (which costs a fraction of what HP charges for ink).

If Congress never passed a law saying manufacturers get to control your gadgets after you take them home, if such a law would be an affront to the very foundation of property, how is it that you can't practically install third-party app stores, generic ink overrides, or a privacy blocker for your car?

The answer lies in intellectual property (IP) law.

Now, people like me are supposed to *hate* the term *IP*. Digital freedom fighters have expended vast quantities of blood and treasure insisting that *IP* is a cheap rhetorical trick, a loose category containing whatever the speaker wants it to, and then that thing is declared to be property, with all the sole-and-despotic dominionism that entails.

But *IP* has a very precise meaning in business circles. When

executives boast of their corporate IP, what they mean is that they have designed their products and services in such a way as to give them a *legal right* to reach beyond their own walls and control the conduct of competitors, critics, and customers.

Take the Digital Millennium Copyright Act (DMCA), an incoherent mess signed into law by Bill Clinton in 1998. The DMCA has many subcomponents that don't have much to do with one another, so it's hard to make blanket statements about it, but for the purposes of this argument, I will be making some *very specific* statements about just one clause of the DMCA, Section 1201.

DMCA 1201 is an “anti-circumvention law.” It regulates by-passing an “access control” for a “copyrighted work.” A simple way to think about this is that DMCA 1201 bans you from “breaking a digital lock,” if that lock is used to keep you from accessing a copyrighted work.

Let's think about that HP printer cartridge. Obviously, the ink sloshing around inside it is not a copyrighted work, so there's no intersection between DMCA 1201 and refilling the cartridge with your own ink. But a printer cartridge is more than a plastic box filled with ink; it's also got a chip in it, and that chip has a program running on it, and that program *is* a copyrighted work.

If HP puts a program—a copyrighted work—on that chip that does a little authentication dance between the printer and the ink cartridge in order to verify that you bought a fresh batch of \$10,000/gallon HP ink rather than refilling the cartridge or buying a compatible one, then defeating that program counts as “circumventing an access control” (the program on the chip) that restricts access to a copyrighted work (again, that *same program* on the chip).

Bypassing that program is illegal under DMCA 1201, and providing someone with a tool to bypass that program is a *criminal offense*, a literal felony. By designing a printer cartridge so that

you have to bypass a program in order to refill it or impersonate it, HP can make refilling an ink cartridge, or buying a third-party cartridge, into a serious crime.

The implications of this are staggering and disturbing. The cost of tiny, high-powered chips is in free fall, which means that more and more devices are becoming “smart.” Once they are “smart,” they can be designed so that using them in ways that the manufacturer disapproves of is illegal—not because Congress ever banned that use, but because *making* that use requires that you bypass a digital lock.

Thus we see the rapid proliferation of “smart” devices whose additional silicon primarily or significantly performs the function of making it illegal to use the device in ways that are good for you and bad for the manufacturer’s bottom line. From insulin pumps to dishwashers, cars to thermostats, wheelchairs to tractors, manufacturers of every description are scrambling to find ways to infuse “IP” into their products in order to allow them to mobilize the courts and federal law enforcement to turn their shareholders’ financial interest into legal obligations.

This DMCA 1201 trick has many guises and names. In the early days, it was called *digital rights management (DRM)* and was primarily mobilized on entertainment devices and in entertainment software—DVD players, gaming consoles, ebook readers. When the automotive sector discovered it, they called it *VIN locking* because it was used to lock engine parts so that they would only work in a car with a specific serial number (the vehicle identification number).

The rising term of art these days is *parts pairing*, which comes from the electronics world. Phones, gadgets, and even ventilators are designed so that each major assembly—like a screen or a memory chip—has its own “security chip” that checks to make sure that the manufacturer’s authorized representative “paired”

the part with the device after it was installed. This means that a farmer can troubleshoot a tractor, identify the malfunctioning part, and swap in a working replacement, but the tractor *still* won't run: not until the farmer books a \$200 service call from a technician who comes out and types an "unlock" code into the tractor's console.

Combine IP law, DRM, and continuous internet connections, and you all but guarantee that any "smart" device that you come to enjoy and rely on will be enshittified.

Take the SNOO Smart Sleeper, a high-tech self-rocking cradle that senses when your baby is crying and has a go at rocking them back to sleep while playing "the sounds of the womb." By all accounts, the SNOO works reasonably well, and as anyone with a newborn can attest, anything that helps your kid (and therefore you) get even a *little* more sleep is a prize beyond measure.

Which is why so many parents have coughed up \$1,695 for a SNOO bassinet of their own. But after the SNOO's initial run, the manufacturer, Happiest Baby, applied lesson one of the Darth Vader MBA and announced that, henceforth, your \$1,695 bassinet would lose its "advanced" features unless you paid the company \$20 a month.

Enshittification is a game of moving value away from end users and business customers to shareholders. The SNOO switcheroo was a pure value grab: Happiest Baby wanted to extract new revenue from SNOO owners who'd had a second child, or who had bought or been given a used SNOO, and, of course, it wanted to hit up new customers for \$20 a month.

Every parent knows that there's a huge, ever-circulating pool of used kids' stuff, from breast pumps to onesies, changing tables to bath toys. You'll find accounts of babies and kids wearing and playing with hand-me-downs all the way back to the days of the Grimm brothers' fairy tales.

Obviously, this isn't ideal for the makers of kids' stuff. They would certainly make more money if they could somehow engineer a world in which every time a new kid was born, that meant demand for a brand-new playpen, crib, booster chair, diaper bag, and wardrobe.

But this has *never* been the way things worked. Many of Happiest Baby's executives are almost certainly parents, and everyone who works for the company was a kid at one point. These people can't *possibly* have been surprised to learn that customers who bought an expensive, specialized gadget to use during their kid's infancy went on to give away or sell that gadget later, or saved it for their next kid.

Doubtless, other makers of children's gadgets have wished that they could get paid again when the gadget changed hands in the secondary market. The makers of SNOO aren't smarter or even more evil than all those other executives. They're just more capable—they have a device with a continuous internet connection that they can downgrade at will. They have DRM and IP law, which felonize anyone who disenshittifies SNOOs, say, by making an alternative app for it that restores all the features they've confiscated.

Enshittification is when you combine the banality of evil with an internet-connected device and a federal law that criminalizes doing anything with that device that the manufacturer dislikes.

Any economist will tell you that products that have secondary markets are more valuable than single-use products. A new car is worth more because you can sell it to someone else as a used car. A house is worth more because when you're done living in it, you can put it on the market and someone else can live in it.

What's more, the value created by that secondary market is "priced in" to the cost of the good you buy. One of the reasons that university textbooks were historically so expensive was that

students knew that they could sell those books to next year's class, and so they were willing to pay extra for them.

The digitization of textbooks—adding DRM to them and requiring a login and password to access course materials that come bundled with texts—destroyed that secondary market, but because textbook publishing is a cartel controlled by a tiny number of firms, those firms were able to use their market power to keep the prices high, even as they killed the secondary market. In other words, they moved value from students to shareholders. Enshittification.

It's grimly funny when enshittifying companies protest that they're only trying to build a "sustainable" business, one that allows them enough recurring revenue to continue to innovate, patch new security defects, keep their servers on, and so on. After all, every textbook publisher, bassinet maker, and other hard-goods company in history, up to a few scant years ago, managed to stay in business by making things that people wanted, charging just once for them, and then enduring the indignity of having their own new products compete with the used products their former customers had no use for.

As these companies are fond of reminding us, they're not charitable enterprises. They're in business to make profits. The problem of how they stay in business by just selling us stuff that we own thereafter is *their* problem, not ours. If they find the prospect of selling things to people emotionally distressing, perhaps they should find a less stressful occupation more suited to their fragile temperaments?

The wounded tone that Happiest Baby executives adopted in the forums where their customers were buying for their blood is pretty darned unconvincing.

Unconvincing, that is, to everyone except for other enshittifying executives, like the managers at Anova Culinary (officially Anova Applied Electronics), who announced in August 2024

that henceforth, they'd be charging a \$2-a-month subscription fee for the app that controlled their sous vide wand (used for cooking food slowly in a vacuum-sealed pouch).

As Anova's CEO, Stephen Svajian, put it on the company website, "As our community has grown, so have the demands on our resources. Our community has literally cooked 100s of millions of times with our app. Unfortunately, each connected cook costs us money."

In other words: Svajian designed an appliance that you couldn't just connect to your phone or laptop with a simple Bluetooth link. Instead, he deliberately chose to make a gadget that had to contact Anova's servers every time you used it—a thing no one in the world would ever, ever want—and realized, a decade later, that the data he swiped from his customers wasn't worth enough to cover the costs of spying on them.

In a world where IP law didn't protect executives at Happiest Baby, Anova, Adobe, textbook companies, and the rest of the enshittification vanguard, enshittifiers would have to contend with the possibility that their sleazy tactics would be neutralized by a rival company hoping to poach their customers. That might be enough to convince Svajian to push an update that let his customers control their sous vide gadgets without looping the commands through an expensive cloud service. And if it wasn't, well, then someone smarter than him would step into the market and bankrupt him by giving his users a way to escape his venal grasp.

Parts-pairing/VIN-locking/DRM techniques are just some of the many ways in which manufacturers exert control over their products.

Take those "terms of service" documents that neither you nor anyone else has ever read. The 1986 Computer Fraud and Abuse Act (CFAA) has been invoked to bring *criminal* penalties down on people who violate those terms of service. So let's say

you've got a gadget that won't run unless it periodically checks in with its manufacturer's server, and you decide to connect to that server with your computer to see what kinds of messages that gadget is exchanging with your device. Your decision—which undoubtedly violates the company's terms of service—can give rise to a *criminal* complaint.

Now let's say that after you've figured out what messages are being exchanged between the gadget and the server, you make an aftermarket device that allows other people who own the same gadget as you to turn off the gadget's "phone home" feature. By helping other people violate the manufacturer's terms of service, you put yourself in *more* jeopardy. Tech manufacturers call this "tortious interference with contract," a once-obscure corner of contract law that has become central to the field. Your malicious tortfeasance can cost you everything—from your home to your kid's college fund.

That's just for openers. If the manufacturer's patents are implicated in your add-on, that manufacturer will come after you for patent violations.

Apple has invented a *diabolical* way to use trademark law to control its customers. The smallest subassemblies in Apple's products get engraved with microscopic Apple logos at the factory. As part of Apple's war on independent repair (which allows people to get their iPhones fixed, rather than replacing them) the company goes to great lengths to prevent non-Apple technicians from getting parts. That's where the tiny engraved logos come in. Broken Apple phones that escape Apple's own "recycling" system (which involves shredding phones so that none of the parts can be reused) are often shipped to Pacific Rim countries where recyclers break them down into their component parts, which American distributors buy and offer to independent repair techs.

Apple uses the existence of these minute engraved logos as a

pretext to get US Customs and Border Patrol to seize and destroy these shipments on the basis of trademark violations.

Now, normally, a trademark claim has to involve misleading someone about the “origins of goods or services.” If I stick a Pepsi logo on a can of Coke to trick you into buying it, that’s a trademark violation.

Selling refurbished Apple parts *as* refurbished Apple parts isn’t a deceptive practice. But Apple argues that because these parts might have been damaged while they were being extracted from dead phones, a buyer could unfairly come to associate the Apple logo with a defective product, under an obscure trademark theory called *tarnishment*.

This is an objectively stupid ploy, but stupid or not, it works. US Customs agents routinely seize and destroy shipments of Apple parts based on trademark tarnishment claims that boil down to something like this: “If you opened your phone after knowingly, deliberately getting it fixed by a third party who told you they’d be using refurb parts, and used a jeweler’s loupe to look at those parts, you would see a tiny Apple logo. Then, if the phone stopped working because the part was faulty, you would develop a negative association with our logo.”

The tech industry leads the world in thinking of new ways to layer IP around its products as a means of securing government assistance in enforcing its commercial preferences on others. As Jay Freeman, the creator of Cydia, an independent third-party app store for Apple iOS devices, puts it, this is “felony contempt of business model.”

Remember (from page 61) the hypothetical product meeting where we were deciding on whether to make the ads on our company’s website 20 percent more obnoxious, but we decided not to, for fear that 40 percent of our users would be inspired to install an ad blocker?

Well, the next item on the agenda is this: Should we make the ads in our *app* 20 percent more obnoxious in order to realize a 2 percent lift in top-line ad revenue?

All eyes turn to the killjoy who pointed out that web users would go on to install ad blockers and so convinced us not to enshittify our website. That person looks around and says, “You’re thinking too small! I think we should make the ads in our app 100 percent more obnoxious and shoot for a 10 percent increase in ad revenue. After all, it doesn’t matter if our users search for *How do I block ads in an app?*, because the answer is *You can’t.*”

Reverse engineering an app creates liability under the CFAA, DMCA 1201, and likely copyright, patent, trademark, tortious interference, and trade secrecy laws. In other words, IP law.

This is why every company is so sweatily insistent that you use its app rather than its website. An app is a website wrapped in enough IP to make it a felony to install an ad blocker or any other modification that makes the product work better for you at the expense of the company’s shareholders.

The metastasis of IP law is another downstream effect of tech’s market concentration. In the 1990s and early 2000s, when tech was composed of many small and medium-sized companies that truly competed, there were as many tech companies that *objected* to “felony contempt of business model”-style IP as there were firms that wanted this. The objectors were hoping to eat the promoters’ lunch by making interoperable products—for example, selling music and/or iTunes replacements that could work with Apple’s blockbuster iPod line. This disunity meant that IP law had far more checks and balances, limitations, and exceptions. To the extent that IP law expanded, it was as a result of demands from competing sectors, notably the entertainment industry, which pushed for a string of legal expansions in the name of fighting tech (the irony!).

Market concentration produced a unified position among tech, which threw in its lot with content in demanding the rapid and significant expansion of IP law, securing both new laws and broader interpretations of existing laws.

While we normally conceptualize regulatory capture as a form of *impunity*—the right to violate privacy, labor, and consumer rights and get away with it by insisting “It’s okay, we did it with an app”—that isn’t the whole story.

The complement to regulatory capture as impunity is regulatory capture as a *fusion* between the regulator and the regulated industry, such that the industry can shape and *wield regulation* against its rivals—other industries and startups that threaten its privileges, using the power of the government to maintain its commercial dominance.

Here’s an example that hits close to home. This book that you’re holding right now has an *excellent* audio edition. (Perhaps you are even listening to it, rather than reading the words off the page with your eyeballs like some kind of cave dweller.) I know it’s excellent, because I narrated it—and I produced it. I happen to think that audiobooks narrated by their authors are really great, because they allow people to literally hear the author’s voice, but I could have done the narration without *producing* my own audiobook—except that I chose not to. I chose to do the production because Amazon—which owns Audible, the audiobook monopolist that controls more than 90 percent of the audiobook market—won’t carry my books unless I agree to allow it to use digital rights management (DRM) technology on them.

Remember DRM? We discussed it back on page 139, in the passage on Section 1201 of the DMCA. As a refresher, DMCA 1201 is a law that makes it a felony to help someone bypass a lock on a copyrighted work. DRM is another name for that kind of

lock. (Recall that the other names for this include parts pairing and VIN locking.)

Every audiobook that Audible sells—which is very near to “every audiobook *anyone* sells”—is wrapped in Amazon’s DRM. That means that only an Amazon-authorized player can play back these audiobooks. As a customer, there’s plenty not to like about that arrangement—for one thing, Amazon has a nasty habit of changing its mind about having sold you something, and it designs its players to allow it to reach into the player and delete the book *after* you’ve downloaded it.

But from an author’s perspective, the problem is that DRM is an invitation to enshittification. If every audiobook you sell is permanently locked in to Amazon, then every reader or listener you have is *also* locked in to Amazon, and the more books of yours that readers invest in, the more locked in they are. If you’ve spent \$20,000 on your audiobook collection, that’s \$20,000 worth of audiobooks you have to forfeit if you leave Amazon. Functionally, that means that every writer’s best customers *can’t* leave Amazon, which means the writers *also* can’t leave Amazon, which means Amazon has those writers over a barrel.

Amazon knows it, too. In 2020, a group of independent Audible authors discovered an unannounced, secret accounting trick that had allowed Amazon to shift *at least* \$100 million from Audible authors to itself. The ensuing Audiblegate scandal convinced Amazon to soften this wage-theft-by-another-name a little, and remarkably few authors left Audible. They can’t; their audience is trapped, and so they’re trapped.

All of this is the perfectly predictable outcome of DMCA 1201: by making it a felony to help someone unlock their Audible books, Congress ensured that Amazon would abuse its authors to benefit its shareholders.

I don’t want my books used as lock-in bait by Audible, so I

don't allow DRM to be applied to them, which means that Audible won't carry them, which is why I don't just *read* my audiobooks, I also *produce* them, paying a director and an engineer to oversee the process. I have accounts with all the DRM-optional audiobook stores, like Libro.fm, Downpour, and Google Books, and I upload the books to each of them.

I love these stores,\* but they're *small*: remember, Audible's got 90 percent of the market, and the rest of these stores are sharing the remaining 10 percent among themselves. So I also do these massive Kickstarter campaigns to pre-sell the book, which takes as much effort—or more—as producing the audiobook itself.

It's a ton of work, and it's meant sacrificing a small fortune in lost revenue. My agent tells me that if I'd been less stiff-necked on this score, I'd have paid off my mortgage and fully funded my kid's college fund by now.

But I still do it. I do it because the Audible shakedown is downright offensive. Here's how perverse DMCA 1201 is: If I write a book, read it into a mic, spend thousands of dollars having the recording polished and packaged, and then allow Amazon to sell it to you, that gives Amazon more of a say over that book than I get—by a long chalk. If I, as the author, narrator, and investor in an audiobook, allow Amazon to sell you that book and later want to provide you with a tool so you can take your book to a rival platform, I will be committing a *felony* punishable by a five-year prison sentence and a \$500,000 fine.

To put this in perspective: If you were to simply locate this book on a pirate torrent site and download it without paying for it, your penalty under copyright law is substantially less punitive than the penalty I would face for helping you remove the audiobook I made from Amazon's walled garden. What's more, if you

\* Well, maybe not Google's.

were to visit a truck stop and *shoplift* my audiobook on CD from a spinner rack, you would face a significantly lighter penalty for stealing a physical item than I would for providing you with the means to take a copyrighted work that I created and financed out of the Amazon ecosystem. Finally, if you were to *hijack the truck* that delivers that CD to the truck stop and steal an entire fifty-three-foot trailer full of audiobooks, you would likely face a shorter prison sentence than I would for helping you break the DRM on a title I own.

Copyright is a system notionally designed to help creators and their investors bargain with other parties in the entertainment industry supply chain. But DMCA 1201—as written and then expanded through a quarter century of practice and jurisprudence—turns copyright into a weapon that powerful intermediaries like Amazon can use *against* creative workers and their investors.

Big Tech’s regulatory capture means that we have arrived at a juncture where copyright affords few rights to creators who make new works, and substantially more rights to a store whose sole contribution to those works is hosting a file server and payment processor that allows the public to buy the works, which gives Amazon not only a 30 percent cut of the purchase price but also the perpetual, legally enforceable right to veto the creators in their relations with the audience making those purchases.

There are examples like this for every form of IP, ways in which IP laws allow dominant firms to structure the whole market, to the detriment of creators, audiences, publishers, labels, studios, and new intermediaries that promise a better bargain for all concerned.

Economists and antitrust theorists spend a lot of time thinking about “market distortions.” Leftists are often skeptical of this line of inquiry, on the grounds that it supposes that there’s an “undis-

torted” market that is efficient, which is put out of equilibrium by certain kinds of regulatory failures.

But you don’t have to believe in the “efficient market hypothesis” to see how monopolies distort markets. The Amazon example provides a very concrete demonstration of market distortion.

Amazon is a powerful seller: the majority of US households have Amazon Prime, and if your household has Prime, you are overwhelmingly likely to start every shopping expedition by searching on Amazon, because, as a Prime subscriber, you’ve already paid for a year’s shipping in advance.

This means that merchants seeking to reach the overwhelming majority of American households *must* sell their goods on Amazon. As we’ve seen (on page 25), merchants are willing to put up with all kinds of nonsense to sell on Amazon, up to and including parting with 51 percent of every dollar they bring in.

For merchants to resist this pressure, they must secure their own market power—they have to become so big that Amazon needs them just as badly as they need Amazon. Thus we see mass consolidation throughout many supply chains, creating ever-larger firms that are scaled up to fight Amazon on fairer terms.

The publishing supply chain is a regrettably clear example of this phenomenon. When I started my career, New York trade publishing was composed of *dozens* of publishers. Today, that number is five. Publishers have gobbled one another up, first to resist the buying power of the big-box stores like Walmart and the major chains like Barnes & Noble (booksellers that grew by acquiring lots of other booksellers). Today those mergers continue in the name of resisting the power of Amazon.

In 2023, the US Federal Trade Commission successfully sued to prevent one such merger, between Penguin Random House and Simon and Schuster, which would have created a conglomerate composed of so many smaller publishers that its

full name would have been “Viking–Putnam–Berkeley–Avery–Ace–Avon–Grosset and Dunlap–Playboy Press–New American Library–Dutton–Jove–Dial–Warne–Ladybird–Pelican–Hamish Hamilton–TarcherPerigee–Bantam–Doubleday–Dell–Knopf–Harold Shaw–Multnomah–Pocket–Esquire–Allyn and Bacon–Quercus–Fearon–Janus–Random House–Simon and Schuster.”\* Penguin Random House is by far the largest of the Big Five publishers, dwarfing the rest by orders of magnitude. And yet PRH is an infinitesimal speck next to Amazon.

The FTC victory marked a major turning point in antitrust enforcement (more about this on page 227). But it was a Pyrrhic victory: having failed to sell itself to Penguin Random House, Simon and Schuster promptly flogged itself to KKR, a rapacious private equity fund whose rap sheet includes lethal rollups of nursing homes and care homes for people with developmental disabilities. KKR rolled up a bunch of companies that make fruit juices and introduced unsafe working conditions that caused an unprecedented spike in on-the-job injuries. It’s the villain that destroyed Toys“R”Us. It helped invent “surprise billing” by buying up hospital emergency rooms and taking them out of the hospital’s insurance deals, so people who arrived at the ER would find themselves on the hook for thousands of dollars in fees (including a “cover charge” just for setting foot through the door that could run to four figures, whether or not the patient received *any* care). KKR is behind the epidemic of dollar stores, with a nasty little scam that targets poor and rural communities by surrounding their only grocery stores with dollar stores until the grocery stores go under, then closing all but one of the dollar stores, with the sole survivor raising prices and slashing staffing.

Simon and Schuster is a beloved publisher whose execu-

\* Also, Scribner–Pantheon–Del Rey–Saga–Atria, and so many more.

tives truly care about books and bookselling, who kept the faith through the years when the company was owned by the massive corporate conglomerates Gulf and Western and then CBS. But they felt the need to sell themselves to the mustache-twirling villains of KKR. Why? Because publishing is in a squeeze. Its retail sales are dominated by a single massive electronic retailer and a single national bookstore chain (which is *also* owned by a private equity fund). There are many independent booksellers in the United States, but they are served by a single nationwide independent distributor. The world of non-bookstore sales (the mass market) is dominated by a handful of big-box stores, which exercise enormous buyer power.

When *any* part of an industry's supply chain is captured by a monopolist, the *whole* supply chain has to monopolize, lest it fall victim to a powerful buyer or a powerful seller.

After a supply chain has undergone this consolidation, only two groups remain, fragmented and disorganized, easy pickings for the cartels that have sewn up the industry: workers and customers. Writers have five major publishers to turn to, as do workers in the publishing industry. Readers overwhelmingly get their books from a big-box store, Amazon, or the one remaining chain. Even if you shop at a beloved indie store, the books you buy cost more than ever, and pass through the hands of the private equity-owned monopoly distributor, or through one of the Big Five publishers.\*

\* *Chokepoint Capitalism*, the book about creative labor markets and monopolies that I co-wrote with the Australian legal scholar Rebecca Giblin, was published by the wonderful Beacon Press, owned by the Unitarian Universalist Association. (Albert Einstein once wrote, "If we succeed in renewing the spirit of the American Constitution after the confusions of our day, it will be in considerable measure to the credit of the courageous efforts of the Unitarians and their Beacon Press.") However, like many other independent publishers, Beacon relies on Penguin Random House for distribution. That meant that Penguin Random House—part of a cartel that comes in for sharp criticism in our book, and that passed on publishing it—still got paid a dollar every time we sold a copy.

This is by no means unique to publishing. Health care in the United States underwent a similar consolidation: Pharmaceutical companies merged to monopoly and used their seller power to gouge hospitals. Hospitals formed defensive regional monopolies and used their buyer power to force pharma prices down—then used their *seller* power to screw the insurance companies. The insurers underwent their own mergers, and forced down hospital prices. But the disorganized, flapping ends of this consolidated supply chain are easy pickings for these giants, which is why, compared with people in other countries, American patients pay more for worse health outcomes, and American health workers get paid less for worse working conditions.

Virtually every sector looks like this: from trucking to groceries, hotels to aerospace. When Boeing airplanes start falling out of the sky, this is the force at work: consolidation, regulatory capture, enshittification.

All of these sectors love IP laws (in the sense of “laws that let me control my critics, customers, and competitors”), but with tech, it’s different. The expansion of IP law in a sector where everything has software—and thus embodies a copyrighted work—and terms of service means that customers and suppliers have lost the most promising, direct tool they have for defending themselves from the enshittificatory impulses of the companies they *have* to do business with.

## The End of Labor Power

When I entered the tech workforce in the 1990s, we were surrounded by the myth of the heroic founder, people like Apple founders Steve Jobs and Steve Wozniak, who kicked around for a few years working at HP\* before striking out on their own and founding a company that put their former employers in the shade. That was what we all aspired to.

But that dream shrank. As Big Tech consolidated its grip on the tech sector, venture capitalists and founders understood that the most likely “exit” for any startup was acquisition by a Big Tech company. This accelerated after the dot-com crash in the early 2000s, when the stock market entered a prolonged doldrum.

The new dream for tech workers became “Work for a big, lumbering company for a few years, then strike out on your own and do a ‘startup’ with the intention of being rehired by your old employer or one of the other giant tech firms.” These transactions are called *acqui-hires*, because the purchaser isn’t really interested in the target’s products, which are typically shuttered immediately following the acquisition. Those products don’t exist to be *used* by people; they’re really just a kind of postgraduate thesis project for techies, undertaken to prove that you *can* conceive, create, and ship a product. The company’s purchase price is divvied up among the early employees of the startup according

\* The old, good HP, back before it got into the inkjet grift.

to their shares, with a hefty payout to the venture capitalists—basically functioning as a hiring bonus and a finder’s fee.

This is an extraordinarily wasteful way to run a corporate recruiting system! The workers who “win” the acqui-hire game spend *years* working on a fake product, pulling all-nighters, and neglecting their families. The customers who love that product sink money and attention into it, not suspecting that it only exists as a way to demonstrate the team’s willingness and ability to wreck their lives in service to shipping code. The “investors” in these acqui-hires spend millions to get one successful acquisition, at very high risk.

But still, for tech workers, acqui-hires represented a shot at winning one of the medium-sized prizes in the Silicon Valley lotto: a lump sum of cash and a chunk of stock in a Big Tech company, and a job that you could do until you got bored and started another “company” in the hopes of getting your old boss to “rehire” you with another cash/stock bonus.

As acqui-hires slowed down, techies’ dreams shrank further. Young engineering grads started to strive for an entry-level job at a gigantic company that provided free massages, a laundry service, and a company kitchen with a complimentary assortment of every kind of kombucha known to humankind. If you hit every one of your key performance indicators, this would be a job for life of the sort that middle-class people once took for granted. (The corollary of the mid-century adage “Nobody ever got fired for buying IBM” was “Nobody ever gets laid off from IBM.”)

Then, in 2023, the US tech sector laid off 260,000 workers. In the first half of 2024, it fired another 100,000 workers.

Tech workers’ dreams have shrunk to pinpricks. Now the aspiration is “Get a \$300,000 engineering degree, get an \$80,000-a-year job at a tech company, and pay off as much student-loan debt as

you can before they fire your ass in the same year you hit every one of your performance metrics while they're making record profits.”

At this point, you've learned about all the ways that companies wriggled out from under the systems that disciplined them and prevented them from enshittifying. Even as they slipped free of those bonds, tech workers held the line.

Even after acquisitions, predatory pricing, preferential discounting, exclusivity deals, and other antitrust violations allowed the tech sector to sew up the market and eliminate competition, tech workers held the line.

Even after the newly consolidated industry captured its regulators and convinced them that violating our labor, consumer, and privacy rights was okay so long as it was done with an app, tech workers held the line.

Even after those captured regulators were pressed into service to smash startups, tinkerers, hackers, and hobbyists whose plugins, mods, and aftermarket parts disenshittified the products their bosses managed to enshittify, tech workers held the line.

But today, after devastating layoffs, the line once held by tech workers has broken.

Tech bosses know this, and they're thrilled with it. In the records of the Delaware Chancery Court where the lawsuit to force Elon Musk to make good on his binding promise to buy Twitter played out, we find evidence of it. Musk and his friend, the “investor” Jason Calacanis, had a chummy back-and-forth by text message in which Calacanis relished the possibility of firing Twitter employees as a means of enticing the survivors to put in longer hours and toe the line on Musk's corporate strategy: “2 day a week office requirement = 20% voluntary departures. Day zero . . . sharpen your blades boys.”

All through 2024 and into 2025, we've been treated to daily triumphant blasts from tech bosses about how they'll replace workers with AI. Tech companies are ordering work-from-home coders back to the office and delighting in the "voluntary" departures of those workers. It's a hard time to be a tech worker.

## Tech Rights Are Worker Rights: Para and Tuyul Apps

As any chickenized reverse-centaur could tell you, enshittified tech can transform any job into a nightmare. But in the absence of enshittification, in a world where workers can seize the means of computation, digital technology is a powerful tool for clawing back power from the bosses directly, even when the regulators and lawmakers who are supposed to have the workers' back fall down on the job.

That's because twiddling is a double-edged sword. While twiddling can erode gig workers' pay (through algorithmic wage discrimination and other, even blunter scams, as we'll see in a moment), *counter-twiddling* can push pay back up again, pitting algorithm against algorithm.

To understand why this is viable, we first need to spend a moment on security theory.

It's useful to conceptualize security matters as a contest between defenders (anyone who wants to keep the status quo) and attackers (those who want to change it). This is a bedrock of security thinking. You may have heard of military exercises that pit red teams (attackers) against blue teams (defenders).

Broadly speaking, attackers and defenders can be assumed to be in possession of similar knowledge and techniques: the same earthmoving machines used to build the ramparts for a fortress can be deployed by a besieging army to tear those ramparts

down. However, despite the two equally matched sets of technological possibilities, the red team usually prevails. For the blue team to successfully defend the status quo (that is, a fortress with walls that are still upright and acting as barriers to entry for the city within), it has to build walls with no flaws. For the red team to undermine those walls, it only has to find a *single mistake* that the blue team made, and the walls will fall.

This is the *attacker's advantage*. Under enshittificatory conditions, workers are on the blue team (hoping to defend their wages) and bosses are on the red team (trying to twiddle those wages down).

But when workers can twiddle back—when they can avail themselves of technology that counters the bossware that turns them into reverse-centaurs and other tormented beings—the teams switch sides. They become the attackers, the red team, and the advantage is theirs.

Here's an example: If you drive for DoorDash, you have to contend with an extremely shabby wage-theft trick. DoorDash tells drivers that they are their own bosses, that they get to pick and choose which jobs make sense for themselves. In practice, though, DoorDash hides a key detail from its drivers (whom it calls Dashers): how much the customer has committed to tipping. Tips are a hotly contested item in the gig economy, and multiple companies, including DoorDash, have been caught stealing their workers' tips, a practice they ended only under legal duress. Since these tips can constitute the majority of a Dasher's compensation, Dashers are required to commit to making runs that are often so poorly compensated that the driver can actually *lose money* on them, after factoring in fuel and vehicle wear and tear.

In hiding the tip from Dashers, DoorDash can entice drivers to commit to money-losing jobs. Why would the company do this? Because cheap jobs are enticing to customers, who love a

bargain. DoorDash started out offering money-losing deliveries that it subsidized out of its investors' capital. (Stage one of enshittification: Allocate surpluses to end users.)

Now DoorDash wants to recoup that investment by removing its subsidy. If it can trick Dashers into clocking in on money-losing jobs, it can shift the subsidy costs to them. (Stage three: Take surpluses away from business customers and hand them to shareholders.)

Meanwhile, DoorDash strongly suggests to its customers that they should tip heavily for better service, hinting that they won't get their deliveries in good time unless they tip (all this on top of creeping junk fees that get piled up at checkout). Some customers take the bait and offer big tips. (Stage two: Make things worse for end users to make them better for business customers.)

The fact that some Dashers can be tricked into taking jobs on a money-losing basis turns ordering from DoorDash into a kind of slot machine: as a customer, you put a dollar in the slot and pull the handle, and if you get lucky, you get a below-cost delivery. DoorDash can tweak the odds here by occasionally stepping in to offer a subsidy when no driver rises to the bait (giving out giant teddy bears).

For Dashers, the fact that some customers will pony up for big tips that you don't find out about until after you make the delivery turns driving into a casino game, too. Put your dollar in the machine (clock on for a job), pull the lever, and if you're lucky, you get an extra \$10 in tips. Again, DoorDash can improve the odds by adding its own subsidy here, giving out giant teddy bears to drivers, too.

This is a grubby little con game, and its technical execution is *very* clumsy. It turns out that when DoorDash sends a job to the app on a Dasher's phone, the job listing includes the tip amount, but the Dasher's app just hides that information from the Dasher.

This is some pretty bad blue teaming: “I sent my attacker a secret, but I put it in an envelope marked ‘Secret: Do not open,’ so I’m *pretty sure* they won’t learn my secret.”

That’s where Para, a small startup, enters the story. Para noticed that this extremely useful information was being sent to Dashers but hidden from them, so it created an app that revealed the tip, the secret number that a Dasher needed to know in order to figure out whether a job was worth taking.

DoorDash *lost its mind*. The company sent a threatening letter (your basic “felony contempt of business model” threat) and smeared Para with nonsensical claims that its app could expose Dashers to identity theft by stealing their Social Security numbers (implying that the DoorDash app stored Dashers SSNs in an insecure state, which is quite a weird flex, but whatever).\*

To its credit, Para refused to back down. DoorDash *poured* resources into fighting Para. I had a conversation with the company founders in 2022 during which they told me that a DoorDash insider told them that there were *forty* engineers assigned to blocking Para from uncovering Dashers’ full compensation.

Today, Para has expanded its offerings, with an “autodecline” feature that lets gig workers automatically decline any job offer that is below a certain level. This is part of a “multiapp” strategy that aims to let gig workers set up accounts with multiple services—Uber and Lyft, DoorDash and Grubhub, and so on—and get a dashboard showing them which service is offering the highest payout from moment to moment, playing the gig companies off against one another.

Gig workers are ground zero for this kind of counterwiddling, because they’re the first class of workers whose boss is

\* The app didn’t store Dashers’ Social Security numbers, thankfully. Also, in mid-2024, *every single Social Security number ever issued* was dumped on the dark net by hackers, so there’s that.

an app. When your boss is an app, you live with algorithmic wage discrimination and other arbitrary forms of abuse, like getting suspended without any explanation or appeal. Apps do all kinds of sneaky things.

The industry has thought up all *kinds* of ways to break the law and get away with it. When your boss is an app and you are misclassified as an independent contractor, you have no one to argue with and you've got little legal recourse.

Of course, this strategy isn't perfect. Instawork is an app that dispatches people to work as low-wage temps. In July 2023, when members of the UNITE HERE Local 11 who worked at Orange County's Laguna Cliffs Marriott Resort & Spa, owned by the University of California and managed by Aimbridge Hospitality, tried to bargain for a contract with their employer, the boss refused to deal, triggering a strike.

So Marriott/Aimbridge turned to Instawork to drum up an army of robo-scabs, dispatching gig workers to cross the picket line in a bid to break the strike. Any worker who refused to cross the picket line was permanently blacklisted from Instawork, which is the primary source of temp work throughout Southern California. Firing an employee for refusing to cross a picket line is extremely illegal, but by muddying the waters about whether workers were contractors or employees, Instawork was able to offer this scab-as-a-service deal to the region's major employers, who were only too happy to take advantage of it. No one called them on it—until they tried to make Thomas Bradley a robo-scab.

Thomas Bradley was an unemployed culinary worker who lived in his car. He refused to cross the UNITE HERE picket line at the Marriott and was blackballed by Instawork. The union took his case to the National Labor Review Board, fundraising to get him shelter and then getting him a real, full-time job at a

nearby union hotel, the Westin Bonaventure Hotel & Suites in downtown L.A.

There's something genuinely wonderful about workers who counter-twiddle their bosses' apps and escape reverse-centaurism. For example, drivers for Amazon Flex—a gig delivery platform that's even *more* exploitative than Amazon's Delivery Service Partner scam (discussed on page 120)—figured out that they could get more jobs if they bought burner phones and hid them in trees near Amazon warehouses. The drivers then installed remote-control software on their main phones that let them see the burner phones' screens and send taps and clicks to them.

This worked by tricking the Amazon dispatch algorithm into thinking that the drivers were at the warehouse's doorstep, which got them priority for new delivery jobs.

Sure, such counter-twiddling is a cat-and-mouse game that Amazon can eventually win by throwing more programmers at its driver dispatch app, but it's also the only way that the drivers can “bargain” with Amazon. Cell phone-festooned trees might be the only path Amazon has to find out how its delivery prioritization scheme affects the actual delivery workers.

Automation supercharges the ability of workers to push back against their employers. In the Lehigh Valley in Pennsylvania, the community of Dashers is small enough that the drivers all know one another. Dashers there were able to use a hashtag, #DeclineNow, to agree among themselves to reject lowball app offers, which pushed wages higher for all drivers. Before long, the #DeclineNow forum had forty thousand users, and wages were rising for Dashers everywhere as a result.

Apps like Para can automate #DeclineNow, and even coordinate among workers to raise the threshold for declining an offer, pushing it up and up.

But to get that kind of counter-automation, startups will need lots of risk-tolerant capital: enough money to pay programmers to bust through a forty-engineer-strong anti-counter-twiddling team at DoorDash, while fending off DMCA, CFAA, copyright, patent, trademark, and other legal attacks.

Other countries dangle a tantalizing hint of how well this can work. In Indonesia, motorbike riders find gig work offering both taxi and delivery services. Early on, these riders formed cooperatively run clubhouses to offer shelter, repair, and social services for members. These co-ops became worker hubs where riders discussed the problems they had with their robot bosses, and that led to the creation of tuyul\* apps: apps that modify the functionality of the gig platforms' apps.

Tuyul apps offer a wide range of functions to riders. One popular tuyul app increases the font size used by the official dispatch app, which allows older riders who struggle with tiny type to read information about the next job without finding their reading glasses. (As a person who is currently typing on a laptop screen that's turned up to 200 percent magnification, I approve.)

Other tuyul apps are *far* more ambitious, like the app that allows riders to spoof their location. This is widely used by riders who are hoping to pick up taxi fares when commuter trains pull into busy train stations. Under normal conditions, the dispatch apps will not assign a train-station pickup to a driver unless that driver is right in front of the station. This creates incredibly dangerous traffic jams, as riders, family members, hawkers, and others press up against the station as the train pulls in. So smart riders install the tuyul app and wait around the corner,

\* The word *tuyul* refers to a childlike spirit in Indonesian folklore that helps its human master earn money by stealing.

while spoofing their location so that, as far as the app knows, they are sitting in pole position to pick up a taxi rider. This is a higher-tech, easier, and more reliable version of Amazon Flex drivers hanging burner phones from trees in front of Amazon warehouses, but it shares the same essential characteristic: by allowing workers to seize the means of computation, these tactics override the shortsighted, dishonest, or just foolish choices of their bosses.

Tuyul apps are a hint of what a fair automation-centaur fight would look like, one in which bosses didn't get a government-backed veto over how their workers' technology worked.

As with privacy blockers plugging the gap for a long-overdue update to privacy law, tuyul apps aren't a substitute for better labor law. But even so, they represent a significant improvement over a world of weak labor laws and *no* adversarial interoperability self-help measures for workers.

What's more, a worker whose wages and working conditions are being (imperfectly) protected by counter-twiddling is a worker who has more time and money to apply to the project of improving labor law and labor protections.

And finally, rational bosses who know that workers *can* counter-twiddle are incentivized to treat their workers more fairly in the first place. Just as a printer company has to factor in the possibility that hiking ink prices will drive users to figure out where to get third-party ink (forever), just as web companies have to worry that making their ads more intrusive will trigger their users' installation of permanent ad blockers, so will bosses using an app to cheat workers have to consider the possibility that this abuse will trigger workers to create and install counter-apps that make it impossible for the bosses to *ever* know whether they are getting accurate data from their apps again.

Of course, lots of executives lack the (ahem) executive

function to act in their own best interest when that means giving in to their workers. When those hotheads yield to their enshittificatory impulses, workers can *still* avail themselves of counter-apps (even as they ask the National Labor Relations Board, which may or may not exist by the time you read this, the state attorney general, a union rep, or a class-action lawyer to step in).

# The Google Walkouts, Tech Solidarity, and Tech Unions

It's hard to overstate how *magic* Google was in its early days. Real magic, not the cheap trick of Uber, which figured out how to get a stranger to pick you up in minutes and drive you anywhere for a fraction of the cost of a cab ride. (The secret was losing a ton of money on every ride.) Google did something no one else had managed to do: make sense of the whole web.

The search engines we all used before Google came along were locked in a losing race against spammers, who figured out how to game the primitive ranking algorithms engines like Lycos relied on. Crude tricks like adding a hundred synonyms for *cat* in invisible white-on-white type to your web page could make it the top-ranked page for searches for *cat*.

To make things worse, these early search engines' method for chasing revenue was purely enshittificatory: they sold search results to the highest bidder. So a search for *cat* might yield several paid ads from companies hoping for your clicks, followed by several more spam results from keyword stuffers and other improbably successful spammers (or, as they would be called today, search engine optimizers).

Between spammers and payola, the search engines were eating themselves from the inside even as parasites consumed them from without. Google had an answer for both pathologies.

In "The Anatomy of a Large-Scale Hypertextual Web Search

Engine,” better known as the PageRank paper, two Stanford grad students named Larry Page and Sergey Brin set out a method for sorting good web pages from bad ones: *citation analysis*.

This is an idea from academia, where publishing in scholarly journals is a key source of validation and career advancement (hence “publish or perish”). An academic’s importance to their field and their institution can be roughly approximated by looking closely at their peer-reviewed publications.

But academics aren’t just counting up the number of publications. Some publications matter more than others—the more important the journal you’re published in, the more your publication matters. In addition, there’s a (seemingly) objective way to measure the importance of a given journal: count how many times the articles published in its pages are cited by *other* journals. A journal like *Nature* isn’t prestigious merely because everyone knows its name—it’s prestigious because other researchers value the work published in its pages so highly that they pay special attention to the articles it publishes, and are more likely to cite those articles than they are to cite articles in rival journals. That means that publication in *Nature* counts more than publication in smaller journals, a measure that academics call *impact factor*. A journal’s impact factor is a measure of the likelihood that a publication in its pages will be cited by other publications.

This isn’t perfect. Like any other “reputation economy,” it’s a rich-get-richer system in which the most-cited journals are the first port of call for every major paper, meaning they are home to the most blockbuster findings, which reinforces their desirability for academics seeking to place their own papers.

Nevertheless, the mere fact that *Nature* chose to publish a given paper *is* a fairly reliable signal that the paper’s findings are significant and noteworthy.

Until the PageRank paper, this whole esoteric business was

the exclusive province of academics, who made something of a game of it. For example, mathematicians like to calculate their “Erdős numbers,” a measure of their proximity to Paul Erdős, a legendary and fantastically prolific mathematician. Erdős was an itinerant, driven, brilliant weirdo who would show up on his colleagues’ doorsteps, install himself in their guest rooms, and then collaborate on field-defining papers about areas of shared interest. (Erdős’s interests were very broad indeed.)

If you collaborated with Erdős on a publication, you have an Erdős number of 1 (Erdős’s own Erdős number is 0, of course). If you collaborated with one of Erdős’s coauthors, you have an Erdős number of 2. *Those* academics’ collaborators have an Erdős number of 3, and so on.

The PageRank paper proceeded from the insight that making links between two websites was a clunky, manual affair and the main reason anyone would link to anyone else was because they thought the link-ee had something notable to say.

By counting the links between websites, the PageRank algorithm was able to identify the sites that were most likely to be linked from other sites, these being the web equivalent to *Nature* or other journals with high impact factors. If these sites had pages that seemed to match the query, they would appear high on the list of results as an authoritative resource. But the authority of these highly linked-to sites didn’t end with the pages they published: these sites were also considered authoritative sources of *authority itself*. If your site was linked to *by* a site that lots of other people linked *to*, some of that Google-juice would be transmitted to your site, giving it more prominence in Google search results for queries that matched its pages.

So a site like the BBC’s ([bbc.co.uk](http://bbc.co.uk)) would be *very* authoritative, because lots of sites link to it. Meanwhile, if your site was linked *to* from the BBC, it would be considered highly authoritative, too,

because the BBC's editors thought it was important enough to link to, and since everyone else on the web was so fond of the Beeb, that site was also likely to be a good one. In other words, the BBC had a BBC number of 0. If the Beeb linked to you, you had a BBC number of 1.\*

And if the *New York Times's* site ([nytimes.com](http://nytimes.com)) linked to you, you'd have a *New York Times* number of 1, which would go into the ranking system, blended with that BBC number to produce an authoritativeness estimation. There's an infinitude of variations on the Erdős-Bacon number (a ranking of how close you are not only to Erdős but also to the actor Kevin Bacon), and Google kept score for all of them.

This system worked *fantastically* well—so well, it was almost spooky. The key insight in the PageRank paper was that all the links on the web as it existed constituted a latent map of authoritativeness produced by people who didn't set out to create this map and thus had no reason to attempt to distort or falsify it.

But remember Goodhardt's law (from page 103): "When a measure becomes a target, it ceases to be a good measure." Thanks to its excellent technique for making sense of the web, Google quickly became *the* authoritative site for search. (In other words, Google has a Google number of 0.) That meant that everyone wanted to be ranked highly in Google's search results.

Citation analysis—the academic impact-factor ranking technique that became PageRank—was very robust *before* it became

\* Perversely, early editorial policy of the BBC banned links to the rest of the web, on the grounds that these pages could change without notice. That meant that even if a linked-to page was found to meet the BBC's editorial standards at the time the link was made, it might later change in ways that fell short of those standards. In 2004, my friend Stef Magdalinski, a renowned UK public interest technologist, created a browser plug-in called News Online Wikiproxy that rewrote any BBC pages you loaded in your browser to add links to relevant Wikipedia articles. Later, the BBC softened its stance, making peace with the fact that the public web, for all its inconstancy, was too important a resource to ignore in its news reporting.

important, but after it became the primary way to garner traffic to one's website, a key weakness in PageRank emerged: it's just not that hard to make links between websites. Soon, "search engine optimizers"\* were creating "link farms" of sites full of links designed to replicate the formal signifiers of authority that Google's algorithm looked for. Google fought back by deploying ever more sophisticated and complex analyses that sought to disqualify pages whose authority seemed to come from inauthentic sources.

This is a surprisingly subtle process. The mere fact that a link farm seems to promote a page should not automatically disqualify that page from being trusted by the algorithm. If Google took this blunt approach, then pranksters, extortionists, and other bad actors could create link farms and direct all their energy to innocent sites (like [bbc.co.uk](http://bbc.co.uk) or [nytimes.com](http://nytimes.com)) and get them kicked out of Google's index.

As Google's ranking algorithm ramified into a dense forest of tests and evaluations, the way Google talked about its algorithm changed subtly, with profound implications.

In PageRank's early, startlingly effective years, Googlers talked about search ranking as though they had discovered a kind of empirical truth about human knowledge. (Recall that Google's mission is to "organize the world's information and make it universally accessible and useful.")

When members of the public complained to Googlers about how their carefully crafted websites were dispreferred by Google's algorithm, the company line was simple: To get a higher ranking in Google search results, make a better page. The only way to increase your ranking was to improve the informative value of the thing you wanted ranked. It was as though Google believed

\* That is, spammers.

that it had used a kind of obscure academic mathematical ranking to trace the location of Plato's cave, and that it had installed a backward-facing camera at its firing line, staring directly at the true forms that cast the shadows on the cave wall.

But for Google, the idea that its rankings were math and not judgment was a double-edged sword. Governments of the world are far more likely to defer to the free speech rights of someone expressing *judgment* than they are about someone solving an *equation*.

That meant that governments grew very interested in telling Google what it had to rank highly—and what it should downrank or exclude altogether. Just because the empirically correct result for *Where can I find illegal content?* is a bunch of websites full of illegal content, it doesn't follow that Google should be permitted to link to these illegal websites. As Google became the canonical index to the web, it found itself besieged by legal demands to alter its rankings in the name of preventing copyright infringement, child sexual exploitation, terrorist recruiting, the dissemination of information about procuring or producing weapons and drugs, blasphemy, libel, and a host of other forms of speech that someone, somewhere didn't want the rest of us to see.

In 2012, Google changed its tune. It commissioned Eugene Volokh, a world-renowned legal scholar and First Amendment expert, to write a law-review article about the expressive nature of what Google was doing when it combined all the "signals" that it used to produce its rankings.

In the paper, Volokh argues—convincingly, to my mind—that Google's core activities are *editorial* in nature, not *empirical*. A Googler trying to find a way to keep a spammer out of the top-ranked results for a search index rarely writes a crude rule like "If the website is spammer.com, then don't put it in the results." Instead, the programmer seeks to identify *qualitative* aspects of

the spammy pages that make them a poor result, and then looks for *quantitative* correlates of those qualities that can be measured and weighed in *every* page on the internet, as a means of increasing the quotient of materials with subjectively positive traits that are likely to appear in the top results of a Google search.

Even when the programmer uses some quantitative test—for example, making a tweak to the ranking system, then waiting a few minutes for a million people to run queries whose results reflect the new system and seeing how many of those searchers run a second query to refine their search because they were dissatisfied with the results the first time around—the decision to use that criterion is, itself, *qualitative*.

In other words, the programmer who tweaks the ranking algorithm, runs some tests, and tweaks it again is doing something analogous to the newspaper editor in chief who rearranges the articles above the fold on the front page, reorganizing them until they *feel* right for the editorial stance of the paper.

Google's narrative switched from claiming to have discovered the mathematical roots of universal truth, to having figured out how to harness mathematics to express its *judgment* about what a good search results screen looked like. This was an important change, both because it was *true* and because it established a basis for internal contention about what qualities a good search page should have.

When “What is a good search page?” became a question up for grabs at Google, it set the stage for later enshittification.

The Gomes/Raghavan affair, discussed on page 75, is a stark example of the way that Google's culture changed as it outgrew the discipline of competition. For decades, Google had insisted that “competition was just a click away,” but as Google bought out the search box on every platform and integrated its surveillance, cloud, and ad-tech services into the majority of the

internet's websites and apps, removing Google from your life became increasingly difficult.

Now, even if you switch your default search engine to Bing or DuckDuckGo, even if you switch from Android to iOS, even if you switch your cloud storage to a self-hosted ownCloud instance, even if you switch your email to Proton Mail, even if you navigate with OpenStreetMap instead of Google Maps, you are still a Google user from the moment you log on until the moment you go to bed—and even as you sleep.

Most of the websites you visit embed one or more Google assets—a tracking beacon used for Google analytics, a “free” font served from Google's servers, or an ad placed by Google after being sold in a Google marketplace on behalf of an advertiser represented by Google's demand-side platform. Whenever your browser interacts with a Google server, the transaction is logged by Google's servers and added to your profile. That profile is augmented with vast troves of information about you bought from the largely unregulated data-broker sector, from the purchases you make to the locations where your devices' unique Wi-Fi and Bluetooth identifiers have been logged. If you have an Android device, it sends a constant stream of telemetry to Google about your activities, even when you're not using it.

So while you can potentially use a competing product—swap Google Photos for Flickr, say—your decision to do so has little impact on Google's bottom line. The subtext of “Competition is just a click away” is that Google will be disciplined by the fear of your defection to a rival service and will govern itself accordingly, resisting the urge to enshittify out of a rational fear of the consequences for doing so.

By decoupling “competition” from “consequences,” Google, you'll recall, inherited the attitude of Ernestine the AT&T operator: “We don't care. We don't have to. We're *Google*.” Competition

for its own sake is an empty fetish, but competition for the sake of making companies fear the consequences of prioritizing profits over quality? That's vital.

From its outset, technologists prized jobs at Google. The company's hiring gauntlet became notorious for the strain it put on applicants' ingenuity and knowledge, but for those who survived the challenge, the company offered something akin to tenure at an elite university, at a salary that was orders of magnitude higher than even the best-paid academic could dream of. Indeed, Googlers were often encouraged to retain their professorships at top universities while drawing a fat salary and socking away generous stock grants at the Big G.

For years at Google, top technical talent literally ran the show. Managers charged with assembling a team to work on a new product had to convince technologists to accept a transfer to the assignment. Engineers maintained a nearly unquestionable veto over these requests. Google management could launch new products or change existing ones only if it could locate enough engineers who agreed with the approach.

That wasn't all: Googlers were also given "20 percent time"—one day in five to chase passion projects within the company. Most of these projects went nowhere (most non-20 percent Google projects *also* went nowhere), but the 20 percent program is responsible for one of Google's few post-Search, in-house successes: Gmail, invented by Paul Buchheit as a 20 percent project in 2004.

Google's founders came out of academia. Larry Page and Sergey Brin launched the company while completing their grad studies at Stanford. Clearly, some of Google's cultural deference to technologists reflected the founders' academic sensibilities—after all, those were the same sensibilities that led to the creation

of the PageRank algorithm, which operationalized the academic practice of citation analysis.

But from the very beginning, the Google Boys had adult oversight: consummate corporate types like Eric Schmidt, whose presence reassured the company's investors about its commitment to profit. The result was a kind of *détente* between profit and technical excellence, and it made everyone involved with the project very, very rich.

Investors' tolerance for Google's "indulgent" deference to its technical staff was justified. Google's reputation as a great (and profitable) place to work attracted top technical talent to the company, including people with incredibly scarce experience in scaling up the business to keep pace with its meteoric growth. Time and again, the engineers charged with maintaining Google's stellar reliability pulled off never-before-seen feats. The unshakable reliability of Google drove its growth, as businesses and individuals came to treat the company and its services as a given. Why bother keeping detailed notes about the things you saw online when you could "just google it" the next time you needed to call up some half-remembered piece of information?

And so Google grew. Even after it captured the vast majority of the world's search business, it continued to grow, by convincing so many of us to treat it as a kind of neural prosthesis. Rather than knowing things, we came to know which keywords we could use to invoke Google's retrieval of those things. Cell phone address books made memorizing phone numbers obsolete, and as-you-type spelling correction rendered memorizing tricky spellings obsolete, but ultra-reliable Google everywhere (especially in your pocket) made memorizing *everything* obsolete.

But eventually that growth petered out. Search could grow by convincing more people to use Google Search, and it could grow

by convincing Google Search users to use Search in more ways. But once all of us were using Google Search in all the ways that Search could be used, growth from Search flatlined.

Google's shareholders weren't going to take that situation lying down. After all, even if Google couldn't find more people to search, or more ways to use search, they could *certainly* find new ways to *charge* for search. Google hadn't run out of worlds to conquer; indeed, its conquest of market share and technical excellence meant that it could turn its attention to conquering its *margins*.

The fact that 90 percent of us used Google; that Google products had been woven into our mobile devices, calendars, email, photos, and education; that every search box we found on every device and service led to Google meant that Google could charge advertisers more to reach us. It meant that it could collude with Facebook to rig the ad market to increase prices to advertisers and reduce payments to publishers (pocketing the difference for itself), committing a brazen act of market rigging, ripping off billions, and although they were sued for this,\* they wriggled off the hook.

And it meant that Google could make search quality worse in order to increase the number of queries it took to get the answers you were seeking, which also increased the number of ads you'd see, and thus the revenue the company makes from you.

In other words, once Google stopped *growing*, it started *squeezing*. Lacking competitors, having locked in its users and business customers, Google could make things worse for both groups in order to make things better for its shareholders and its executives.

But there was one force that still stayed Google's hand: its

\* *State of Texas, et al. v. Google LLC* (SDNY 2002).

almighty engineering staff. Googlers who believed in the company's mission, "to organize the world's information and make it universally accessible and useful," were stubbornly uninterested in goosing the company's bottom line at the expense of its utility to a grateful world.

As Google put profit over mission, Googlers gave the company a lesson in the double-edged nature of vocational awe (discussed on page 64). Sure, Googlers had been willing to pull long hours, putting work before personal life and health in order to realize the company's mission. But the quid pro quo those workers expected was for the company to take the mission as seriously as they did.

Google managers had always tried to cajole workers into siding with shareholders over users, with the workers pushing back. Broadly speaking, the workers won those fights. When Google management began to steamroll workers who used internal channels to challenge the company's ethical drift, those workers took this violation of the contract as a signal that all bets were off. They went public.

The Googler uprising began in 2018, when Jack Poulson, a Google AI scientist, resigned after learning of the existence of Project Dragonfly, a neutered search engine designed to mollify Chinese state censors and pave the way for the company's reentry into the Chinese market. (Poulson learned of Project Dragonfly after memos concerning the project were leaked to *The Intercept*.)

While Google is utterly reliant on Chinese manufacturing for its hardware, and while versions of its Android operating system are widely used in Chinese products, Google's products—its search engine, its app store, and its cloud services—haven't been available to Chinese users since 2010. That was the year that Chinese government hackers broke into Gmail and stole

dissidents' private email messages. The Chinese state uses these kinds of intercepts not only to know whom to target for further surveillance but also to run covert smear campaigns and employ overt tactics like arrest or extrajudicial kidnappings, torture, and execution.

According to high-ranked Googlers, news of the Chinese government's breach touched a nerve for Google cofounder Sergey Brin. Brin had come to the United States as a refugee from the Soviet Union in 1979, when he was just six years old. He was raised on tales of KGB brutality, and had a visceral horror of totalitarian spying and the violence and intimidation it enabled. When Brin learned that his company was playing a part in Chinese state oppression, he unilaterally decided that the company would withdraw from the Chinese market. So Google's sudden 2010 withdrawal from China didn't require a huge fight. There were lots of business and ethical reasons for it—and, of course, one of the Google founders wanted it.

But by 2018, things were very different. Yahoo! was barely a going concern, and Google's dominance of search was near total. While this unarguably represented a monumental achievement and a triumph for Google's business and technical management teams, it also represented a problem: Google's growth could no longer come from getting more people to use Google Search, or from getting people who used Google Search to do so in more ways.

That's the context for the Googler uprising that began in 2018. The first tremors came with the leaks about Project Dragonfly. If Dragonfly ever became a live Google product, workers knew, Google would quickly become embroiled in the roundup, arrest, and torture of dissidents on an industrial scale that would make the worst sins of Yahoo! circa 2005—when the company helped the Chinese government round up, arrest, and torture Yahoo!

users over their anti-government speech—look like amateur hour.

The revelation that Google management had created this program and kept it secret from Googlers—flouting Google's own system of internal ethics reviews—provoked a series of confrontations between Googlers and management. These began on internal chat and message boards and led to a series of contentious “town hall” meetings. (Senior leaders had long entertained challenging technical disputes from their employees with gusto, but at these meetings their appetite for defending the indefensible was palpably lacking.) Those led to more leaks, more press coverage. Then a Googler named Liz Fong-Jones called for a Google-wide strike if the company proceeded with the project without its normal security and ethics review. (Insiders understood that there was little chance that Dragonfly would pass this review, which was why management had bypassed it.)

Faced with this uprising, Google management blinked. The company canceled Project Dragonfly in spectacular fashion: the announcement came in the form of congressional testimony that included a promise not to attempt future reentry to China without normal consultations (again, with the tacit understanding that Google's policies, if followed, would preclude this reentry).

For Googlers, the uprising was a heartening example of how much power they had over their bosses, and how collective action could hold the line in moments when management rationalized their way into choosing profit over not being evil.

For Google management, the Dragonfly affair highlighted the danger that their empowered, uppity workforce represented. In the year after Dragonfly, Google management would confront a series of fresh revolts from a workforce that saw itself in the model of the thirteenth-century barons who pressed King John to sign the Magna Carta.

The next major uprising came with the news that Google had embarked on a secret project to build AI tools to help guide lethal US drone strikes. Like Dragonfly, Project Maven bypassed Google's much-vaunted internal ethics checks. (Subsequent leaks revealed top Google managers shouting at one another in ALL-CAPS emails about the absolute necessity to keep the project secret from Google's workforce.) The revenues from Project Maven amounted to pocket change: a mere \$9 million, barely enough to cover the kombucha budget for the cafeterias in just one of the dozens of Google's worldwide offices.

But further leaks revealed that the managers involved had sold Project Maven to top government officials for the promise of "exponential" increases in military contracting, especially for weaponized AI. (In the late 2010s, Google was considered the world leader in AI, having scored a suite of impressive technical feats through its DeepMind division. Later Google dysfunctions owe much to management's panic when upstarts like OpenAI shot past the company with chatbots and image generators. Today, Google is playing catch-up with its comically inept Gemini AI.)

Silicon Valley has a long history of close collaboration with the US military. The region's mix of naval shipbuilding and high-tech companies, along with historic ties between Stanford, Sand Hill Road venture capitalists, and the Pentagon afforded many opportunities for tech giants to fund their business- and consumer-facing products with fat, secret military contracts. As an added bonus, the Pentagon had a history of stepping in to rescue its key tech contractors from antitrust enforcement with emphatic statements to regulators and courts that the United States could not win its many wars unless its tech monopolists remained intact.

But Google had been printing money ever since it figured out how to sell ads against search results, and its reputation as

the “Don’t be evil” company, along with its quarter-over-quarter steady growth, gave it a *huge* advantage in hiring the world’s top technical talent, so the company had largely steered clear of military contracting.

So long as Google kept growing, its share price kept increasing. So long as Google’s share price kept increasing, its employees would happily accept Google shares over cash, which is a very handy situation, since Google can only get cash by convincing businesses and users to pay it, while it can make as many shares as it needs simply by typing numbers into a spreadsheet.

Thus, Google’s conquest of the search market was something of a Pyrrhic victory. If Google couldn’t keep growing, its share price would remain static or (heavens!) decline. Without a robust share price, Google’s wage bill would shoot through the roof, as its most skilled techies—always in short supply—took job offers elsewhere or demanded cash instead of shares as compensation. Paying its top workers’ healthy salaries with cash would further erode its balance sheet and risk more damage to its stock price, while losing key workers would endanger Google’s ability to keep running its global-scale, utility-grade infrastructure, which would *also* hurt its bottom line.

Google’s bosses were still stinging from a 2010 DOJ enforcement action against the company over its “no poach” agreements with other tech giants (as well as entertainment companies like Pixar), in which top brass from the Valley’s biggest companies colluded to suppress the wages of top workers by promising not to offer jobs to their competitors’ talent, and while they maintain they did nothing wrong, they still spent \$415 million to settle the case.

All this left Google desperate for growth. Unfortunately, the opportunities for growth were the sort of thing that would piss off workers: helping China spy on and neutralize dissidents or

helping the Pentagon drop bombs on distant populations. The company's solution to this problem was to try to keep its sellouts a secret. Secrets are hard. The company failed.

As news of Project Maven spread among the workforce—and then in the press, as outraged Googlers leaked the worst of it—another Googler uprising began. Thousands of Googlers signed open letters to CEO Sundar Pichai demanding that the company halt its military project altogether. A dozen of Google's most esteemed technologists publicly resigned on a single day, and made sure the press knew about it. As with Dragonfly, Google bosses were mercilessly grilled in the company's normally chummy town hall meetings, news of which leaked to the tech press, starting the cycle all over again.

By 2018, Googlers had their bosses on the run. Diane Greene, the executive responsible for Project Maven, quit the company in disgrace, and the company publicly bowed out of the race for a multibillion-dollar Defense Department contract.

Googlers were moving from strength to strength. There was widespread discussion, inside the company and out, of joining with one of the trade unions that had finally started to make small inroads in Silicon Valley, after decades of near-total failure.

Then came the walkouts.

Nominally, the Google walkouts were triggered by a sexual abuse scandal. Andy Rubin, founder of Android, was outed as a sexual abuser of his subordinates, but worst of all was the way that Google leadership dealt with Rubin's offenses.\*

A woman who'd complained about Rubin had apparently been pressured into accepting a cash settlement that came with a

\* Rubin denied the allegations, but Google management deemed the evidence against him to be "credible."

nondisclosure agreement. Every Googler's employment contract contained a "binding arbitration" waiver that banned them from suing the company, no matter how it had harmed them, and forced them instead to seek redress through arbitration.

Binding arbitration agreements have their roots in corporate disputes. When large companies have contract disputes, the resulting court cases can drag on for years and cost both parties millions in direct court costs, and even more in the indirect impact on their businesses during the lengthy battles.

That's where arbitration comes in. Corporate negotiators can agree ahead of time to settle their disputes with a neutral third party who is paid to interpret ambiguous contract language and solve other disagreements in a speedy fashion. Up until the 2010s, arbitration waivers were enforceable only when they were freely negotiated by parties of relatively equal size and power. This was a measure to ensure that the rights that Congress granted to individuals and companies couldn't be magicked away by powerful companies that could just hang out a shingle over their entrance that said, "By entering these premises, you agree to surrender your right to sue us, no matter what we do to you."

But from 2006 to 2013, amid rising market concentration and inequality, Supreme Court justice Antonin Scalia wrote a series of opinions in which the court stripped away safeguards from binding arbitration. By the mid-2010s, companies could add arbitration waivers to "contracts of adhesion" (contracts you don't negotiate, like the fine print at the bottom of your phone bill, or in a website's click-through terms and conditions, or in your employment contract), and these would be binding, even if the business insisting on arbitration was *far* more powerful than the person or business on the other side of the contract.

These binding arbitration waivers usually require the company

to hire the arbitrators. This is presented as a fairness measure: the company may take away your right to sue it, but at least it'll pick up the tab for arbitration.

However, this means that when you accuse a company of harming you, defrauding you, or stealing from you, the person who decides whether you're in the right and, if so, what kinds of restitution you're entitled to is *working for the company* that you're upset with.

Unsurprisingly, this is good for the companies that insist on arbitration. Compared with judges or (especially) juries, arbitrators are overwhelmingly more likely to find that the corporations that sign their paychecks have done nothing wrong. In the rare instances in which arbitrators find against their clients, they overwhelmingly impose weaker penalties on those companies than courts do.

The Googler who was abused by Andy Rubin signed a binding arbitration waiver as a condition of working at Google—as had every other Googler. Binding arbitration waivers are common among workers in Silicon Valley and elsewhere. (The cashier who rings up your order at a drive-through has almost certainly signed one, as has the driver behind the wheel of your Uber.) Googlers who signed binding arbitration waivers thought they were agreeing to have their overtime or stock-option disputes settled by a mediator—not that they were losing their rights after they were raped by their bosses.

That meant that when Rubin's victim went to Google's human resources representatives, she bargained from a position of weakness. If she had been able to credibly threaten Google with a blockbuster lawsuit—including a bruising discovery process through which internal memos about Rubin's behavior would be dragged into open court—Google would have been incentivized to make a *much* larger settlement offer to her.

What's more, in the absence of binding arbitration waivers, Rubin's survivor could have chosen *not* to settle, and instead to go public, demanding that Google clean up its internal processes to protect similarly situated women at Google from predatory conduct by its top execs.

But that's not what happened. Google heard complaints from Rubin's survivor and—*finally*—Rubin's abuse exhausted the patience of Google management and he was fired. But on his way out, Google's bosses *paid him \$90 million*, hoping to forestall any ugly public repercussions.

In other words, Google knowingly allowed a man to terrorize an employee, then paid him tens of millions of dollars to go away. The woman he victimized was bound to silence and prohibited from suing the company for his actions.

Unsurprisingly, workers who signed on to work at the “Don't be evil” company were unwilling to keep this secret. After several Googlers spoke to *The New York Times's* Daisuke Wakabayashi and Katie Benner in 2018, Rubin's abuse—and Google management's complicity—became public knowledge.

That was the trigger for the Google walkouts: multiple days on which tens of thousands of Google workers publicly put down their tools and protested outside their workplaces, demanding an end to binding arbitration waivers and nondisclosures for sexual abuse claims.

The Google walkouts were about Rubin and the culture of misogynist impunity he represented, but they weren't *just* about that. Leaders of the walkouts—like Meredith Whittaker, now serving as president of the Signal Foundation—had also been key to organizing the Googler protests against Dragonfly and Maven. The walkouts were explicitly connected to a long run of Google conduct that chased growth by compromising on the ethical principles that the company had promised to its workers since its founding.

They worked. Google caved. In 2019, Google announced that it was releasing all employees from their nondisclosure and arbitration clauses for claims of sexual harassment and misconduct. Googlers had their bosses on the run.

But Google's bosses still felt the need to chase growth. The shareholders wanted it, and growth also let Google attract and retain top talent, paying them in rising stock (which Google could manufacture to demand on its own premises) rather than in precious cash (which originates with the Federal Reserve and is a felony to make on your own).

Luckily for Google, there were lots of interesting technical ideas floating around that showed growth promise. One of the most exciting was AI (or rather, "AI," since the label *artificial intelligence* is more marketing category than technology, historically slapped onto whatever looks exciting at any given moment). Google's DeepMind division had achieved technically impressive results with its convolutional network technology, which turned out to be a rich seam that threw off new, cool demos that dominated several viral news cycles.

But DeepMind's dominance couldn't last. Deep-pocketed competitors sprang up, and new, AI-powered chatbots built on large language models (LLMs) started to steal focus away from Google. The company responded with a full-court press to make its own LLMs, leveraging its vast resources to build some of the largest models ever conceived of.

This move attracted the attention of some of Google's top scientists, including Timnit Gebru, a distinguished AI researcher whose career had involved stints at Apple, Microsoft, and Stanford before she came to Google to work on AI ethics.

In 2021, Gebru and several outside peers wrote a paper titled "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?" that was accepted for the Association for Computing

Machinery's highly selective Conference on Fairness, Accountability, and Transparency.

This was a perfectly normal thing to happen at Google. Much of Google's success, after all, was down to its ability to lure top academic researchers into industry, where they were offered a corporate version of tenure—the freedom to pursue their research interests and publish their results. Google's top scientists appeared on the bill at academic conferences all over the world, a fact that made it easier for the company to lure in even more leading scientists. This represented a significant advantage for Google over competitors like Microsoft, which routinely prohibited its scientists from talking to the public about their research. (In 2020, I had to kill a story commissioned by *MIT Tech Review* when Microsoft told one of its researchers—the top scientist in a specialized field who had published far and wide on his area of expertise—that he had to cancel his interview with me and cease talking to the press about his work.)

The fact that Gebru and her colleagues' work was implicitly critical of Google's own research agenda was also unremarkable. After all, tenured professors were allowed to criticize their employers—that independence was the whole point of tenure. If Google was right and Gebru was wrong, that could be determined by conducting further research and publishing the results, as in any scholarly, scientific, or academic dispute.

That's not the attitude that Gebru's bosses took. They demanded that she and her colleagues withdraw their paper. Even after Gebru offered to remove her name from the paper, they remained insistent that this technical paper, written by esteemed non-Google employee scientists and scholars, not be presented to a group of their peers at a learned meeting.

When Gebru and her colleagues went public with this news, it sent shockwaves through Google's workforce. For two decades,

the world's top scholars had come to Google on the basis that it was equivalent to getting tenured at an Ivy League college, if Ivy League colleges handed out stock options and employed an army of gourmet chefs for their free commissary.

When a Google manager ordered one of the company's most distinguished AI scientists to suppress a research paper that had already been accepted into a highly selective scientific conference, it revealed another important difference between tenure and a job at Google: Google is a massive multinational corporation. At gigantic corporations, mouthing off to your boss gets you in trouble. It can even get you fired.

Google proceeded to fire Timnit Gebru.

After years of ever-more-muscular displays of worker power by Googlers, the firing of Timnit Gebru—at the peak of the COVID-19 lockdowns, in December 2020—marked a shift in the attitude of Google bosses to their cherished employees.

The Googlers I know describe 2021 as a year of tightening discipline and managerial impatience with the workforce's demands. But while Google was getting snippier with its workforce, it was pitching woo to its shareholders.

In 2022, the company announced its first-ever dividend, at \$0.20/share. After all, the pandemic lockdowns that transformed “work from home” into “live at work” for hundreds of millions of white-collar workers around the world were a bonanza for Google, as demand for its services soared. The company posted massive profits, and the fact that it dabbled with its first-ever dividend felt right to many.

But Google didn't stop at a \$0.20/share dividend. It *also* announced a *\$70 billion* stock buyback. Stock buybacks are a controversial “financial engineering” maneuver through which a company offers to buy and delete its own shares on the open

market. As the number of shares declines, the value of each of the remaining shares goes up.

Normally, increases in a company's share price reflect an increase in investors' beliefs about the company's future—that is, share prices go up because the company just did something that makes it more valuable.

But stock buybacks make share prices go up while *decreasing* the value of the company. Google was \$70 billion poorer after its buyback program—nevertheless, its share price rose by 13 percent within hours of the announcement. To be clear, that announcement didn't include any information to indicate that Google had found a way to make more money: Google hadn't found more customers or discovered a way to charge its existing customers more. It hadn't invented any new technology or launched any products. Instead, Google had *removed \$70 billion* from its balance sheet, depriving itself of \$70 billion that it could use to hire new smart people or fund its existing smart people to make new things that the rest of us would pay for.

Through most of the history of US public markets, buybacks were classed as illegal stock manipulation, not all that different from “wash trading” (when a company has its own shills buy its stock to drive the price up). But as markets grew more concentrated, large companies were able to increasingly capture their regulators. In particular, they convinced US Securities and Exchange Commission enforcers that stock buybacks satisfied the “safe harbor” clause in SEC rule 10b-18, a narrow exception to the ban on stock buybacks that has been stretched to swallow the rule.

Many tech companies have engaged in this stock swindle. (It's a long-standing favorite at Apple.) But Google—the “Don't be evil” company—had never felt the need to engage in stock manipulation. Not until late 2022, when it lit \$70 billion on fire.

What came next was even more shocking: in early 2023, Google announced that it was laying off *twelve thousand workers*. The \$70 billion Google had just spent on its buyback would have paid those workers' salaries for the next *twenty-seven years*. (Meta did its own buyback and mass layoff shortly thereafter.)

The Google layoffs were part of an industry-wide trend. As growth in tech slowed and investors continued to demand sky-high profits, the tech sector turned to cost-cutting, with an emphasis on firing workers. As noted earlier (page 156), 2023 was a bloodbath: 260,000 tech workers were fired. The first half of 2024 was little better, with tech bosses firing another 100,000 workers.

This is different from other mass tech layoffs, like the firings after the dot-com bubble burst in 2001. Back then, tech companies were hemorrhaging money, many of them never having earned a cent in profit. Without their investors' largesse, they couldn't keep the lights on.

But the layoffs of the early 2020s came from companies that were posting tens of billions of dollars in profits. In 2001—when bosses had to extend job offers to two or three workers before one of them accepted the offer—firing workers was the very last resort. In the 2020s, it's been the first.

Mass firings aren't just a way to cut costs and beef up the balance sheet. They act as a powerful disciplinary force on workers, changing their posture from "I won't enshittify that product I missed my mother's funeral to ship, and you can't make me" to "Whatever you say, boss."

Recall the exhibits from the Delaware Chancery Court case over Elon Musk's Twitter acquisition, the direct messages in which the venture capitalist Jason Calacanis relished the thought of mass firings as a way to put those cocky tech workers in their place: "Sharpen your blades boys."

All the Big Tech companies are enshittifying, responding to

the market conditions that allowed them to make life worse for us to make things better for their shareholders, without fear of competitors, regulators, interoperability, or their own workers.

But no tech giant was ever quite so beholden to its workers as Google—and no company has executed such a total transformation of its relationship to its workforce as Google, either. At Google, workers held the line on all kinds of unethical behavior, not just the spectacular struggles over drone warfare and Chinese censorship but also a thousand everyday struggles that cashed out in favor of workers who harbored at least some fidelity to “Don’t be evil” or at least “Organize the world’s information and make it universally accessible and useful.”

Google’s anticompetitive conduct goes back decades, all the way back to deals like the 2007 bargain to make Google Search the default on iPhones. But for all that Google had arranged the game pieces so that it could cheat at will, mustering that will was always complicated, as Google contended with its workforce.

Axing twelve thousand Googlers in 2023 and thousands more in 2024 was a small price for Google to pay to allow managers total discretion about when they’d cheat and how. It was a price Google paid gladly, and we’re all living in its aftermath.

# Rent Seeking and Technofeudalism

Right about now, you might be thinking something like this: *What did you expect? That's just capitalism, right? Minimize costs (including labor costs). Maximize profits. Take care of the shareholders first, as is the sacred duty of every CEO.*

But is it capitalism? In his 2023 book, *Technofeudalism: What Killed Capitalism*, the radical economist Yanis Varoufakis, formerly both the chief economist of the video game company Valve and the finance minister of the sovereign nation of Greece, argues that tech firms have transitioned away from capitalism and into a new system he calls *technofeudalism*.

Varoufakis defines *capitalism* as a system designed to preference profit over rent. *Profit* here refers to income that someone reaps by investing in capital (machines, facilities, etc.) and then paying workers to use that capital to bring in money. Whatever is left over after the capitalist pays off loans, depreciation on the capital, and wages for the workers is profit.

By contrast, *rent* is income that someone reaps merely by *owning* something, often something that a capitalist needs to make a profit (economists call such things *factors of production*). The most obvious form of rent is, well, rent.

If you want to run a coffee shop, you'll have to invest in capital (like espresso machines), consumables (cups, stirrers, milk, and beans), and labor (the baristas). You also have to pay rent to your landlord.

If you do this right, you will make a profit: you'll sell enough coffee, at a high enough price, that you'll come out ahead. But profits are fragile things. If someone opens a better coffee shop across the street and your customers and workers switch to that shop, your profits will dry up and you'll go bankrupt.

For the eighteenth-century “moral philosophers” who defined capitalism, this precarity was a feature, not a bug. The fact that every capitalist knows that they are one competitor away from losing their customers, their workers, and their fortunes means that they must invest in training and rewarding their employees, upgrading their capital, and finding ways to improve the quality of their products while lowering their prices.

For Adam Smith and the other “fathers of capitalism,” profits were a kind of magical carrot that could be dangled before frail, imperfect, greedy, and rationalization-prone human beings to get them to do the right thing for all of us.

Unsurprisingly, Smith and company hated rent. The landlord who owns the building where your coffee shop went bust, thanks to competition from a hot new café across the street, is in *great* shape. After all, that landlord now has an empty storefront to rent out that's on the same block as the hottest coffee shop in town!

The feudal lords who preceded the capitalists of the Industrial Revolution owed their fortunes to rents. The aristocracy had large landholdings on which dwelled peasants who were “bound to the land,” prohibited from moving without permission from their patrons. Peasants were “free” to work the land, and work it they did, because each peasant owed annual rents to the lord—rents that were due irrespective of blights, droughts, floods, and fires. The lords controlled the key factor of production—the land—and extracted rent from peasants, who bore all the risk associated with planting and sowing. The lords got paid no matter what. Nice work if you can get it.

The Industrial Revolution transformed feudalism into capitalism. In order to produce the wool demanded by the capitalists' textile mills, land that had been given over to agricultural commons had to be "enclosed"—fenced off and used for sheep grazing.

Peasants were turned off the land, which was good news for the capitalists, because those landless peasants no longer had any way to feed themselves, meaning that they were willing to provide wage labor for the textile mills.

When ex-peasant labor became too expensive, capitalists invested in new, more automated machines that were "so easy, a child could use them," which was also good news for them, since the mill owners had taken to kidnapping Napoleonic War orphans from London and indenturing them to a decade's service. These children were used to displace the organized guilds of textile workers who operated the older machines.

Those workers were unable to get help from Parliament, so they formed guerrilla armies and propagated the half-joking myth that they were led by a giant called Ned Ludd (or sometimes King or General Ludd). They called themselves Luddites. Never let anyone tell you that the Luddites were afraid of technology or angry about "progress." That's a lie propagated by history's winners, whose great fortunes required oceans of blood from child laborers, murdered protesters, and enslaved Africans in the "New World" who provided the cotton for their machines.

The transition of millions of workers from peasant to proletariat was a bloody one, and it rightly attracts most of our notice when we think about the Industrial Revolution. But just as important was the transition from a society built on rents to a society built on profits. For the capitalists of the "dark Satanic Mills" to make their fortune, their right to profit had to triumph over the hereditary landowners' right to rent. The enclosure of the com-

mons produced two key factors of production: wool and workers. This came at the expense of the lords' fortunes and their hereditary right to rent. For capitalists to win, rentiers had to lose.

Now, no one argues that profits were *invented* as part of the Industrial Revolution. For as long as coin money existed, there have been people who invested cash in capital, hired workers to operate the capital, and pocketed the surplus as profit.

The feudal era wasn't defined by the absence of profits—rather, what made feudalism “feudal” was the triumph of rent over profits. When the interest of rentiers conflicted with the aspirations of capitalists, the rentiers won.

Likewise, the defining characteristic of the capitalist era was not the abolition of rents, but rather the triumph of profits. When capitalism's philosopher-theorists lionized “free markets,” they didn't mean “markets that were free from regulation,” they meant “markets that were free from *rents*.” For capitalism's theorists, every penny spent on rents was a penny that couldn't be invested on keeping the capitalist's profits flowing—that is, better wages, better products, better prices, and better processes.

The capitalist era had plenty of rents, but those rents were secondary to profits, and where they conflicted with profit, rentiers were told to pound sand.

Varoufakis's technofeudalism thesis holds that, in the years after the Great Financial Crisis of 2008, tech was transformed from a primarily profit-seeking enterprise to a primarily rent-seeking enterprise. The thing that makes the tech giants powerful is that they control “factors of production” that they rent to actual, productive businesses.

This is a powerful frame. It's impossible to deny that the majority of Big Tech revenue comes from these rents. Amazon rents search placement to its merchants, to the tune of \$38 billion a year. Amazon also corrals merchants into paying to use its

delivery system, penalizing merchants who make arrangements with third parties, even when those rival delivery services are as reliable and fast as Amazon's own. Naturally, Amazon charges more for its delivery than anyone else. And Amazon leads the cloud computing market, charging other businesses rent on servers and storage.

Apple and Google make even more money from rents than Amazon does, creaming 30 cents off every dollar that is paid through an app. Sure, they sell hardware, but they tie that hardware to their rent-generating clouds and app stores. Of course, merchants *also* pay billions in rent for placement on Google Search results pages.

Uber's platform is likewise a pure rent-accumulation system. Uber controls a factor of production: the system that connects drivers to riders. That asset produces income even when drivers are going broke.

Monopolies are key to an economy that runs on rents. Cable operators can bargain from a position of strength when it comes to licensing TV channels from their lineups, because in nearly every city and town in the United States, there's only one cable operator, with an exclusive municipal franchise to use the city's poles and sewers, and to wire up its homes.

A *monopoly* is an economic system in which markets are dominated by powerful *sellers*—like the movie theater business, in which one giant chain (AMC) and one small chain (Loews) and a smattering of indies and small chains sell movie tickets, whose price goes up and up.

But a *monopsony*, in contrast, is an economic system in which markets are dominated by powerful *buyers*.<sup>\*</sup> If you work in a

<sup>\*</sup> In a strict, technical sense, a *monopoly* is a market with one seller and a *monopsony* is a market with one buyer. But in the colloquial language of economics and antitrust enforcement, *monopolist* and *monopsonist* refer to companies with *market power*, primar-

company town with only one employer, you have to work for whatever wages the boss is offering, or leave town. If you want to reach the American retail buying public, you have to sell on Amazon's terms. The majority of US households have Prime, and the majority of Prime households start their shopping search on Amazon and don't go any further if they find a suitable item.

Uber's a monopsonist, too. Having spent \$31 billion of its early investors' money (mostly drawn from the Saudi royal family, who funneled the funds through the Japanese entrepreneur Masayoshi Son's venture capital firm SoftBank) subsidizing taxi rides, the company now dominates urban transport. The tens of billions of dollars that Uber blew on subsidies (losing 41 cents on every dollar it brought in for twelve years) convinced many cities that public transit was an irrelevant historical curiosity and that cheap ride hailing would be here forever, prompting a lost decade of disinvestment in transit. Meanwhile, rival taxi companies shuttered, unable to compete with Uber thanks to the company's labor misclassification, in which Uber pretended its employees were independent contractors and got away with it because Uber did it "with an app."

Uber now dominates urban transportation in many US and global cities, and it has used its monopolistic power to drive up prices—but it has also used its *monopsonistic* power to drive down drivers' wages.

Platforms aspire to both monopoly *and* monopsony. After all, platforms are "two-sided markets," brokering between buyers and sellers. What's more, the consumer welfare standard theory of antitrust is far more tolerant of monopsonistic conduct—where costs are lowered by squeezing workers and suppliers—than it is

---

ily the power to set prices. Formally, today's monopolists are really *oligopolists* and our monopsonists are *oligopsonists* (that is, members of a cartel who share market power), but no one can pronounce these words, so we stick with the *mono* prefix.

of monopolistic conduct, where prices are raised. Broadly speaking, when companies use their market power to drive prices down, they can do so without fear of regulatory reprisals. So platforms preferentially squeeze their business customers, and only hike prices once they're truly too big to jail.

A key aspect of market power is the ability to extract rents. Think of Amazon. As Varoufakis puts it, Amazon appears to be a bazaar where millions of independent merchants have arrayed their goods for sale. But in reality, one guy—Andy Jassy, the handpicked successor to Amazon founder Jeff Bezos—is in charge of this entire marketplace. That one guy decides what can be offered for sale, what price it sells at, where it's shelved, and, indeed, whether you ever see it.

This is Varoufakis's technofeudalism exemplified. It's an economic system in which the majority of value is being captured by people who *own* stuff, at the expense of people who *do* stuff. Of course, workers are used to living under this system: whether their bosses are people who rent access to their assets, or people who pay the rent so they can get something done, the person doing the actual work gets the smallest cut. The fight between technofeudalism and technocapitalism is a fight over whether the landlord or the café owner takes the value that's created by the barista.

In other words, the story of technofeudalism is a story about struggle, and the way to figure out whether you're living under technofeudalism or technocapitalism is to ask how conflicts between profits and rents cash out.

Take the app stores offered by Apple and Google (for mobile phones) and Microsoft and Sony (for games). There's nothing wrong with a system in which a distributor puts together a catalog of wares, carefully organized and laid out to be optimally

attractive to buyers. That's what every bookstore, every shoe store, and even the great model train store in my neighborhood does. But Apple, Google, Microsoft, and Sony are the *only* stores that can sell the wares created by a vast panoply of independent software authors. If you make an app for an iPhone, you *must* sell it through Apple's App Store, because iPhones are designed to refuse to run any app that isn't delivered via the App Store.

IP law—felony contempt of business model—gives this design choice the force of law. If someone wants to sell you an app for your iPhone, and you want to buy it from them, and they facilitate that by giving you a “jailbreaking” tool that circumvents the DRM on your iPhone so you can run an unauthorized app, they're violating Section 1201 of the DMCA and face a five-year prison sentence.

This is *very* different from, say, a bookstore. You can, for example, buy the first book in my Martin Hench series from Barnes and Noble, and the second book from Amazon, but that won't stop you from picking up the third book from an *excellent* independent bookseller like Third Place Books in Seattle, Vroman's in Pasadena, or Bakka-Phoenix Books in Toronto.

No matter who sells you my book, that merchant doesn't get *any* say over whose light bulbs you have to use in your reading lamp, or whose bookshelves you must shelve them on. And no one gets to stop you from selling the book to someone else, passing it to a friend, or leaving it to your kids in your will.

The fact that even large, powerful booksellers can't control your behavior means that it's much harder for them to control *my* behavior. If I decide not to sell books through Amazon, that'll cost me a lot of sales. It'll *hurt*. But, having sold you *one* of my books, Amazon can't threaten me with a *prison sentence* if I decide to help you find someone else to sell you another one of my books.

The fact that you can only run Apple-approved software on your iPhone, Google-approved software on your Pixel, Sony-approved software on your PlayStation, and Microsoft-approved software on your Xbox isn't merely a matter of how these companies relate to you as monopolists.

Just as important is how they relate to software authors: as a *monopsonist*. The fact that tech platforms are able to criminalize the act of authors selling their own work to the platform's users gives the platform enormous control over sellers. Sometimes, that control is reflected in high-handed editorial decisions, like when Apple Books blocked titles that linked to competitors like Amazon. (Imagine if Walmart refused to sell any book that contained directions to Target!)

But more often, that control is exercised in service to extracting *rents*. The mobile app stores charge a 30 percent commission on every sale of an app, and every sale *in* an app, and block any app that encourages users to buy direct from its author's website.

This is a classic fight between *rents* and *profits*. The app is a product, and the person or company that made it is engaged in profit-seeking behavior. The maker bought capital (computers, software development toolkits, offices, chairs, air conditioners, and foosball tables) and procured the labor of programmers who worked that capital, in order to make a product that it hoped to sell for more than it paid to produce it, thus generating a profit.

By contrast, the app store owners make their money by owning something—not just their app stores, but also the legal right to force the public to use their stores, and their stores alone. This lets them command fees that are 1,000 percent higher than any normal payment processor.

The fact that the law comes down on the side of the rentier over the capitalist here is a solid indicator that we're trending toward technofeudalism, and there are plenty of similar conflicts

where the government steps in to defend people who own things from people who do things.

For example, the US Patent and Trademark Office (USPTO) has a shameful record of rubber-stamping ridiculous, overbroad, incredibly obvious patent applications for “inventions” that often boil down to “doing something obvious that has been around forever, but with a computer.” These junk patents get filed by the thousand during every tech bubble, as startup hustlers seek to prove to venture capitalists that they have some “defensible IP” that will allow them to grow without worrying about competition. The USPTO’s attitude to junk patents has historically been “Grant ‘em all and let the courts sort ‘em out.”

Now, most startup hustlers spend nearly everything on salaries, and acquire few material things of value with their investors’ capital. When their startups fail, and get liquidated by their investors, their meager assets get sold at knockdown prices to whoever will take them off the receivers’ hands. When the AI bubble pops, there’s gonna be some great deals on fancy office chairs, espresso machines, and foosball tables.

It used to be that a failed company’s junk patents would end up forgotten, along with its server logs, web designs, and custom T-shirts. But early this century, a new kind of predator emerged: the patent troll.

Patent trolls buy up junk patents—some even have “R&D labs” where they manufacture their own—and then use them to extract huge amounts of money from productive businesses.

Patent trolls have no products. In fact, the polite name for them is non-practicing entities (NPEs). The only thing they manufacture is litigation threats. They use low-level, barely trained staff to seek out companies whose activities intersect in some way with the patents they’ve acquired. Then they send those companies “speculative invoices”—bills for licensing fees

for their patents, accompanied by bloodcurdling threats about the damages and fees the victim will be on the hook for if the case goes to trial. (US patent law provides for *triple* damages for “willful infringement,” so a patent troll can argue that once you’ve been notified that you’re violating their patent, you will have to pay three times over if you lose in court.)

For small and medium-sized enterprises, the license fee is set relatively low—most often, the sum is smaller than the amount you’d have to pay a lawyer just to review the threat and advise you whether you should pay or ignore it. That’s a pretty clever gambit, making it cheaper to pay than it is to find out whether you should pay.

A more ambitious, premeditated version of this scam sorts out potential victims by size, and targets the smallest fry first, seeking relatively small fees.

This was the tactic used by a company named Acacia Research, which claimed a patent on all streaming video. (The patent, acquired from a defunct dot-com, was granted long after the advent of streaming video!) The point of the demand letters Acacia sent out wasn’t to collect the small-dollar fees from mom-and-pop businesses—it was to amass a list of companies that had acknowledged the validity of Acacia’s bullshit patent.

Armed with this list, Acacia approached larger, better-funded, more profitable concerns, seeking a larger payout from each. After all, if dozens of companies have acknowledged the patent’s validity and paid to license it, you’d be nuts to tear up the demand letter and roll the dice on a court case.

Acacia was working its way up to the really big fish—national broadcasters, universities, and other massive video streamers—when the Electronic Frontier Foundation (EFF) stepped in, seeking to have the patent reexamined. Before the EFF got to it, the patent was voided in a lawsuit granted by some of the biggest

cable and satellite companies in the United States, and Acacia had to find another racket.

But that was then. Today, patent trolls often emerge victorious from the courtroom, sometimes winning *hundreds of millions of dollars* from companies like Apple and Samsung. That's thanks to the Eastern District of Texas, whose courts are notoriously sympathetic to patent trolls. This has given rise to a regional patent troll industry, so that dusty office buildings in small towns like Marshall, Texas, are the nominal headquarters to *hundreds of companies* whose presence in the city gives them the right to sue tech companies in the Eastern District. (Tech companies, meanwhile, try to curry favor with local juries by lavishing their East Texas towns with absurd gifts, like the year-round outdoor skating rink that Samsung installed in 2008, in a town where summer temperatures routinely climb to 90 degrees Fahrenheit.)

The Eastern District of Texas is a “made town”—the old-timey con-artist term for a city where the local law is on the side of the swindlers and not the marks. It's home turf for patent trolls, who produce nothing but own the right to sue for rents. If G+ Communications, maker of nothing, takes \$142 million out of Samsung as punishment for its making *something*, rents have triumphed over profits.

Varoufakis's message is that we are in an age where profits exist at the sufferance of rents, where conflicts between rents and profits are almost certain to settle in rents' favor.

He's got a point.

Patent trolls, after all, aren't the only form of IP troll. (Recall my definition of IP law: any law or regulation that allows a company to reach beyond its own walls and exert control over its competitors, critics, and customers.) There are copyright trolls, who acquire the right to harass people who violate someone's copyright.

The earliest copyright trolls were “porno copyright trolls,” like Prenda Law, which specialized in buying the rights to sue on behalf of pornographers. These trolls would use legal demand letters to internet service providers to extract the identities of people they observed downloading their pornography from BitTorrent sites, and would then send legal demand letters that contained a threat to expose their victims’ pornographic viewing habits as part of a legal claim. They gave special attention to the religiously devout, as well as teachers and the clergy, on the ground that these people would be especially frightened at the thought of exposure and would pay a premium to settle the matter.

Prenda played fast and loose with the law. At some point, the members of the firm realized that they could drum up a *lot* more victims if they used fake accounts to upload their own movies to pirate sites, and then participated in the BitTorrent download “swarm,” which would give them direct access to their victims’ network addresses. (In BitTorrent, downloaders form a swarm that swaps around small pieces of the file until everyone has a complete copy.)

Then they started stealing the identities of various relations and hangers-on in a bid to hide their corporate structure and assets from courts where they found themselves losing cases, spinning an ever-expanding web of fraud and perjury until, well, they went to prison.

But the porn copyright trolls were just the start. Copyright trolls were on the march, looking for rights holders who’d deputize them to threaten people who reproduced their works online. Photographers and newspapers assigned this enforcement power to various trolls, who made fortunes for themselves and their patrons by terrorizing people who pasted a photo into their blogs or quoted a news article in a discussion forum. Like patent trolls, copyright trolls typically set the price for a “license and settle-

ment” below the cost of consulting a lawyer to find out whether you should pay in the first place, and laugh all the way to the bank, rents in hand.

Even weirder and more odious than copyright trolls are copyleft trolls. *Copyleft* is a term of art for copyright licenses that encourage sharing of works. You’ve probably heard the term *open-source software* (or even the more ideologically oriented term *free software*): software that is released as open-source is governed by a license that allows anyone to copy it, run it, modify it, or share it. By creating a “commons” of open software, software developers transform their projects into collective works, allowing many people to customize and/or fix the code, and then build atop it. The GNU/Linux operating system is the most successful instance of this—GNU/Linux powers Google’s Android operating system, but it’s also the most common OS for embedded systems, and you probably have several tiny computers in your home running some version of Linux and hidden in everything from light bulbs to home routers, printer ink cartridges to speakers.

Sharing-friendly licenses for software have been around since the 1980s, but it wasn’t until the early 2000s that we saw a concerted effort to make similar licenses for “traditional” copyrighted works like books, movies, music, illustrations, and photographs.

In 2003, the Creative Commons (CC) project launched with a suite of licenses that sought to bring free/open licensing to these works. Creators can choose from a suite of licenses, depending on whether they want to restrict activities beyond mere sharing, such as incorporating CC-licensed material into new works, or making commercial uses.

CC licenses were a stunning success. *Billions* of works have been licensed CC, including all of Wikipedia.

The CC project is hugely ambitious. After releasing its US licenses, CC worked with legal teams all over the world to produce

localized versions of each license. These aren't mere translations: each one takes account of each country's unique copyright laws in order to ensure that the license is valid within its territorial borders.

The result is nothing short of heroic. A Creative Commons user can grab the CC-licensed text of an American's short story; animate it using CC-licensed, 3D-modeled characters from a French animator; and back it with a CC-licensed musical score composed by a Brazilian and recorded by a Japanese pianist—and the whole thing just . . . works, in *every* country with a CC license. Normally, this would require intense collaboration by half a dozen specialist law firms in countries all over the world, each of them working for hundreds of hours, with each of those hours billed out at hundreds of dollars. Instead, anyone can just grab these CC-licensed works and mix and match them, without consulting a single lawyer.

Amazing.

The Creative Commons lawyers are skilled, careful, and dedicated, but they're not infallible. The first three versions of the CC licenses (CC 1.0, 2003; CC 2.0, 2004; CC 3.0, 2007) were all haunted by the same bug.

These early CC licenses “terminate automatically upon any breach” of their terms. That means that if you make *any* mistake in using a CC-licensed work, you instantly become a copyright infringer. The fines for these infringements are *titanic*: for works registered with the Copyright Office, US law provides for \$150,000 *per infringement* in statutory damages.

To make things even worse, all CC licenses have a rather finicky set of administrative tasks you must perform in order to comply with them. For all of these licenses, you must do the following:

- Link to the original work.
- Name the author of the original work.
- Link to the license.
- Identify the license, with its version number.

If you get any of that wrong—for example, if you forget to include the version number of the license the original was released under—you have “breached the license” and you might now owe \$150,000 per use.

This shouldn’t be a big deal. After all, people who choose to release their works under a Creative Commons license *want* them to be shared, and if the sharer makes a minor error in their attribution, the original creator will probably just send them a friendly note asking them to fix it (or, more likely, ignore it altogether).

That’s how it should work, and how it *did* work, until the “copyleft trolls” arrived on the scene.

A copyleft troll is a rentier who sends out the same threats as copyright trolls, with a focus on CC-licensed works whose users have made minor errors in their attributions. Some copyleft trolls are sleazy lawyers who seek out people who’ve released CC-licensed works with offers of free money in exchange for the right to threaten people on their behalf.

But most people who release CC-licensed works aren’t interested in terrorizing strangers who made petty administrative errors. After all, the point of CC licensing is to encourage creative reuse and sharing, not to entrap and punish people who forget to include the version number.

So copyleft trolls took a page out of the Prenda Law entrapment book; just as Prenda Law acquired the rights to pornographic videos and then uploaded them to pirate sites in the hope of enticing downloaders whom they could shake down, prolific

copyleft trolls like the German photographer Marco Verch uploaded photo illustrations inspired by each day's top headlines to Flickr—a photo-sharing site with a massive trove of CC-licensed images—under the original CC 2.0 license. When unwitting victims used these photos on their blogs and websites while making tiny attribution errors, Verch threatened them with expensive litigation unless they coughed up hundreds or even thousands of dollars.

This scheme worked—for Verch (if not for his many victims, including a small Dutch nonprofit that was forced to shutter after it paid all of its cash reserves to Verch as punishment for using a single image).

How did Verch manage to produce fresh images every day? He stopped taking his own photos and instead hired photographers through the gig-work platform Upwork, asking them to take pictures based on top headlines and assign their copyrights to him.

Verch also outsourced his legal shakedown operation, partnering with the copyleft troll company Pixsy, which bills itself as a service to help photographers “protect their rights” but is a prolific legal-threat issuer, acting on behalf of copyleft trolls like Verch.

This is the pure triumph of extraction over production. People who make things—websites—are forced to cough up vast sums to a guy who does *nothing*. (By his own account, Verch works for four hours per week, and the “passive income” he gets from paying impoverished photographers to produce bait used to entrap small-time websites lets him pursue his hobbies, like running marathons.) These sums are sometimes so large that they actually extinguish the victims' enterprises, shutting down websites and the organizations that produce them.

These penny-ante scams, swindles, and hustles are the

spillover effect of technofeudalism. The transformation of IP law into a set of policies and regulations that allow the greedy and unscrupulous enshittifiers of the world to reach beyond the walls of their businesses to control their critics, customers, and competitors creates a Pixsy/Marco Verch-shaped hole in the economy, conjuring these rackets into existence.

Look, I love Creative Commons and I publish work under CC licenses literally every single day. I know and admire the lawyers who crafted the licenses, and I'd entrust them with my legal defense any day, on any charge. The point here isn't that CC was reckless or sloppy—it's that even well-financed, brilliant lawyers working to figure out how to make IP law into something that encourages innovation, sharing, and, well, a *commons* still find it nigh impossible to do so without creating a billion immortal weapons that can be exploited by the scum of the earth. If "the purpose of a system is what it does,"\* then the purpose of IP law is to help rent extractors extract rent, and any benefit to creative workers or creativity is an incidental, regrettable side effect.†

\* It is.

† Stafford Beer.



## Part Four

# The Cure

Just as there is an entire genre of nonfiction books that have a phrase somewhere in them that reads, basically, “Midway through the production of this book, a once-in-a-century global pandemic struck, and everything changed,” there is also going to be a vast collection of books that contain something to the effect of “Midway through the production of this book, Donald Trump won a second term as president of the United States, and everything changed.”

Sadly, this book is among them.

Donald Trump’s election represents the ultimate triumph of enshittification in the political realm. The policies that enable enshittification—lax antitrust, regulatory capture, weak labor laws, and state intervention on behalf of incumbents—are all on Trump’s agenda. After a four-year period of antitrust and labor vigor not seen for two generations, the United States has taken a huge step back—and its major trading partners like the United Kingdom and the European Union are also backsliding dramatically.

Technofeudalism is ascendant, but there’s a burgeoning sense that something has gone wrong. After years of increasing power of rents over profits *and* wages, we’ve had enough. Enshittifiers ruin the things we love, stick their hands in our pockets and their noses in our business, and feign shock when we refuse to go along with their plans. “Can’t you see that we just want to stay in business, and to do that, we’ve *got* to find recurring sources of revenue—like subscriptions to things you already own, and the pennies we get from spying on you all the time, in every way imaginable?”

During the Biden years, enshittifiers keep overestimating the degree to which their conduct has been normalized, mistaking the court of public opinion for a McKinsey staff retreat. When they pull the enshittification lever too hard, they get their fingers caught in it and hop around in agony, howling at the unfairness of it all.

You love to see it.

As discussed earlier (page 101), Unity, the widely used game engine, shocked its millions of customers by announcing that it would henceforth charge a “runtime fee” on the games its customers made with the software they’d purchased. The fees involved would have bankrupted a large plurality of Unity’s customers, including several who had invested large amounts of money on *forthcoming* games with Unity tools. These games were now write-offs, because their makers would lose money on every sale if they tried to release them.

Unity was manifestly unprepared for the shitstorm of bad publicity that followed. Game developers announced that they were halting all Unity work and would never develop with Unity again. These pronouncements came from indie game devs, then small studios, then large ones.

Hoping for some damage control, Unity president Marc Whitten tried answering his irate customers’ complaints in a YouTube “fireside chat.” He said, “The most fundamental thing that we’re trying to do is we’re building a sustainable business for Unity. And for us, that means that we do need to have a model that includes some sort of balancing change, including shared success.”

*Nobody* bought this. If one Unity customer does well, the “shared success” that Unity gets is to trumpet that it provided the tools used to produce a smash-hit game. It doesn’t get to demand a share of the revenue that game brings in.

Imagine if Picasso’s paintbrush maker demanded a cut of

every painting Picasso sold. Imagine if the carpenter who installed your new kitchen got a share of the closing price of your house when you moved.

Unity wanted to “share in its customers’ success,” as though providing the software those customers used entitled the company to an equity stake in their businesses. But equity holders don’t just share in success; they also share in *failure*. Unity wasn’t offering to help pay the salaries of the workers who built products with its tools. It wasn’t offering its tools for free in exchange for a cut in the profits it contributed to. It was offering the classic rentier’s wager: “Heads I win, tails you lose.”

The truly galling thing about Unity’s rent grab was how *affronted* its top execs sounded when they were asked about the backlash: “We’re only looking to grab some rent from people. We own something very important. We own IP. As everyone knows, you can’t ever truly buy IP—you just license it. You never bought one of our tools and you never will. You’ve only rented it. Pay your rent, you deadbeats. You know what happens to tenants who get behind in the rent? They get evicted.”

If you think that sounds like a caricature, just check out this statement from an unnamed spokesperson on a Unity forum where its customers were furiously decrying the company’s new pricing:

*Our terms of service provide that Unity may add or change fees at any time. We are providing more than three months advance notice of the Unity Runtime Fee before it goes into effect. Consent is not required for additional fees to take effect, and the only version of our terms is the most current version; you simply cannot choose to comply with a prior version. Further, our terms are governed by California law, notwithstanding the country of the customer.*

This is the enshittifier's credo: "We're just doing the thing that makes life worse for you so we can make life better for us. The socializing, buying, selling, publishing, driving, riding, working, and hiring you do on our platform is less important than the platform itself. Your job is to create as much value on that platform as possible. Our job is to harvest all of that value, leaving behind the smallest quantum of utility that will keep the platform from imploding. That is the *deal*. We're *owners*, you're *users*."

Happiest Baby made this pitch to end users who bought its SNOO Smart Sleeper bassinets, and evinced the same affronted protestations when its customers complained as Unity's bosses did when developers revolted. Remember, enshittification is an equal-opportunity predation scheme, and all platform users are ultimately on the same side of the enshittification wars: Uber drivers and Uber riders, Amazon sellers and Amazon shoppers. If you're not paying for the product, you're the product. If you are paying for the product, you're *still* the product.

They repeat this so calmly and confidently, as though we're unreasonable toddlers whose tantrums just prove that we don't understand how the world works.

There are times when this actually lands, especially if the company has managed to cultivate a cultlike following among its customers. Apple is the uncontested master of this. (It's no coincidence that Apple's defining marketing lead, Guy Kawasaki, called Apple customers the "Cult of Mac.") A large and vocal subset of Apple customers have been convinced that buying products from one of the most profitable corporations in human history makes them members of an oppressed minority, and they treat any criticism of Apple's—broadly terrible—business practices as sectarian attacks on their tribe.

But even Apple is losing stalwarts, as it attacks right to repair, gouges software vendors, spies on its customers, and contributes

to the mountains of immortal e-waste that are poisoning our land and seas. The fact that Apple's avuncular CEO, the billionaire Tim Cook, gave a \$1 million "contribution" (bribe) to Trump for his inauguration and sat behind him on the dais certainly took some of the shine off the Apple.

And Unity? Well, it might be the most widely used 3D tool around, but it's certainly not the most *popular*. Unity's customers still use its products because they work reasonably well, but their attitude toward the company is hardly affectionate.

Unity's customer revolt was so clamorous, so widespread, and so sustained that it ended the careers of the company's executives. CEO John Riccitiello was forced to resign. So was president Marc "Shared Success" Whitten. Unity's stock price cratered and never recovered.

This is how it's supposed to work. Bosses *want* to yank the enshittification lever, but they can't, because it's gummed up by several factors: By competition. By regulation. By interoperability. By the tech workforce.

Once, we had an old, good internet. The old, good internet had a succession of search engines that each improved on the last, which withered and died. It had hundreds of small and medium-sized companies that vied for our business. When big companies like Microsoft tried to enclose the internet, they were defeated by a mix of open standards—developed by hundreds of companies that joined together to make a commons because they knew they couldn't possibly capture the internet for themselves—and by vigorous antitrust enforcement. Hackers, tinkerers, and entrepreneurs built interoperable tools that plugged in to dominant services and defended value for end users and business customers, at the expense of platforms that got too big for their britches.

The old, good internet was full of intermediaries: hosting providers, ad-tech platforms, internet service providers (ISPs),

browser vendors, server software makers, email hosting companies, mailing list services, and everyone who made specialized software for file transfer, email, chat, and so on (before all this stuff disappeared into our browsers).

These companies were intermediaries, and they existed to help the people on either side of the connection transact with one another. Indeed, that was the formal, founding ethic of the old, good internet. The old, good internet came into being as a result of something called the *end-to-end principle*, which held that an intermediary's highest duty was to transmit information from willing senders to willing receivers as quickly and reliably as possible.

This was in contrast to older networks, especially the Bell System operated by AT&T, in which the kinds of data you could send or receive were subject to AT&T's approval. If you invented caller ID (for younger readers, this was an innovative feature that let you see the number that was calling you before you picked up the phone!), you couldn't make that work by telling the people you called how to receive your caller ID signals so they'd know it was you. Caller ID—and every other feature in the Bell System—had to be specifically provided for on AT&T's switches and other infrastructure. AT&T got to decide whether caller ID was allowed to exist, and how much it would cost.

The engineers who designed the internet had a vision for a “permissionless” network, grounded in open protocols. Your ISP's job was to receive the data your computer transmitted to it, inspect the envelope around that data saying who it was destined for, and shovel it down the line, without attempting to understand, prioritize, slow, or block that data.

The Bell System was built around a single, powerful intermediary: AT&T, which had accumulated political and market power by buying rivals, capturing regulators, and sending billions to its shareholders.

The “Netheads” who designed the early internet distinguished themselves from their sworn enemies, the “Bellheads,” with their belief that intermediaries shouldn’t override the decisions made by the users of their network.

Early internet intermediaries were both necessary and good. Necessary, because the early internet was *very* complicated for users, and each layer of intermediation was a chance to simplify that use. But also *good*, because the end-to-end principle meant that the scales tilted in favor of users who wanted to do things that benefited themselves, and away from intermediaries who wanted to make things worse for users in order to make things better for themselves.

Take email. In the memorable phrasing of Mike Masnick, founder and editor of the blog *Techdirt*, email is “a protocol, not a product.” In 1982, a technical standards body called the Internet Engineering Task Force created a standard for the format of text messages known as RFC 822, which defines the core of how email works.

Anyone can get a free copy of RFC 822, along with related standards like 1982’s RFC 821 (Simple Mail Transfer Protocol), and, with the right computer know-how, build an email client, an email server, or any number of other email programs (for example, an email bot that sends you reminders).

Email was born with caller ID as a standard feature: the *FROM*: field in RFC 821, which your email program can see even before the rest of the message is received. (Among other things, this is useful for rejecting email from people you don’t want to hear from—remember, the end-to-end principle is about delivering data between *willing* parties.)

The company that makes your email program *could* create a “feature” to hide that information from you, not displaying it in your inbox. It could simply omit the *FROM*: column from the inbox

view, or it could draw a black bar over it, or maybe fuzz the text. Then, it could charge you \$1.99 a month to turn off that “feature.”

But if your email provider did that, you’d probably just switch email programs. Remember, anyone who downloads RFC 822, 821, or any other technical standard can make a program that will send and receive email on your behalf. The enshittified email program would lose its users, and everyone else would gain users.

The old, good internet was full of intermediaries that tried as hard as they could to be useful and good. When they fell short (or talked themselves into abandoning this approach), they were supplanted by better services.

The old, good internet, in other words, was a place where enshittification had *consequences*. Competition, regulation, interoperability, and the moral sensibilities of tech workers all combined to keep tech honest, and to punish tech that wasn’t.

That’s what we need from our intermediaries: the discipline that comes from real consequences that arise when they wreck the things we use, rely on, and love.

The old, good internet was a place where people with a large dollop of technical knowledge, or a burning desire to acquire it, could meet with one another, conduct dialogues with one another, inspire and frustrate one another, sell things and buy things from one another, and take action together—without needing permission from a handful of tech giants.

The enshitternet that succeeded the old, good internet was also a place where people could do all those things, but only at the sufferance of unaccountable multinational tech firms that are largely or wholly insulated from any repercussions when they are malevolent, negligent, or just plain wrong. These firms grew steadily worse over time, abetting genocide and siding with fascists.

But the enshitternet had one key advantage over the old, good

internet: It was a lot easier to use! That meant that a lot of people joined, and many of those people improved the lives of those geeky early adopters with their presence. Those newcomers' lives were, in turn, improved by the community and fellowship of their geeky pals.

Lowering the barriers to entry for participation in digital life is an unalloyed good. "People who are good at using complicated technology" are—at best—a subset of "people whose ideas, support, companionship, and friendship you would value."

As a young aspiring writer growing up in Toronto, I was fascinated with a local character who went by Crad Kilodney. Kilodney wrote grotesque, dirty, funny short stories, which he edited and typeset himself, had privately printed, and then sold on street corners in the downtown core.

I would run into Kilodney all the time. In winter, when the sun sets in Toronto before five o'clock, I'd step out into a cold dusk after wasting a couple dollars' worth of quarters at one of the Yonge Street video arcades, and run into Kilodney wearing a tuque and gloves, and holding a hand-lettered sign with a phrase like SHABBY NO-NAME WRITER on it, along with a chapbook with a title like *Bloodsucking Monkeys from North Tonawanda*, *Suburban Chicken-Strangling Stories*, or *Putrid Scum*. (Kilodney had other signs as well. One simply read MARGARET ATWOOD. Atwood herself did a stunt for a Kilodney documentary in which she stood on one of Kilodney's habitual corners wearing a sign that read SHABBY NO-NAME WRITER.)

Kilodney was a lot of fun to talk to. He was a bitter, weird, middle-aged writer with a pipe who spent all day and night standing on busy streets, selling his books, and having strange dialogues with passersby. (He secretly recorded these dialogues and assembled the weirdest and most offensive clips into anthology cassettes, titled "On the Streets with Crad Kilodney," which he

also sold.) He made quite a name for himself as a gadfly and as a writer, and I can't be the only writer he inspired.

And yet I do not stand on street corners selling my books. I go through intermediaries: an agent, an editor, a publisher, distributors, booksellers, publicists. If my career imploded tomorrow and I absolutely *had to*, I might be able to pull off a Crad Kilodney: I'm pretty extroverted and I don't embarrass easily.

But the *vast* majority of writers I want to read would never, ever, *ever* do what Crad Kilodney did. Many are simply incapable of doing so. I'm glad that intermediaries exist who make it possible for all these other writers to participate in literature.

But.

Or, perhaps, *and*.

I'm glad that intermediaries exist who make it possible for all these other writers to participate in literature—*and* those writers' lives and my life as a writer will be better if the intermediaries who sit between us, the writers, and you, the readers, are powerful enough to get our books into your hands, but *not* so powerful that they can rip us off, or exercise a veto over what kind of literature is allowed to exist, or rip *you* off.

Which brings me to the *new*, good internet. The new, good internet is like the old, good internet, where lots of intermediaries exist that can help us focus on the business of conversing, arguing, mobilizing, romancing, transacting, buying, and selling. But it's also like the enshitternet in that it has all the ease of use that brought all our normie friends into the Web 2.0 world, so that *everyone* could come to the party.

Tech bosses howl with derision at this suggestion. They claim that the features of the enshitternet that make it easy to use are inseparable from the parts that make it easy for them to abuse us. To hear Mark Zuckerberg tell it, it's literally inconceivable that you might carry on a casual conversation with a friend or organize a

potluck dinner without being spied on by his platform, your data harvested and monetized for targeted ads. For Zuck, “friends without commercial surveillance” is like “water that’s not wet.”

Same goes for Google and search surveillance. Google claims that there’s no way to improve search results without monitoring your behavior, both to customize which items are prioritized and to monitor how you respond to those customizations. There’s some logic here: if a search engine knows what region you’re in, it might do better in answering a question like *When does Daylight Savings start?* But Google is palming a card here, conflating the marginal improvements it gets from using context to customize search results and data-mining responses to those customizations with the massive, pernicious, multifaceted program of commercial surveillance it carries out for ad targeting.

Apple gets in the game, too, claiming that there’s no way to deliver a convenient, safe, easy-to-use computing experience without giving its corporate executives a veto over which software you install, and without the company sucking 30 cents out of every dollar you spend on that platform.

Amazon claims that there’s no way to deliver a reliable logistics system to ship items to your home without letting the company cream 51 percent off all its sellers’ purchases; without unethically misclassifying its delivery drivers; without forcing its warehouse workers to piss in bottles and undergo injuries at up to three times the rate of its competitors; and without allowing counterfeits, scams, and dangerous products to overrun its platform.

Microsoft claims that there’s no way to deliver its Azure cloud computing platform without anticompetitively trapping Azure customers into using its Outlook email/calendar system and without locking them into using its cloud-based Office365 platform. It also claims that there’s no way to deliver Office365 without letting your boss count the number of keystrokes you make and produce

ranked lists of the most “productive” employees in your division based on this meaningless metric.

This trick—insisting there’s no possible arrangement of affairs apart from the current one, no matter how miserable it makes you—is literally neoliberalism’s oldest and cheapest rhetorical gimmick.

It’s a gimmick that starts with the former UK prime minister Margaret Thatcher, Britain’s answer to Ronald Reagan and Augusto Pinochet. Thatcher’s all-purpose maxim was “There is no alternative,” though perhaps *mantra* is more apt than *maxim*, as Thatcher repeated this so often that her supporters turned it into an acronym, TINA, and sometimes referred to her as “TINA Thatcher.”

TINA allowed Thatcher to paint her ideological choices as historical inevitabilities: *Sorry you’ve lost your job and your kids are hungry, but that’s just what the Great Forces of History have dictated must occur at this juncture. Alas, there is no alternative.*

“There is no alternative” *really* means “Stop trying to think of an alternative.” It’s a demand dressed up as an observation of truth. Its job is to extinguish your imagination and foreclose on the possibility of your even conceiving of another way of doing things.

“There is no alternative” also serves to insulate the individuals who built and profited from the Enshittocene from criticism. If they are merely conduits through which the inevitable outcome flows, then it would be unfair to hold them responsible (or liable) for the harms they enacted on their way to amassing their vast fortunes. (This is what Dan Davies, author of *The Unaccountability Machine*, calls an “accountability sink.”)

But of *course* there’s an alternative. We know there is! We know that you can use Facebook without being spied on because that’s how Facebook worked for *years*, back when the company was pitching itself as the anti-surveillance alternative to MySpace.

Not only was Facebook able to operate without spying during that era, but that was *also* the best era of Facebook, the time when Facebook served you a feed consisting of the things you asked to see, not boosted content and ads (that is, the things Facebook's shareholders *wished* you wanted to see).

Google Search can be great without spying, too. We know *that* because the 1998 PageRank paper in which Sergey Brin and Larry Page laid out their plan for a "large-scale hypertextual web search engine" declared that "advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers." Which is why, during Google's early years, the company did no commercial surveillance *and* served the best search results of its entire commercial life.

Apple can provide you a secure, reliable computing experience without telling you that you're not allowed to download a dictionary because it contains swear words, or that you're not allowed to download the Tumblr app because some Tumblr accounts post images that include nudity, or that you're not allowed to download an app that tracks civilian casualties of US drone strikes (all of which are apps that Apple rejected at one time or another on behalf of their billion-plus iPhone and iPad users around the world). There is nothing about operating a high-quality software store that requires Apple to scrape 30 cents out of every dollar earned by every software author.

We know that's true because *every product Apple sells*, except for its mobile devices, works this way. Your desktop Mac, Mac Mini, and Mac laptop all somehow manage to deliver reliable, desirable services without these requirements.

Can Microsoft offer an Office suite that doesn't spy on you and rank your typing speed for your boss? Can it deliver an Office suite that works with rival suites, rather than locking you in? Given that this is how Office worked until just a couple of years

ago, I think the answer here is a resounding yes. What's more, no bearded prophet ever came down off a mountaintop with two stone tablets reading "Yea, and thou shalt payeth a gigantic cash penalty shouldst thou attempt to use Office365 with a cloud provider other than Microsoft Azure." That's a choice Microsoft makes. It used to make a different choice. It could make another choice again.

A new, good internet is one that retains all the ease of use, the sensible defaults, and the simplified abstractions of the enshitter-net, but combines them with the technological self-determination of the old, good internet.

Apple wants you to think that the "elegance" of the iOS platform is a slippery gas, like hydrogen, and if the European Union forces it to add a checkbox that says, "Let me choose my own apps," all the elegance will escape out of that box. It's nonsense. If Apple's defaults are good, Apple customers will choose them.

But more important, if Apple's customers can choose to override the defaults and leave Apple's software store behind, it will provide a damned good motivation to Apple to make sure that its store is as good as possible.

When the tech giants insist that the final word on how you use the products and services they make should come from them, not you, they set the scene for a situation in which you don't use those products and services because you like them, but rather because you can't bear the cost of leaving.

A new, good internet is possible. More than that, it's *essential*.

# Antitrust Is Back, Baby

To halt the internet's enshittification and throw it into reverse, we need to restore the four forces that discipline technology firms, pressuring them to treat us well and tossing the products and services that fail to do so on the scrap heap of history.

Those four forces, again, are:

1. Competition
2. Regulation
3. Interoperability
4. Tech worker power.

After two generations of neglect and decline, *all* of these forces are surging today, but the most startling comeback story of all is in antitrust enforcement.

Recall that starting with the Carter administration and then accelerating through the Reagan revolution, each US presidency weakened antitrust, directing the Department of Justice, the Federal Trade Commission, and every other federal agency to ignore even the most blatant antitrust violations.

Forty years of failing to stop companies from forming and maintaining monopolies led to . . . monopolies. The result was every sector of the global economy looking like the tech industry, from cheerleading leagues and NASCAR to coffins and financial services.

Of course, if you ask the orthodox economists who oversaw this transformation about the monopolization of the economy, they'll insist that there's no way to dispositively connect the pro-monopoly policies they supported with the monopolies that resulted.

It's as though we used to put down rat poison, and we didn't have a rat problem. Then the millionaire economists convinced us to stop putting down the poison, and now the rats are gnawing our faces off and the economists are all saying, "Now, now, don't get *hysterical*, dears. There's no way to know if these rats have anything to do with our pro-rat policy prescriptions. Perhaps the great forces of history bore down on this moment to produce a surge in rat fecundity. Maybe this is just the Time of the Rat."

This used to work surprisingly well, but over the past decade, the manifest deficiencies of the "Who can say where the fuck these rats came from?" school of economics have weakened its grip on power, and a new, heterodox school of anti-monopoly economic thought has gained currency.

In the United States, this anti-monopoly movement is sometimes called *neo-Brandeisian*, after Louis Brandeis, who sat as a Supreme Court justice from 1916 to 1936, and whose career was dedicated to stamping out the "curse of bigness."

But anti-monopoly isn't wholly—or even primarily—a US phenomenon. In the European Union, the European Commission took up the cause, dusting off the kind of merger scrutiny and muscular enforcement that prevailed until the late 1970s, bringing major cases against (primarily US-based) tech giants and promulgating muscular new regulations such as the Digital Services Act and the Digital Markets Act, both of which entered into force in 2024.

Europeans are as alarmed by monopolistic control over their

economy as their American cousins, but they are far more likely to see action on Big Tech, thanks to the US origins of the tech cartel. US lawmakers are torn between their voters' concern over tech monopolization and their sense that these are American companies that act as a source of American soft power abroad and of national pride at home. That's why Donald Trump traveled to Davos in early 2025 to berate European regulators for bullying the poor, defenseless US tech giants.

Though Big Tech tries its damndest to present itself as European—or at least “Western,” as opposed to the sinister menace of Chinese Big Tech—no one really buys it. Nick Clegg, the former UK deputy prime minister who made millions as Meta's policy ambassador to the EU, can insist that Facebook's economic dominance is necessary to keep “European cyberspace” from being swallowed by the Chinese Communist Party all he likes, but the prevailing attitude in the EU is that Meta is an invader, not a protector.

The UK has been in political chaos since the Brexit vote (something Clegg can largely be blamed for, thanks to his decision to form a government with David Cameron's Conservative Party in 2010). It's true that elements of the British state are remarkably deferential to US tech giants. (See, for example, Prime Minister Keir Starmer's plan for virtually unlimited “AI data center” construction, without any planning permission, and without regard to the impact on the crumbling national power grid and water system.)

But even through fourteen years of business-friendly Conservative Party rule, the UK's competition regulator, the Competition and Markets Authority (CMA), has brought a series of major enforcement actions and anti-merger rulings. What's more, the CMA boasts the world's largest tech-focused division, the Digital Markets Unit (DMU), where seventy full-time engineers work

on deep, technical market studies and detailed, highly nuanced, and highly informed policy prescriptions.

The DMU was formed in 2021, with a governmental promise that it would get its own secondary legislation, giving it unique enforcement powers. That legislation repeatedly died “on the order paper” (without getting a vote because it didn’t make it onto the main agenda), though not due to any particular animus toward the DMU’s mission—rather, it was caught in the yearslong, post-Brexit swirl of chaos, leadership crises, and scandals.

At last in 2024, the Digital Markets, Competition and Consumers Act made it through Parliament, establishing broad enforcement powers for the DMU. But the DMU didn’t sit idle for the three years between its founding and its receiving of power; its engineering staff used the power of the CMU to compel responses from tech giants, combined with its own technical insight, to produce some of the best-researched, most complete, most *actionable* studies of some of tech’s worst markets, like ad tech and mobile devices.

These didn’t just sit on a shelf, either. While the UK trustbusters had a huge technical staff and a shortage of enforcement powers, the EU Commission had sweeping enforcement powers and a massive deficit of technical staff.

And it turns out that Big Tech commits the same sins wherever it operates. The EU picked up those DMU studies and used them as schematics for planning their own regulations and enforcement actions against tech giants.

Not just the EU, either. Many smaller countries have twigged to the fact that the tech giants have a single giant playbook, and the same facts and evidence used to convict a tech monopolist in the EU can be translated and recycled for enforcement cases all over the world.

That’s how South Korea and Japan were able to land cases

against Apple's App Store monopoly. It's true that Apple and Google are larger than most governments, but it's also true that once *any* government cracks open a tech giant, all the other governments can get in on the action.

The UK's CMA played an important convening role in this global effort, hosting annual tech antitrust events in London attended by the top competition regulators—and their technical staff—from around the world. These events are partly private, government-to-government affairs, and partly open to the public with outside speakers. (I've had the pleasure of being one of those speakers.)

All over the world, governments are getting the antitrust bug, even if they don't always get it right. Australia decided to tackle Big Tech's predation on the news industry with a "bargaining code" that forced tech companies to pay fees for linking to news stories and indexing them for search. The coalition that supported this included both Rupert Murdoch's own monopolistic, low-quality newspapers and the struggling community papers he's spent years destroying. This was a coalition with something for everyone—whether you're the kind of pro-business politician who adores Murdoch or a crunchy progressive who wants the local paper to survive.

The problem with this approach is that it completely misconstrues the nature of tech's exploitation of news, and treats tech as the solution to the news's problem, rather than the cause.

When Google indexes the news and makes it easier to find, that's *good* for the news. When Facebook provides a forum to discuss the news, that's also *good* for the news. News you can't find and aren't allowed to talk about isn't news—that's a *secret*.

But if Big Tech companies aren't stealing *content* from the news, what *are* they stealing? That's easy: they are stealing *money* from the news. If you're a news provider and your subscribers

use an app to pay you, Apple and Google steal 30 percent of every dollar you bring in. If you rely on advertising, Meta and Google steal 51 percent of every dollar the advertising generates. If you expect to reach your own subscribers on platforms they have explicitly instructed to deliver your feeds, you will have to pay Meta, Twitter, or TikTok to “boost” your content so it actually shows up in the feeds whose users asked to have it there.

Australia missed an opportunity with its bargaining code. The country *could* have targeted tech’s cash rip-offs, but instead, it made the media *dependent* on tech. Tech companies still get to steal from the media, but Australia makes them give some of that money back. Not only is this a very weird way to bring tech to justice, but it also stops working if we ever *do* cut tech down to size. Rather than watchdogging every corrupt act of the tech sector, the news media’s survival now depends on the tech sector staying *as large as possible*.

This approach is not only misguided but also self-defeating. When you tell a tech giant that it’s going to have to pay to allow discussions of the news, or to index the news, the tech giant’s next move is pretty straightforward: it just blocks links to the news, and makes the news disappear for everyone who relies on its services.

That’s what happened in my native Canada, where in 2023 the Trudeau government implemented its own version of the Australian solution. Meta promptly banned links to the news from all of its platforms in Canada, causing chaos when wildfires tore through the north in 2024 and Canadians were cut off from timely news reports about evacuation orders and logistics. Trudeau’s Liberal Party narrowly avoided a stinging electoral defeat in 2025, despite projections for an overwhelming victory by a far-right conspiracist named Pierre Poilievre, a man whose fol-

lowers get all their news from far-right influencers on sites devoid of even a residual hint of actual news thanks to Meta's ban on news sources. Donald Trump's incontinent demands for Canada to become "the fifty-first state" sank Poilievre's electoral fortunes, but his base remains strong on Facebook, where authoritarian influencers rule the roost and actual news is banned.

But the news from Canada isn't all bad. For most of Canadian history, the Competition Bureau, charged with preventing monopolization of the economy, has been extraordinarily ineffectual. In its entire history, the Competition Bureau has challenged only *three* mergers, and it has prevented *zero* mergers. At last, in 2024, Canada passed a bipartisan law that completely overhauled its Competition Act, with sweeping new powers granted to the bureau. Sure, it took more than a century, but Canada finally has an anti-monopoly cop on the beat.

Antitrust fervor is sweeping governments all over the world, even China, where the New Measures for Cybersecurity Review, issued in 2022, ban tech giants from blocking new companies by breaking interoperability. Contrary to the scaremongering of Meta shills like Nick Clegg, the Chinese government has no particular love of its tech giants. Xi Jinping clearly views these companies as *competitors* of the Chinese state, not as a convenient way of projecting Chinese soft power abroad. This explains why Xi keeps throwing their CEOs in gulags.

Putting *anyone* in a gulag is wrong, of course, but the fact that tech bosses are on Xi's shit list really undermines Meta and Nick Clegg's yellow peril-inflected argument that Chinese Big Tech is a stalking horse for the Chinese Communist Party (and that argument's corollary: that Meta is the main force keeping "European cyberspace" free from nefarious Chinese rule). This is nonsense, but it's productive nonsense. It gave us the TikTok ban,

and it's giving America's bloated, overcapitalized AI giants political cover as they attack nimbler Chinese rivals like DeepSeek.

Antitrust is global, but it's especially powerful in the United States, thanks to a mix of both government and private action. While I was writing this book, Google lost *three* antitrust cases, one brought privately by Epic Systems, the others brought by the DOJ. Having thrice been adjudicated a monopolist by a federal judge, Google has now been ordered to open up its app store and begin distributing rival app stores *as apps*, so you can switch from getting your apps from Google to getting your apps from anyone else, just by installing an app using the software Google included with your Android device.

That's just the appetizer. The main course will come when the court hands down a remedy in the DOJ antitrust case, where the DOJ has asked for Google to be broken up (spinning off Chrome to a separate company), and when the court orders Google to stop looking at the private data that gives it an edge on Search queries.

And there's another federal case against Google that wrapped up in the last days of this book's editorial process with a rout for Google. It concerned Google's dominance of the advertising market, and now that the DOJ has prevailed, the most likely remedy will be more breaking up of Google, forcing the company to sell off the different parts of its advertising stack.

Biden's trustbusters didn't win every case. A case against Apple for the abuses of its App Store failed, as did the FTC's suit to halt the Microsoft/Activision Blizzard merger. That's to be expected: federal judges are sitting atop forty years of hard-bought pro-monopoly precedent. Four in ten federal judges attended one of the Manne seminars, the lavish, billionaire-backed "continuing education" junkets where judges were propagandized by pro-monopoly economists. These seminars paid off handsomely,

with judges measurably shifting to a pro-monopoly stance in their decisions after their retraining.\*

But for a while there, the direction of travel was *great*. In July 2021, the Biden White House released its Executive Order on Promoting Competition in the American Economy, written by Tim Wu, then installed as the special assistant to the president for technology and competition policy. (Fun fact: Tim and I also went to elementary school together and have known each other since I was nine and he was eight!) The order lists seventy-two pro-competition actions that various federal agencies, from the Department of Transportation to Commerce to Health and Human Services, could take *right away*, without any further action from Congress.

The Biden admin proceeded to use that as a punch list, executing every item on it in order. Agency heads who dragged their feet—like Secretary of Transportation Pete Buttigieg, who presided over a series of catastrophic aviation and rail IT failures—were given assistance. (In Buttigieg’s case, this was Jen Howard, Lina Khan’s FTC chief of staff, who was parachuted into the DOT as its new head of competition, whereupon the DOT became a powerhouse of pro-competitive activity.)

The agencies in Biden’s administration showed remarkable technical skill and creativity in crafting and enacting new policies. One shining example was the Consumer Finance Protection Bureau (CFPB), whose chief, Rohit Chopra, previously worked at the FTC alongside Khan. As boss of the CFPB, Chopra surrounded himself with skilled, principled technologists who were a wellspring of excellent, actionable ideas that hacked away at the power and profits of monopoly abusers.

\* See Elliott Ash, Daniel L. Chen, and Suresh Naidu, “Ideas Have Consequences: The Impact of Law and Economics on American Justice,” NBER Working Paper 29788 (February 2022).

Take financial comparison shopping sites. You might well have entered your financial details into one of these sites, looking for an impartial recommendation. What you probably didn't know was that the recommendations these sites produced weren't based on the bank that would cost you the least and pay you the most interest—they were based on which bank paid the biggest bribe to be at the top of the list.

The CFPB ordered a stop to this—and went further. It used its power to compel truthful disclosures from banks to force them to supply up-to-date, machine-readable rate cards enumerating all their rates, fees, and penalties. These are being fed into a “public option” comparison shopping site that the CFPB itself would operate, giving you a true, current, reliable picture of which bank is your best bet.

Here's where things got *really* cool: The same CFPB rule orders the banks to build account migration tools that allow you to instantly export *all* your financial data (all your transaction histories, your payees, etc.) to a new institution with a single click. What's more, you can use all that data from your bank to power a search at a comparison shopping site.

So under this rule, you'd be able to export your account history to a CFPB-operated comparison shopping site with one click, and that site would use the data to see which bank would charge you the least for the services you use and pay you the most for the money you deposit (and the site wouldn't share that data or use it for any other purpose). Then one more click would transfer your account to the best bank in the country for you.

At the time of writing, the Trump administration has mothballed the CFPB, amid numerous legal challenges. However, shutting down the CFPB doesn't necessarily halt enforcement of

CFPB rules, because every state attorney general in the United States is empowered to enforce those rules. As is the case with so much occurring in the early days of the second Trump administration, the future of this rule is hard to determine.

Look, I'm not one of those Milton Friedman-pilled weirdos who thinks that markets and competition will solve all our problems, but the two most important critiques of market-driven policy are these:

1. Market participants have imperfect knowledge, which stops them from making the best transactions.
2. Transactions are high-friction, so even if you can get a better deal somewhere else (and therefore increase the success of the companies with the best deals and punish their inferior competitors), you might just sit pat and accept a worse offer from a company you're already doing business with because changing is a giant pain in the ass.

By using its statutory authority to compel full and truthful disclosures, and combining that with open standards for interoperability, the CFPB set up a situation in which Americans should have access to timely, accurate, and complete information about banks that will automatically produce recommendations they can take advantage of with just a few clicks.

Multiply that by every federal agency, each of which has been charged with combing through its authority and conducting investigations, imposing punishments, and making rules.

Of course, Biden's executive order on competition came at the start of his term, before the Supreme Court upended much of the settled law that Biden's skilled technocrats were counting on. For the purposes of this discussion, the most consequential Su-

preme Court decision is the outcome of a 2024 case called *Loper Bright Enterprises v. Raimondo* (which I mentioned in the footnote on page 108).

The *Loper Bright* decision killed something called *Chevron* deference, named after a 1984 case that gave federal agencies broad latitude to make regulations that affected the whole sector they oversaw. For example, *Chevron* deference meant that Congress could tell the Environmental Protection Agency, “Just make sure our air and water aren’t too poisonous for us to breathe and drink, okay?” and EPA could investigate business practices, smokestack emissions, and effluent discharge, and tell companies what they could—and couldn’t—emit.

After *Loper*, federal judges are supposed to weigh these regulations and decide whether they involve “major questions.” If they do, the judges can say, “Well, if the agency wants to make a rule like this, it’ll have to wait for Congress to pass a law giving them the specific power to do this.”

Killing *Chevron* deference makes the jobs of American regulators a *lot* harder and makes it a lot easier for corporations to cheat us, steal from us, poison us, maim us, and kill us. But the death of *Chevron* deference isn’t the end of regulation, for two reasons.

First, judges don’t *have* to send every major question back to Congress. Some regulations—even big ones—will survive judicial scrutiny and stand.

Second, and more important, though: *Chevron* deference applies to *regulations*, but not to “conduct remedies.” If a company is convicted of violating the law—for example, Section 5 of the FTC Act, which bans companies from engaging in “unfair and deceptive methods of competition”—then the regulator gets to impose a special rule just for that company. Like, if Facebook violates its users’ privacy, the FTC could create a conduct rem-

edy that strictly limited Facebook's ability to gather, retain, and analyze its users' data.

Now, it would be a big lift for the FTC or some other agency to catch hundreds of companies doing something rotten and make rules for each of them. But one silver lining to the monopolization of so many sectors is that a very small number of very large companies are responsible for nearly all of the corporate abuses in the sectors they dominate.

There's not much to like about the cartelization and monopolization of our economy, but at least antitrust regulators all over the world face the same global monopolists (and so can recycle one another's legal cases), and at least each sector is dominated by just a handful of companies that can be tractably, individually brought to justice.

## Antitrust Under Trump

Even for campaigners who'd worked on this issue for years, the Biden administration's antitrust renaissance was a surprise. The political deal struck between Biden and the Elizabeth Warren/Bernie Sanders wing of the Democratic Party led to the appointment of some of the most creative, competent, and principled antitrust enforcers in living memory, and from the moment they assumed office, they undertook a flurry of regulations, investigations, court cases, and rulemakings. This was aided in part by a wing of the MAGA movement that promoted antitrust as part of a "populist" agenda.

No one was more synonymous with this antitrust surge than Lina Khan, Biden's FTC chair.

In 2017, a *Yale Law Journal* paper titled "Amazon's Antitrust Paradox" leaped out of obscure legal circles and into the public eye. This is not normal. Law review articles are barely interesting to *lawyers*, let alone the broader public. What's more, this wasn't just *any* law review article; it was a law review article about *antitrust*, one of the dustiest, least-regarded, most abstract, and frankly most irrelevant areas of law, dominated by dull, mathematical models created by and for extremely specialized economists.

The article's author was a third-year Yale law student named Lina Khan. Four years later, Khan was the youngest-ever chair of

the US Federal Trade Commission, the most powerful consumer regulator in the world.

Khan is an extraordinary figure. Charismatic and quick-witted, she has a knack for cutting through the professional obfuscation that kept antitrust out of the public eye and connecting antitrust policy to bread-and-butter issues, like who you work for, what kind of health care you get, and how much you pay for eggs.

Khan's Senate confirmation was seismic. Twenty-two Republicans broke with their party to vote for her. While some of those Republicans have since turned on her, she remains popular with the party's leading faction—JD Vance called her “one of the few people in the Biden administration that I think is doing a pretty good job.”

Senate observers were shaken by her approval. According to *Bloomberg's* Josh Eidelson and Max Chafkin, when Senator Amy Klobuchar “blurted out” that Khan was going to be FTC chair, “Amazon officials assumed it was a joke.” They didn't laugh for long. Khan sued Amazon in 2023, and the case survived the company's initial motions to dismiss, including a motion to force Khan to recuse herself on the grounds that she had written a groundbreaking paper about Amazon and that made her “biased.” In other words, only FTC chairs who *aren't* experts on the problems with Amazon should be allowed to bring a case against it.

Khan made a lot of enemies. During the 2024 election, billionaire Democratic Party donors like Mark Cuban and Reid Hoffman called for Kamala Harris to eject her should Harris win the presidency. They were in company with megadonor billionaires like Barry Diller, Vinod Khosla, Chamath Palihapitiya, Joe Lonsdale, and Peter Thiel. Though they may back opposite parties,

they all share a common factor: every one of them stood to lose millions—perhaps hundreds of millions—from the enforcement actions and merger scrutiny that Khan and the FTC have brought against companies they are involved with.

In the first three years of Khan's term as FTC chair, *The Wall Street Journal* ran more than one hundred op-eds condemning her. While the *Journal* found a lot of reasons to hate Khan (for example, accusing her of a conflict of interest—opposing monopolies—that disqualified her from prosecuting monopolies), the common thread running through them is that Khan was technically incompetent, someone who wasted public funds while getting nothing done.

It's nonsense. Under Khan's leadership, the FTC did more in four years than it had in the previous forty. Companies like Nvidia, Lockheed Martin, HCA Healthcare, Sanofi, and Illumina all abandoned mergers after her office challenged them. What's more, the billionaires in her haters' club even (especially) admit that far more mergers are simply being killed before they can be announced, because the parties involved don't want to risk a bruising and expensive fight with the FTC. As Khan frequently pointed out in interviews, the point of any law enforcement is *deterrence*, and under Khan, the entire mood in American business has shifted. As one venture capitalist told me, "It used to be that we would plan the whole merger and *then* ask the lawyers about the FTC. Now we don't do anything until the lawyers have had a chance to explore the FTC's likely position on a merger." More often than not, those lawyers are recommending that the companies don't even try.

This was especially true with regard to Big Tech. In 2024, Google made the largest-ever acquisition offer for a startup in world tech history, when it bid \$24 billion for Wiz, an information security company. Wiz turned the offer down flat, something in-

siders attributed to fears of a lengthy merger scrutiny process with the FTC. Rather than being folded into Google, Wiz would have to become a stand-alone business whose services would be available to Google and its competitors. Of course, once Trump was elected, Google and Wiz announced that the merger was back on.

On the eve of Trump's 2025 inauguration, the FTC had litigation pending against Amazon and Meta. It had punished Rite-Aid for subjecting customers to nonconsensual facial recognition, and gotten refunds for the Fortnite players who were ripped off by Epic's sleazy in-game marketplaces. Khan and her counterpart at the DOJ's Antitrust Division, Jonathan Kanter, produced a new set of merger guidelines that explicitly address the labor and privacy issues that arise from corporate mergers.

Not every one of Khan's cases succeeded, but that's because she took *very* big swings. As Tim Wu told *Bloomberg's* Eidelson and Chafkin, the FTC used to be "a very hardworking agency that did nothing." (Wu worked for the FTC during this period.) For four years, under Biden, the FTC got stuff *done*.

What's even more amazing, all of this was happening because *the people* wanted it. There's no giant corporate dark-money fire-hose that's secretly pushing to get the government to take action on corporate concentration. There's no super PAC funding attack ads about out-of-control mergers. Even the media outlets that cover the subject most ardently are owned by the kinds of businesses that trustbusters want to smash—a fact that John Oliver is never shy about mentioning when he covers monopolies on his excellent program *Last Week Tonight*, which is produced by Discovery/Warner.

Which is to say, monopolies actually *make money* from anti-monopoly media! John Oliver's wildly successful show is a money-spinner for Discovery/Warner.

There are a million stories like this in late-stage America: People whose pets are killed by private equity–owned pet groomers, whose minimum-wage employees are locked in to contracts that force them to pay thousands of dollars if they quit or get fired. Or people whose *grandparents* are killed by private equity–owned nursing homes whose employees are put on thirty-six-hour shifts and threatened with *criminal abandonment charges* if they quit.

People in the United States and all over the world have figured out that there is something rotten going on with corporate power. A genuine, spontaneous groundswell of popular rage at the enshittification of *everything* is all around us. Lina Khan is an extraordinary leader, a person who can articulate the legal and economic basis for that rage in language that the general public can grasp.

But as brilliant as Lina Khan is, she was also just filling a Lina Khan–shaped hole that inexorably occurs at moments like these. America’s billionaires fixated on her because she was good at her job; because she had a high profile; and, let’s face it, because she’s young, female, and not white.

Khan didn’t survive the Trump transition. Neither did her DOJ counterpart, Jonathan Kanter, or Rohit Chopra, head of the CFPB. Indeed, while I was doing final edits on this book Elon Musk’s DOGE unilaterally shuttered the CFPB.

This year, 2025, is the year that the Empire struck back. By the end of January, the head of the UK Competition and Markets Bureau had been fired by Keir Starmer’s Labour government and replaced with Doug Gurr, the former head of Amazon UK. In the United States, at the 2025 inauguration, Trump spoke from within a decorative semicircle of tech billionaires: Meta CEO Mark Zuckerberg, former Amazon CEO Jeff Bezos, Google CEO

Sundar Pichai, Apple CEO Tim Cook, TikTok CEO Shou Zi Chew, and, of course, Elon Musk.

These men intervened in many ways on Trump's behalf. Bezos ordered the editorial board at *The Washington Post* (which he owns) not to endorse Kamala Harris. Cook personally donated \$1 million to Trump's inauguration. Both TikTok and Twitter changed their algorithms to favor Trump-oriented news in the run-up to the election.

Within days of assuming office, Trump illegally fired the head of the National Labor Relations Board. His FTC chair, Andrew Ferguson, claimed that he would devote his energies to fighting Big Tech. But Ferguson's day-one agenda involved killing ongoing enforcement actions to stop predatory pricing (selling goods below cost to prevent competitors from entering a market) and surveillance pricing (using commercial surveillance data to adjust prices based on your estimation of how much you can squeeze them for). In their place, Ferguson shifted the FTC's whole focus to rooting out "wokeness." As the FTC commissioner Alvaro Bedoya wrote in his dissent:

Andrew Ferguson could have made his first public act as Chairman a motion to study the rising cost of groceries. He could have acted on a pending public petition from a group of wall and ceiling contractors to investigate how lawbreaking contractors can effectively rig contract competitions in the commercial construction industry. He could have moved to investigate a pending public petition from shrimpers from Louisiana, Mississippi, and Alabama to investigate potentially false and misleading claims about shrimp imports from India that are farmed with forced labor and shot full of antibiotics.

Chairman Ferguson could have done any number of things to actually lower the cost of living and create opportunities for American businesses and workers. He did none of them. Instead, he cancelled “DEI” . . .

I have met with corn growers and cattlemen in Iowa. I have met with shrimpers in Biloxi. I have met with pharmacists in Knoxville, grocers in Tulsa, and patients and their doctors in Charleston, West Virginia. I met with the men who build Miami’s million-dollar skyscrapers in 110-degree heat.

Let me tell you what they didn’t talk about: “DEI.”

What they *do* talk about is how powerful companies are skirting or abusing the law to force farmers, workers, and small businessmen to do what they want, when they want, or else. How the government isn’t doing anything about it. And how they’re going broke because of it.

But Chairman Ferguson seems uninterested in the challenges that regular human beings face.

Commissioners Alvaro Bedoya and Rebecca Slaughter were illegally fired by Trump shortly after Bedoya published those comments. Both Bedoya and Slaughter maintain (correctly) that they are still sitting FTC commissioners because Trump does not have the power to fire them, and while they challenge Trump in court, they are continuing to do their jobs as best they can, though they are locked out of their offices and email accounts.

When Trump bellowed his support for US tech giants at Davos, it doubtless lifted the spirits of those in Google’s C-suite, who are currently facing a breakup after losing an antitrust case brought by Biden’s DOJ. But Trump’s DOJ told the judge that they agree with the Biden DOJ’s proposed punishments for the monopoly that Google was convicted of establishing and maintaining.

All of this is pretty grim. The backlash to the techlash has been swift and demoralizing.

At times like this, it's important to remember where the antitrust revolution came from. The brilliant public officials who prosecuted that revolution under Biden were the *effect*, not the *cause*. Like I said, there's no billionaire dark-money organization that backed antitrust. Biden's own political legacy is firmly pro-big business. The Democratic Party is no friend to working people, and has voted time and again for policies that made the rich richer and big corporations bigger, at the expense of working people.

The reason Biden's Democratic administration backed a generationally significant antitrust agenda is that *the people demanded it*. You. Me. Us. We were pissed off enough, and loud enough, about corporate abuse that a party and a politician with a long history of doing nothing (or worse than nothing) on these issues finally *did something*. This is even more remarkable than it sounds, because the academic research on this is clear: the US government almost *never* acts on the policy preferences of working people, when those preferences conflict with the desires of the rich.

Something extraordinary happened in 2020–2024. It's still happening. Getting rid of the agencies that turned our demands into law doesn't make those demands go away. Not hardly.

## Bringing Back Regulation

When the companies within a sector become larger and more concentrated, they don't just stop competing with one another for customers and workers—they also stop competing with one another for regulatory outcomes.

Take net neutrality, the idea that your ISP should deliver the bits you request as quickly and reliably as it can.\* (This is just a restatement of the end-to-end principle we learned about on page 65.) Net neutrality is such an obviously good idea that it's very weird we even fight about it. Imagine if Uber decided not to provide “pizzeria neutrality,” and so when you paged an Uber to take you to a beloved family-owned pizzeria, the car took an extra ten minutes to arrive and then took a roundabout route that tacked another twenty minutes onto the journey. But Domino's could pay for “priority service,” meaning that if you booked an Uber to the local Domino's, you'd get picked up as quickly as possible and taken there by the most direct route.

Put that way, it's obvious that the job of an intermediary should be to deliver the things you want, not the things that they wish you wanted (because someone would pay them extra to connect to you). Platforms—whether Uber, eBay, Google Search,

\* Net neutrality was the de facto policy for US ISPs for most of the internet's history, and was formalized as an FCC regulation under Obama. Trump's FCC rescinded it in his first term. Biden's FCC restored it, but Trump-appointed judges nullified that order. Net neutrality is still the law of the land in much of the world, including the EU.

or AT&T fiber—should be in the business of connecting willing users to willing publishers or sellers in the way that most accurately matches wants and offerings. They shouldn't thumb the scales (or smash down their fists on them) in favor of their own interests.

Given that this is obvious, how is it that regulators have such a hard time getting it right? Well, in the case of the FCC, the problem is threefold:

1. *The revolving door.* The overwhelming majority of industry execs who rotate into public service are henhouse-guarding foxes willing to help their former employers at public expense. This was especially true of Ajit Pai, the Verizon lawyer whom Donald Trump put in charge of the FCC during his first term. Pai took office having vowed to destroy the FCC's net neutrality rule and proceeded to do just that, by the sleaziest means imaginable. For example, when Pai received over a million identical anti-net neutrality emails with bogus @pornhub.com addresses, he had them entered into the record as real public comments opposing net neutrality. He did the same for 8.5 million more obviously fake messages whose return addresses were drawn from giant identity-theft datasets, treating comments from dead people, imaginary people, and sitting US senators who were on record as *supporting* net neutrality as *opposing* it. (These emails were sent by sleazy contractors working for the big ISPs, which subsequently settled legal action brought against them in the Southern District of New York.)
2. *The assault on the administrative state.* The American business lobby has spent decades neutering the expert agencies that oversee industry, an effort that relies on Republican

presidents making lifetime appointments of Federalist Society judges who believe that the agencies should do effectively *nothing*. This far-reaching takeover of the judiciary puts severe limits on the FCC's ability to regulate ISPs. In 2024, a court struck down an order passed by Biden's FCC. As I write this, Trump's FCC is taking a wrecking ball to the few FCC policies that protect the public from predatory, monopolistic conduct.

3. *The misuse of public comments.* For the FCC to do *anything*, it must first solicit multiple rounds of public comments. The Administrative Procedure Act, in force since 1946, says that expert agencies can act only after building up an evidentiary record in support of their policies. That's why Ajit Pai was so interested in getting all those millions of fraudulent anti-net neutrality comments into the record, because they justified his actions to get rid of net neutrality. This kind of evidence-gathering is fundamentally incompatible with market concentration.

Nearly all of the telecommunications in the United States are in the hands of a few gigantic companies that largely don't compete with one another. (Cable operators and phone companies have divided the country into exclusive, non-overlapping territories.) If these companies competed head-to-head, you'd expect some of them to support net neutrality. After all, if your biggest competitor's policy is "We slow down delivery of the stuff you want to see," then *your* policy could be "We give you the stuff you ask for, as quickly and reliably as we can." Sure, forgoing bribes for "premium carriage" from the biggest websites would cost you some revenue, but you could make it up by poaching your rivals' customers.

But because these companies only incidentally compete with

one another, it's easy for them to all maintain the same, anti-net neutrality policies. They don't need to poach one another's customers; indeed, they *can't*, because you can only supply internet to customers in your exclusive territory. Shriveled of any competitive risk, each company can offer a product that is materially, obviously defective, and still sell it.

This means that when the FCC opens a docket seeking comment on a net neutrality rule, every large ISP in the country files nearly identical comments, and the only contradictory evidence comes from tiny, one-town ISPs, along with academics, hobbyists, civil society groups, and so on. In their reply comments, the big ISP cartel just writes something like “We provide internet service to tens of millions of people, while these jerks have got a couple hundred (or maybe thousand) households on their books. They cannot credibly comment on whether it is technically feasible to offer a neutral internet. Only we can do that, and we say it isn't, so let us go on charging rent to the services that our customers want to reach.”

These three factors all play into one another. The most credible reason for hiring FCC commissioners from the C-suite of the major telcos and cable operators is that US telcos and cable operators are so gigantic and insular that only industry insiders can hope to understand them well enough to regulate them.

Meanwhile, monopoly produces the excess profits that the telecoms cartel flushes into the Federalist Society and the constellation of dark money groups that have stacked the federal judiciary with judges who think it should be illegal for regulators to regulate.

Finally, the fact that telecoms are so concentrated starves the federal record of credible comments from tier-one companies that support net neutrality.

While that's all admittedly a little depressing, there's also a bright side to it: the more we de-monopolize telecoms, the more legible the resulting, smaller companies become to regulators, which puts paid to the argument that only insiders are capable of regulating the industry.

Also, the more we de-monopolize telecoms, the more the individual firms will have to compete, which means that prices will come down for subscribers, which means that the profit that the sector has available to piss away on grand, corrupting schemes will also evaporate.

Finally, once there's competition in telecoms, companies will start debunking one another's claims in FCC dockets. A telecoms sector with a couple hundred small and medium-sized companies won't be able to maintain the message discipline that comes naturally to the small handful of companies that have captured the US market. When one company says, "It's technically impossible to offer a neutral internet connection," a rival will slide into the docket with reply comments: "What nonsense! We do it, and here are our server logs, cash books, and customer testimonials to prove it!"

Monopoly is a flywheel: Big companies subvert politics, paving the way for corrupt practices and anticompetitive mergers. This lets the companies grow, as does their corrupting influence, which paves the way for greater profits, more growth, and still more corruption.

Anti-monopoly is a flywheel, too: competition-enhancing regulation reduces profits and clears space for new companies that pose an innovative threat to the big incumbents, which must spend their competition-eroded profits to compete. This leaves big companies with less money, and thus less power, making it easier to pass even more muscular regulation. As a sector grows

more competitive and less cozy, the companies in it start to police one another's lies and cheating in public and before regulators.

As the anti-monopoly movement gains ground all over the world, this new flywheel is gaining momentum—without any big corporate donors, all thanks to people like you and me, who create the political will for big, ambitious regulatory adventures.

## Privacy First

My friend James Boyle says that before the term *ecology* came along, there were a bunch of people who cared about issues but didn't think of themselves as being in the same fight.

Say you care about endangered owls and I care about the ozone layer—are we fighting the same fight? Like, what do your charismatic nocturnal avians have to do with my worries about the gaseous composition of the upper atmosphere?

The term *ecology* turned all those issues into a *movement*, pulling many different kinds of people with many different concerns into a broad coalition that could get more done together than they could ever do on their own.

It's hard to overstate how important coalitions are to political struggle. Broadly speaking, if there's a group of people who've been trying to change something for a long time, it's *possible* that they just need to think up some cool new tactic and that'll finally get things moving. But it's far more likely that they just aren't powerful enough to make the change they're seeking.

Whenever you see a big, sudden political change—for better or for worse—you're usually witnessing the result of a new coalition. And, luckily for all of us, there's a new coalition forming around the privacy vacuum in US law—a vacuum that owes its existence to the lobbying might of the heavily concentrated industries that benefit from unregulated commercial surveillance.

Recall that Congress hasn't bestirred itself to update federal consumer privacy law since 1988, when it made it illegal to leak your VHS rental history. This inaction—expensively procured by the commercial surveillance industry—has hurt a *lot* of groups. Many of those groups are starting to recognize that while they are all concerned with very different *effects*, those effects have a common *cause*: the failure of Congress to protect Americans' privacy.

For example:

- Maybe you think that Facebook used commercial surveillance to build a kind of Big Data mind-control ray to sell your nephew fidget spinners, only to have evil conservative billionaires hijack it and use it to turn your grumpy into a conspiracy-addled QAnon follower.
- Or maybe you think Instagram turned your teenager anorexic.
- Or that TikTok brainwashed a bunch of millennials into quoting Osama bin Laden.
- Or maybe you're worried about Black Lives Matter protesters whose identities were swept up by Google's constant location-based surveillance and who were then reported to law enforcement after a "reverse warrant."
- Or maybe that doesn't worry you, but you are pissed about the same thing happening to the January 6 rioters.
- Or you're angry that people of color are being discriminated against by algorithms that determine hiring, lending, and housing based on surveillance data.
- Or that you or someone you love is being targeted by an online scammer, an identity thief, a ransomware creep, or some other criminal who got into your or your loved one's

bank account with the help of surveillance data that was either sold or leaked.

- Or that someone is using AI to make deepfake porn of you.

I think you'd be hard-pressed to find anyone who agrees that all of these issues are problems; I personally think that some of them are actually imaginary. But that doesn't have to matter when it comes to coalition-building. I don't have to agree with you that TikTok is brainwashing millennials to agree with you that a muscular privacy law would be a good thing.

Which is why we are seeing a procession of ever-improving privacy bills being introduced in Congress, each with more support than the last.

Surprisingly, Big Tech and other commercial surveillance firms sometimes get dragged into endorsing these privacy bills (usually when they're in the midst of some genuinely ghastly scandal). They can support privacy bills in a pinch, because they've figured out Two Weird Tricks for sabotaging consumer privacy law.

The first Weird Trick is making sure that a new privacy law doesn't get enforced. The way to do this is to limit enforcement to government prosecutors: district attorneys, attorneys general, and federal regulators. Historically, tech companies have found it easy to intimidate, buy off, or otherwise placate these officials.

That's why privacy advocates want a privacy law with a *private right of action*. That means that private persons—you and me—will be able to bring privacy claims, even if our supposed defenders in government don't seem to think we deserve to have our privacy defended.

The business lobby hates private rights of action wherever they appear. For corporate America, the ideal situation is one in

which everyone who might sue them either signs away the right to do so (through a binding arbitration waiver) or has that right taken away (through a law without a private right of action). For decades, American businesses have fought to be above the law, pushing disinformation. Remember the woman who spilled her McDonald's coffee on her lap and was awarded millions of dollars by a jury? The story was often held up as an example of a frivolous lawsuit. In reality, the woman received third-degree burns and had to undergo debridement and skin grafts. McDonald's had been repeatedly ordered to fix the temperature of its coffee, due to other burn cases, and nearly all the money the woman was awarded was clawed back by the court. Every time you hear about an "ambulance chaser" or a greedy "no win/no fee lawyer," you're being propagandized as part of a massive, long-running campaign to make corporations literally above the law.

No surprise, then, that even when privacy laws are introduced with private rights of action, these clauses are made so hugely controversial by lobbyists that they stall out in the legislature.

Now, Capitol Hill isn't the only place where Americans can ask lawmakers to protect them. While Congress has slept on privacy law, state legislatures have taken up some of the slack. That's where the second Weird Trick comes in.

Laws like Illinois's Biometric Information Privacy Act and the California Consumer Privacy Act have dragged privacy law into the twenty-first century, at least for people in Illinois and California. Californians have a broad right not to have their online and offline activities tracked, and Illinoisans' biometric data can't be captured or used without their meaningful opt-in consent.

Obviously, this is a problem for the commercial surveillance industry, but what kind of problem is it? *I* think the problem is that it forces these companies to stop spying on those of us lucky

enough to live in states that have privacy laws. *They* think (or claim to think) the problem is that there's a "patchwork" of laws that are too hard to comply with.

Surveillance industry lobbyists use this pretense to lobby for something called *preemption* in proposed federal privacy laws. If they get their way, any new federal privacy law will preempt (annul) all the state privacy laws. Federal privacy law will represent the most privacy we're allowed to have, rather than the baseline of privacy we're all guaranteed.

Naturally, privacy advocates aren't having any of this. Again, preemption has become a deal-breaking controversy when privacy bills are debated in the House and Senate.

Private rights of action and preemption are the trip wires that keep tangling up new privacy laws, but each law gets a little closer to passing with a private right of action intact and without a preemption clause. A new privacy law isn't a foregone conclusion, but it's closer than it's been since *Die Hard* was still in theaters.

## The EU's Digital Markets Act and Digital Services Act

Earlier in my career, I served for some years as the European director for the Electronic Frontier Foundation, splitting my time among London, Brussels, and Geneva (along with a lot of side quests, totaling thirty-one countries in three years). Based on my experience then and since, I can confidently state that the European Parliament is no less corruptible than the US government.

But just because the two are both susceptible to corruption, it doesn't follow that the European Union will experience the same *type* of corruption as the United States. In particular, the EU is far more willing to take on Big Tech than the United States is.

There's an obvious reason for this: the United States views the multinational tech firms that were founded in Silicon Valley and Seattle as *American* companies, and they are, in several important ways. (In other ways, Big Tech is pretty dang borderless, shifting its profits, manufacturing facilities, and jobs all around the world to chase favorable regulatory regimes that allow it to launder money, cheat on taxes, exploit workers, and pollute the environment.)

In the EU, Big Tech is (correctly) viewed as an American phenomenon. This fact means that in Europe versus the United States there is (at the moment) much more space for bold, muscular regulation—of the sort that will weaken the tech giants' market power and drain their cash reserves with punishing fines.

That's how the EU came to pass the 2016 General Data Protection Regulation (GDPR), a broad, sweeping consumer privacy law. I was still living in the EU when the GDPR was being debated, and I even did a bit of lobbying on it in Brussels. I got a firsthand view of the *army* of lobbyists that descended on the European Parliament in the run-up to the GDPR's passage. One EU commissioner told me that it was the largest-scale, most intense lobbying they'd ever experienced in their long career.

The GDPR is far from perfect. You may know it as the origin of all those tedious “click here to accept cookies” banners. Tech companies maintain the pretense that this satisfies the GDPR's main edict, which is that companies can collect and process your data only with your consent.\* Under the GDPR, the fact that you don't give your permission to collect or use your info can't be used as the basis for a company to deny you access to its service, or to charge you more to use it. A company *does* have to ask your permission before spying on you, but if you ignore the question, it has to let you just get on with using the service.

Obviously, that's not how companies behave. Instead, they bombard you with “cookie consent” dialogues that flagrantly violate the GDPR, and, what's worse, they get away with it.

Why is this? It's down to the intrinsic weaknesses of federalism—the system of government whereby autonomous regions form a federation and cede some of their power to its government. If that sounds abstract, perhaps it'll be easier if I tell you what that overarching body is called: a federal government.

\* Or, under limited circumstances, when they have a “legitimate purpose” to collect and use your data. For example, if you give your address to a merchant so it can ship you a parcel, it doesn't have to separately ask your permission to collect your address and use it to ship your parcel, because that would be really stupid.

The United States is a federation, too (hence *The Federalist Papers*, the pamphlets that Alexander Hamilton, James Madison, and John Jay wrote to promote the ratification of the Constitution), albeit one that is much older than the EU, with far more powers claimed by the federal authorities. (When I studied for my US citizenship exam, I was required to answer a skill-testing question about this, explaining the meaning of the tortuous syntax of the Tenth Amendment: “The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.”)

The twenty-seven member states that make up the EU have a lot of autonomy, for good and bad. Part of that autonomy is broad leeway in how their tax policies are structured. Several EU nations have spent decades locked in a race to the bottom in the hopes of becoming the EU’s top tax haven.

EU law generally lets a company pay taxes in its home country, no matter how low those taxes might be. So, for example, Amazon EU pretends that it is based in the infinitesimal and wildly corrupt Grand Duchy of Luxembourg, a flyspeck nation claiming 672,000 residents and 41,000 companies. Some of those companies are genuinely Luxembourgian, of course, but tens of thousands of Luxembourg companies’ “headquarters” are staffed by a few lawyers and their assistants, who shuffle paper around and help them avoid taxes. That’s why Amazon is a Luxembourg company, with 4,500 paper pushers who help it duck its tax obligations to the other twenty-six EU member states. (Meanwhile, Amazon employs 220,000 people in France and 25,000 people in Spain.)

But—Amazon notwithstanding—Luxembourg is far behind in the EU tax-haven sweepstakes. The clear leader here is Ireland, where most of the largest American tech companies pretend

their EU operations are based. Having an Irish address allows those companies to insist that their profits are floating in a state of untaxable grace, somewhere over the Irish Sea.

The thing is, a tax haven *always* turns into a crime haven. Any company willing to do the paperwork to pretend to be Irish this week could pretend to be Luxembourgian next week (or Cypriot, or Maltese, or Dutch—even Holland has much to offer by way of tax avoidance for footloose tech companies). To keep companies from defecting to rival tax havens, countries like Ireland have to promise lax law enforcement across the board, not just when it comes to taxes.

Which explains how the GDPR failed. The way the GDPR is written, Europeans whose privacy has been invaded have to first seek justice from the regulators in the company's home country, though they can eventually appeal a decision up to the European Court of Justice, the EU's federal court.

The largest American commercial surveillance companies pretend to be Irish, and in exchange Ireland has the worst privacy regulator in Europe, taking far longer than its non-Irish counterparts to produce a ruling, upholding facially absurd excuses for surveillance, and (eventually) getting overruled by Europe's federal appeals court at a rate that outstrips all the other EU privacy regulators.

To give you an idea of how bad the Irish privacy regulator is, consider Facebook's absolutely laughable excuse for spying on Europeans. Remember, the GDPR allows a company to collect, store, and use your data only if you give your explicit consent, or if it has a "legitimate purpose" for doing so.

Now, on to Facebook's laughable excuse. In 2023, Facebook told the Irish privacy regulator that spying on its users to target ads to them was a "legitimate purpose," because those users had a *contract* with Facebook wherein Facebook *promised* to spy

on them and flood them with targeted ads. That “contract” was Facebook’s novella-length terms-of-service document, which (to a first approximation) no Facebook user has ever read. Facebook’s argument boiled down to this: “Our users *want* us to spy on them and bombard them with ads, and we know this is true because they wouldn’t have clicked ‘I agree’ on our terms of service otherwise. Imagine how *disappointed* those users would be if we didn’t spy on them! We don’t need to get their consent for that surveillance. We have a contract to spy on them, and spying on them to fulfill that contract is *definitely* a legitimate purpose.”

The long, expensive road to holding these mock-Irish American tech companies to account for flouting European privacy law bought them about a decade of noncompliance with the GDPR, though some cases are finally making their way to the federal courts.

The problems of enforcing EU corporate regulations are well understood by EU policymakers, who are plenty steamed about the GDPR’s failure, over its first decade, to notably curb commercial spying in Europe by the biggest tech companies in the world. That’s why new EU tech regulations like the Digital Markets Act (DMA) and Digital Services Act (DSA), both of which took effect in 2024, shift enforcement from EU national courts to the European Court of Justice. This is an extremely promising approach! Though, of course, it’s not without its risks: as the EU consolidates power in its federal institutions, it will face resistance from the member states. (Americans will be familiar with this phenomenon, of course.) Also, a federalized enforcement system for Big Tech may not be corruptible in the same way that the decentralized, national enforcement system is today, but that doesn’t mean it’s incorruptible.

Meanwhile, the DMA and the DSA represent *very* big swings. At their best, both acts strike at the root of Big Tech’s power. Both

laws have interoperability requirements—rules forcing tech companies to open their app stores, to allow third parties to connect to their services, and to drop the various gambits they use to fight against third-party payment processing.

These laws also have *structural separation* provisions—these are rules that force companies to spin off or shut down divisions that compete with their business customers. The idea of structural separation is venerable, simple, and effective. Early US antitrust laws forced banks to spin out their investment arms, on the grounds that banks that owned companies that competed with the businesses that depended on them for loans would have an unstoppable temptation to cheat. If you own a pizzeria and the bank that loaned you the money to start your business also owns the pizzeria across the street, the bank can put you out of business anytime it wants—it can “loan” its own pizzeria enough money to sell pizzas below cost until you go out of business (at which point the bank’s pizzeria can jack up its prices). It can increase your interest rates when your loan rolls over. It can loan itself money to get through an economic downturn and deny the same loan to you.

It’s very hard to figure out whether a bank has loaned its own business money but denied the same loan to a competitor for fair reasons (the competing business is badly run, say) or for unfair ones (to drive a superior rival out of business). Unless the bank manager puts a confession in writing—sends a memo to a colleague admitting to their motivations—you will never be sure about the reasoning behind a loan or a denial.

In the wake of the Great Depression, the United States imposed structural separation on its banks: banks could either make investments (“investment banks”) or take in deposits and make loans (“retail banks,” or just “banks”). This worked extremely well, and when the United States ended this practice—when Bill

Clinton signed the Gramm-Leach-Bliley Act, under the guise of strengthening Americans' privacy rights—the eventual result was the Great Financial Crisis of 2008, which brought the world economy to its knees.

Structural separation is a bedrock of democratic political and legal systems. Lawyers object strenuously to judges who have a conflict of interest, as when the judge is related to one of the parties, or has an investment in their adversary's client's business. By and large, judges recuse themselves from these cases, even if they're sure they can be fair. (The obvious exception is the US Supreme Court, where, shockingly, there appear to be no limits to conflicts of interest.)

With its 2024 regulations, the EU is bringing structural separation to Big Tech. Platform owners are broadly prohibited from competing with platform users—meaning, for example, that Amazon won't be able to spy on its sellers' orders and then clone their best products, and that Apple and Google will have to decide whether to operate app stores for your phone or make apps that compete with the ones in their app stores.

As with judicial recusal, forcing Apple, Google, Amazon, and other platforms to recuse themselves from competing with their own customers resolves their otherwise unresolvable conflict of interest by eliminating it altogether.

This is a marked departure from decades of tech policymaking, especially in the EU. For most of its history, the EU has devoted its energy to making tech companies better rather than making them weaker and so making their errors less consequential.

For example, in the decade before the passage of the new DMA and DSA, many EU countries enacted some form of “harmful content” rule, which makes the platforms responsible for their users' harassment, hate speech, and other odious conduct.

On the one hand, this sounds reasonable: the platforms har-

bor toxic users who force women, LGBTQ people, racial minorities, and other marginalized groups to choose between facing a nonstop shower of the most ghastly abuse and being able to fully participate in public life, with access to all the communities and services that organize on the platform. No one should have to make that choice.

On the other hand, if platforms are to control their worst users' conduct, they must be able to conduct fine-grained, continuous surveillance (to spot the statistical correlates of coordinated harassment, such as a small group of users all communicating intensely with one another and then bombarding a separate user with multiple, similar messages), and they must be able to control those users' conduct. A platform that is responsible for policing coordinated harassment is going to want to do things like control the number of participants in a conversation, limit the actions of new accounts, and take other steps to counter bad activity.

Likewise, a platform that is responsible for policing hate speech needs to have a deep understanding of each social interaction. Are the people using a racial or gender-identity slur part of the group the slur refers to, doing some kind of reclamation of a hurtful word? Is the person publishing a slur describing a traumatic incident ("And then he called me the n-word") or are they *manufacturing* a traumatic incident ("Yeah, I called you the n-word, what are you gonna do about it?").

Making platforms responsible for their users' conduct requires that platforms have *more* power and *more* control over their users than they do now. Interoperability orders that force platforms to allow communications from rivals, and privacy rules that ban platforms from intercepting and processing other services' user data, are fundamentally incompatible with orders that force platforms to control their users.

In other words, we have to choose: *Either* we make the

platforms more powerful in hopes that they'll use that power to fix the problems they've created, *or* we make the platforms *less* powerful so that the people they've failed can escape from them. We can't do both.

I think the verdict is in on “making the platforms use their power wisely.” It's a fool's errand. The problem with the platforms isn't that they abuse their immense power. It's that they *have* that immense power.

The DMA and the DSA are trying to both fix and weaken the platforms—and that's their biggest stumbling block. They're the legislative version of a lungfish, an evolutionary link between an old model of tech regulation and a new one that's just emerging, with properties of both.

A promising step, in other words, but still a work in progress.

# Administrability

So here we are, in a moment when there's been more regulation in four years than in the previous forty, when we're shifting our emphasis away from forcing the platforms to be better and toward making the platforms less powerful.

You, as a person who cares about this stuff, are partly responsible for this trend: your interest, mine, and that of everyone else who is exercised about tech and talking about it constitute that nebulous but all-important force we call *political will*.

There's no big money funding the modern antitrust movement; it's an entirely grassroots phenomenon. That's another way of saying that we're experiencing a surge of political will, a wind that fills the sails of anyone who is trying to steer toward a new, good internet.

That means we're going to get a *lot* of tech policy proposals. You and I, and the others on our side, are going to play a role in the messy process by which some of these proposals will become law. Which proposals should *you* get invested in?

I've already talked about one way to measure whether a tech policy will help produce a new, good internet: *Does it make the platforms weaker?* The enshitternet exists because the platforms got too big to care, so making them weaker will (1) make them try harder to be better and (2) make it easier for us to go somewhere else and kill them off if they aren't up to the challenge. That's why laws that try to fix the platforms *and* weaken them—

like the EU's Digital Markets Act and Digital Services Act—are less effective than they could be.

A good question to ask about a policy proposal is this: *What does it do?* In this section, I want to talk about another question, one that is, if anything, even more important, namely: *Will this proposal succeed once it makes contact with the real world?*

The tech platforms have shown time and again that they are bad at self-regulation. To get them to do anything, they're going to need *external* forces of discipline, like regulators, auditors, watchdogs, transparency requirements, private litigators, and public prosecutors. The easier we can make the job we ask these enforcers to do, the better they'll be at it.

So, what makes a policy *administrable*? Two key considerations here are (1) how hard it is to spot rule-breaking, and (2) how hard it is to agree on whether the rule was broken.

Think of those “harmful content” regulations that have popped up in the EU, Canada, Australia, and elsewhere. Broadly, these rules demand that platforms take reasonable steps to detect and block hate speech and harassment. Hate speech and harassment are huge problems on the platforms, and these problems are disproportionately experienced by the most marginalized people in our society. Despite the harms that being subjected to abuse can cause, many of the users targeted by abusers stay on the platforms because leaving means cutting off communications with their professional community, the families they left behind in a distant country, their customers, and local groups that are vital to their well-being.

So there is nothing wrong with the idea of protecting social media users from harassment and hate speech.

But a *rule* that says that platforms must accomplish this through content moderation and account deletions is *very* hard to administer.

Say you're a user who has been subjected to on-platform harassment. You've exhausted all of the platform's own mechanisms for addressing this, and the abuse won't stop. So you take this case to the regulator (or possibly to a court, depending on how the rule is structured).

To address this case, the regulator must now:

- Define *harassment*.
- Determine whether the conduct you experienced meets that definition.
- Investigate the procedures the service has in place to protect you from harassment.
- Determine whether these procedures are adequate.
- Determine whether the platform has correctly employed these procedures.

This is what lawyers call a fact-intensive rule. It can be enforced only after extensive fact-finding, along with all that entails: comments from the platform explaining why the facts favor their case, counter-comments from you or your lawyer explaining why they're wrong, and so on (and on and on).

What's more, determining whether a platform's technical measures meet a test for "reasonably effective" involves interpreting technical information about its server configurations, its automated software tools, and other technical systems that are typically built from scratch for each of the large platforms. That means almost no one has a complete understanding of the platform's technical workings, and the few people who *do* understand them are almost certainly on the platform's payroll and thus not the most neutral testifiers as to whether the system has been well made or not.

Now, the mere fact that a law requires extensive fact-finding

and interpretation doesn't disqualify it from consideration. Probate law, for example, often requires a deep inquiry into the facts. But you only die *once*, and most people don't leave behind messy estates that require long court battles to resolve. It's fine to have a complicated law to deal with these rare, high-stakes occurrences.

Contrast "dying and leaving behind an ambiguous will" with "having an unpleasant interpersonal interaction on a big social media platform." The former arises less than once per lifetime for each of us; the latter can happen six times before breakfast.

That makes fact-intensive anti-harassment rules profoundly unsuitable for the real, serious problems they seek to address. Indeed, it's *because* online harassment and hate speech are so important that we should ensure that any rules we create to address them are fit for the purpose.

It's not enough that these rules be well intended and well crafted. They also have to be *administrable*.

So, how can we grant much-needed relief to the people who endure vicious online hate and harassment campaigns?

To answer this question, we first need to acknowledge that there is a simple step that all people who are targets of online harassment and hate can take to escape the trolls: they can resign from social media, drop their email addresses, and delete all their instant messaging accounts. Indeed, this is something that a few high-profile targets have done.

Given that this powerful self-help measure is so readily available, why do we even talk about solving this problem any other way?

The answer is obvious: because quitting the field comes at a very high price. Recall page 13, where I discussed switching costs. If you use online tools to reach the family you left behind when you emigrated, or a support group for your rare disease, or your customers, or the carpool-organizing parents on your kids'

sports teams, or the teachers at your kids' school, or your elected officials, or fellow targets of online harassment, then resigning from all your online accounts means that your life will be substantially worse. It can mean that you and the people who rely on you end up poorer, lonelier, or sicker.

Once we understand that the root of the problem isn't that people are mean online but that escaping online sociopaths comes at a high price, a whole universe of new policy prescriptions opens to us.

What if we switched our emphasis from "making platforms nicer" to "making platforms less important"? What if there was a way for you to leave a platform whose moderation policies have failed you, without severing your connections with friends, family members, communities, and customers?

The good news is that this is *absolutely* possible. Indeed, some social media platforms already have this technical facility. What's more, a rule that required social media platforms to facilitate their users' painless departure would be extremely easy to administer, without any of the fact-intensiveness that makes anti-harassment rules so cumbersome.

Mastodon, for instance, is a *federated* alternative to Twitter and Facebook. Signing up for a Mastodon server yields a familiar experience: you follow the people you want to hear from, and when they post something, you see it, in a timeline that puts the most recent posts first. You can create thematic lists of accounts (e.g., "journalists," "artists," "friends") and tune in to just a few feeds. You can exchange direct messages with others and post your own words, pictures, and videos.

The thing that makes Mastodon federated is that there are *lots* of Mastodon servers, with all kinds of management structures: some are co-ops, some are nonprofits, some are run by hobbyists, and some are run by businesses. Meta's Threads is a Mastodon

server, and Truth Social, Donald Trump's social media platform, is also a Mastodon server (more on this in a moment).

By default, Mastodon servers are designed to exchange messages with one another in the same way that, say, email servers do. You can send an email from your Gmail address to a work colleague on an Outlook address, cc'ing an old friend from university using a northeastern.edu address, as well as your weird computer-savvy buddy who runs their own email server on a domain like craphound.com. (That's *my* personal domain—it's a long story.)

In the same way, you can sign up for one of the big Mastodon servers like mastodon.social (a server run by the nonprofit, open-source group that maintains the code for Mastodon) and follow me (on mamot.fr, a server run by the French digital rights group La Quadrature du Net), as well as the news source ProPublica (on newsie.social, a server for news publishers); my fellow Farrar, Straus and Giroux author James Gleick (on mas.to, which relies on donations); and the computing legend Tim Bray (on cosocial.ca, a cooperative). You can follow artists, shitposters, porn stars, religious leaders, Nazis, politicians, anti-fascists, and your friends and family.

Again, by default, all these different kinds of servers exchange messages with one another without you having to know anything about them or their management structures or philosophy.

But though servers *can* exchange messages with one another, they don't *have* to. Every server gets to decide whether it will *defederate* (block) other servers. When Truth Social joined the “fediverse” (as all of these federated servers are collectively known), a lot of users decided they didn't want to hear from, be read by, or see anything posted from a conspiracy-addled fever swamp of Trump cultists, so they blocked Truth Social. If you *want* to interact with Truth Social users, it's not hard: you can

sign up for Truth Social, or hang out on the small (but nonzero) cluster of servers that remain federated with it. But no one forces you to hang out with a group of users that has a higher-than-average level of harassment campaigns.

Truth Social isn't the most contentious fediverse server. There are plenty of servers run exclusively by harassers and trolls that federate only with each other (but not always—unsurprisingly, trolls often feud with one another).

So if you join the fediverse,\* you can do some research in advance and figure out whether the server you're joining has policies that are to your liking. You're not limited to just one set of moderation policies.

But if doing your homework about Mastodon server moderation policies doesn't excite you, don't sweat it. Just join *any* Mastodon server—there's a list of reputable ones at [joinmastodon.org](https://joinmastodon.org)—and get set up.

It doesn't matter which Mastodon server you choose, because if you later regret your choice, you can *change your mind*. By default, Mastodon comes with a link that packages up the list of everyone you follow, everyone who follows you, and all the people you block and mute, and sends it to you in a neat little file.

When you want to change Mastodon servers, all you need to do is click the “Export” link in your settings for your old account. Then you sign up for a new account, click the “Import” link, and select that exported file. With just a couple of clicks, you're set up on that new server. Anyone who followed you in your old digs will continue to see your posts, and you'll keep seeing the posts of the people you follow.

In other words, the switching costs of leaving one Mastodon server for another are damn near *zero*. If you are on a server you

\* And I hope you will! Say hi! I'm @pluralistic@mamot.fr.

don't like, find another one! Switching Mastodon servers is a bit like switching cellular carriers: do a little administrative work, wait a few minutes, and—*bam*—you're all set up with a new network, but everyone who calls your old phone number can still reach you. Even better, when you switch Mastodon servers, you don't have to talk to a “customer retention specialist” who is paid to try to talk you out of switching.

Mastodon is built on a free, open, robust standard called ActivityPub. The account-switching stuff is standardized, and there are free, open-code libraries that implement it, which any company can use to update its own server software to permit this kind of freedom of movement between servers.

Which brings me to a policy proposal: Rather than forcing Twitter or Facebook to spy on their users and control their behavior in the name of preventing harassment, we can force these companies to facilitate the departure of users who have been failed by their moderation policies. We can force these giant social media companies to federate with other servers, and to provide their users with the files needed to leave the big platforms and go to an alternative, all while maintaining contact with the family, friends, communities, and customers they leave behind. That way you could leave Facebook or Twitter without cutting off the people who matter to you.

We can make the platforms less important, rather than making them less terrible.

The thing about this “right-to-exit” policy is that it is *highly administrable*. If a user claims that he left Twitter (or was kicked off) and capriciously denied the file he needed to get set up on a new service, a regulator doesn't need to do *any* fact-finding. She can just send a message to Twitter saying, “Look, I know you *say* you gave Cory his data, but he never got it. Rather than figuring out what happened, just send that file to *me*, and I'll forward it

to Cory.” The regulator always knows whether Twitter sent the file to *her*.

A right-to-exit policy need not—and should not—fully replace other policies aimed at curbing terrible behavior on the platforms. Some harassment rises to the level of a crime, and acts that threaten users’ physical safety (doxing, sharing nonconsensual nudes or deepfakes, committing fraud) demand a serious response, which the platforms themselves should play a role in.

But if we give users a self-help measure—if we let them leave a platform that has failed them—we give them immediate relief. They might *still* pursue official retribution against their tormentors, but they get to do this while ensconced in a digital home that takes their safety and well-being seriously.

A right-to-exit rule moves scarce moderation resources to the most serious cases, gives the targets of online abuse immediate relief (and thus punishes tech platforms for failing their users), and gives communities a way of overcoming the collective action problem of deciding whether to leave a platform, and when and where to go. On top of all that, it’s the kind of rule that can be administered at scale, with a small staff covering a large number of disputes. After all, every dispute has the same resolution: “Give that person the file, now. If you don’t, we’ll fine you. If you keep on failing to comply, we’ll make things *really* ugly for you.”

A right-to-exit rule that relies on open standards with free reference implementations avoids the trap of a “capital moat”—when a regulation is so expensive to comply with that only the largest and most profitable companies can afford to be in business.

Finally, a right-to-exit rule focuses on the real problem: the platforms are so powerful that we can’t afford to quit them, even when they fail us.

A right-to-exit rule isn’t the only highly administrable tool

for making platforms weaker and giving technology users immediate relief.

Recall our discussion of intermediaries and the end-to-end principle on page 65. Intermediaries play a vital role: without middlemen, anyone seeking to connect with an audience, sell a product, or form a community would have to run the whole show, from web hosting to payment processing and everything in between. There are *plenty* of people who have something to contribute, sell, or say who are not capable of—or interested in—being a payment processor or a web-hosting provider.

The problem isn't the existence of intermediaries; it's intermediaries that grow so powerful that they usurp the relationships between the individuals who rely on them.

How can we keep intermediaries in their place?

Recall that the internet is founded on a principle that limits the role of intermediaries: the end-to-end principle, which holds that the only thing an intermediary should do is deliver data from willing senders to willing receivers as efficiently and reliably as possible.

When we apply end-to-end to your internet connection, we call it net neutrality: the idea that when you click a link, your ISP should get the bits at the other end of that link and shove 'em down your internet connection as quickly as possible. If you want to watch a Netflix video, your ISP should make its best effort to get you that video, even if Max has offered your ISP a bribe to slow down Netflix in hopes that you will switch to Max. Your ISP should give you the data you ask for, not the data your ISP's shareholders *wish* you'd asked for.

Neutral *connections* gave us the old, good internet, but end-to-end has never been formally applied to *services*, which is a pity, because a requirement for services to be end-to-end would

go a long way to curbing excessive intermediary power, and is highly administrable to boot.

An end-to-end intermediary has a duty to deliver the data you asked for as reliably and quickly as possible. We can apply this rule to all *kinds* of services. If we apply it to email, then we'd say, "If I drag an email out of my spam folder, then you *must never* put email from that sender into my spam folder unless I tell you to." That way, the independent newsletter writers you subscribe to, the merchants you've asked to send you information about their new offerings, and the politicians whose mailing lists you've opted into can all be *certain* that if they email you, you'll get the message. Not only is that good for you, but it's also good for them, because an end-to-end email provider can't force the people you want to hear from to pay for "premium" services to ensure delivery.

We can apply end-to-end to social media, of course. When you sign up to follow someone on Facebook, Instagram, TikTok, Twitter, or YouTube, those services should offer you a feed where you see *everything* posted by the people you follow.\* Yes, that will severely limit how many ads and boosted posts—or "sponsored content"—those services can shove into your feed, but that's the point. An intermediary's job is to faithfully serve the parties it sits between, so Facebook's job is to deliver the data you asked for, not the ads and sponcon they wish you'd asked for. Again, this means that you'll get what you ask for, but also the performers, posters, publishers, and other business users you follow on these platforms will be protected from shakedown demands to pay to "boost" their content to reach their own confirmed subscribers.

\* Alas, when Mark Zuckerberg says he wants Facebook to "get back to its roots," this isn't what he's talking about.

End-to-end applies equally well to search results of all kinds. Did you search for an album on Spotify? Then Spotify should return the album at the top of the search results, not a playlist (with the same title and graphic as the album) filled with insipid, AI-generated covers that Spotify gets to play for you for free, rather than paying any musicians.

Did you search for a specific product on Amazon? The top result should be the match for that product, not a copycat product that someone has paid a fortune to stick at the top of the results.

There's a very simple principle at work here: When you ask a company for one thing and it shows you something else in hopes that you won't notice, that's fraud. Specifically, the FTC alleges that it's a violation of Section 5 of the Federal Trade Commission Act, which prohibits "unfair and deceptive methods of competition."

Companies that break end-to-end do so in order to create opportunities to charge other people money to try to trick you, and to create opportunities to charge money to the people whose products, services, performances and materials you're *trying* to find, to "boost their content" and get it to the top of their list. It's a double whammy: an auction for your attention for scammers, and a ransom demand to the people you're actually trying to connect with.

So a bright-line rule that says "The role of a service is to connect willing senders and willing recipients as efficiently and reliably as possible" would extinguish the vast majority of this conduct. It would force platforms to be *good* intermediaries, whose role is to facilitate connections, not steer them.

What's more, this rule is very easy to administer. If a user complains to the regulator about not getting accurate search results of faithful delivery of feeds and messages they asked to see,

the regulator doesn't need to do an intense fact-finding; it can just replicate the user's searches and subscriptions and observe what happens.

This isn't treating companies as "utilities" or "common carriers" (both of those terms have extremely specific meanings in law). This is, foundationally, a prohibition on "unfair and deceptive" practices. People who sign up for an email account want to get all the email sent by the people they want to hear from—not just the fraction that an email provider chooses to deliver. People who search for a product want to see listings for that product—not for competitors who've paid to be listed over the best match for their queries. Companies will complain that making them give customers the things customers ask for "stifles innovation." That is broadly true: it will stifle innovation *in fraud*. Sounds good to me.

Tech regulation is undergoing a global transformation. Bold new rules are under consideration or have already passed through legislatures. Rules that strike at tech's dominance, its impunity, and its market power are necessary to instill the fear of regulation in companies run by executives with a healthy sense of self-preservation—and to put the executives who don't get the message out of a job.

Not every tech regulation is good, and a rule can certainly be *bold* without being *good*. A new, good internet is a well-regulated one, and to be well regulated, it needs rules that curb corporate power, rather than cementing it, and those rules need to be administrable so that they can be enforced.

## Bringing Back Self-Help

It's one thing to get the tech companies to fall in line behind new, good rules, but what about the old, bad ones?

*Interoperability*—the latent power of every digital system to run every valid program—is a powerful anti-enshittification force. Sure, platforms shouldn't do bad things to their users and business customers, and sure, our democratically accountable lawmakers and enforcers should step in to smack them around when they get out of line.

But the wheels of justice grind slowly, and tech is *fast*. Even the most administrable, simplest-to-enforce rules are going to lag the endlessly imaginative fuckery that tech companies (and regular companies that have discovered the enshittificatory potential of making their products “smart”) devote every working hour to.

When a product or service that you rely on gets enshittified, you want public enforcers to have your back, but you don't want to have to wait for them to get around to fixing things. When your printer rejects the ink you bought at Costco, when your car breaks down, when your *wheelchair* breaks down, when a service you rely on changes its terms of service to suck up your data for AI training, when your wireless speaker gets an update that stops it from playing your own music, when you figure out that your TV is spying on you, you don't just want a place to complain, you want *action*.

Interoperability is a way for users of technology to help themselves, either while they wait for a regulator to take action or as a backstop in the event that no regulator wants to champion their causes.

There are a lot of different actors that can get in on the reverse engineering and modification game. Fix-it shops are an inherently local phenomenon because no one wants to send their phone or laptop away for repair—to say nothing of their cars, refrigerators, or solar panels. A neighborhood fix-it shop is a source of jobs (landfilling a ton of e-waste creates *one* job, while fixing that e-waste creates two hundred good, local jobs), is good for the environment (diverting e-waste from a landfill isn't merely about jobs, after all), and lets you and your friends spend less on gadgets and get more value out of the stuff you buy.

Repair is a big part of the interoperability story. So is adaptation. Digital services and gadgets are overwhelmingly designed by young, able-bodied, well-educated people living in one of a small number of large coastal cities. Even when these designers try hard to imagine all the situations their users will find themselves in and try to accommodate them, they will necessarily fall short.

Think of the COVID lockdowns and the supply-chain shocks that followed. Chinese high-tech manufacturing dried up overnight, and it became hard to impossible to source commodity components like the cheap microchips that Epson used to lock its printer-ink cartridges. Epson was forced to start selling ink cartridges without the security chips that its printers required, meaning that Epson printers were rejecting the official, expensive cartridges that Epson itself was selling. The company was forced to distribute instructions for disabling the cartridge-checking function on its own printers!

None of the design briefs for the gadgets made before the

pandemic contained a contingency labeled “Supply chains break down during a global pandemic.” But that’s exactly what happened. It’s nice that Epson decided to voluntarily disable its own profit-extraction system to accommodate the once-in-a-century pandemic, but not all companies did, and owners and users of digital tools shouldn’t have to rely on the largesse or rationality of the companies that sold them their stuff.

For one thing, companies go under! “Smart” devices are almost universally designed without any fail-safes for this eventuality. Google bricked its first-generation Nest home automation hubs, which were often used to coordinate monitoring, access, and safety at remote weekend places, where they couldn’t be readily replaced; the automaker Fisker went under and bricked all its unsold inventory; and the med-tech company Second Sight went bust and bricked the *artificial eyes* its customers had wired into their optic nerves.

Obviously, this is an area crying out for regulation, but until that happens—and even after it does—securing the rights of interoperators will allow users of “smart” devices to avail themselves of alternative servers or even new firmware for their gadgets that obviates the need for a server altogether.

A company doesn’t have to go under for its gadgets to be downgraded or even bricked. In 2024, Sonos, the leading “smart” speaker company, pushed an update to *all* of its speakers that took away the majority of their functionality and severely downgraded the functions that remained. I got caught in this, and months later, I’m still waiting for Sonos to make good on its promise to restore functionality to the thousands of dollars’ worth of home audio I unwisely bought from the company. (I foolishly assumed that the biggest risk of owning Sonos products was the fact that they came with microphones that could be hacked, so I bought models that didn’t have mics.) My speakers are all but useless—

one pair keeps playing booming music in the middle of the night and takes multiple tries just to set the mute. I ended up unplugging them. I would *much* prefer to buy a new operating system from some enterprising startup, one that severs my ties with Sonos forever. So would millions of other furious Sonos owners. If we restored the rights of interoperators—repealing or modifying laws like Section 1201 of the DMCA—there'd be a tidy little business for a new company to come in and scoop up.

Interop can also be brought to bear on services as well as products. The people who run online services are consistently *very bad* at figuring out what their users need, generalizing from their own bizarre billionaire lives to those of their users.

In late 2024, Elon Musk, owner of Twitter, unilaterally altered the function of the service's block button, so that the people you block on Twitter would still be able to see your posts, just not “interact” with them. Users and experts on online harassment were furious and appalled. Twitter users who have historically been subjected to dogpiling by trolls have relied on mass-blocking tools to keep their messages away from groups of vicious hate-mongers, who are often followed by the kinds of unhinged maniacs who are one viral hate campaign away from doxing their targets, calling them or their employers or spouses, swatting them (sending police to their homes after claiming that there is a fire or murder underway there, which can lead to death-by-cop), or even showing up themselves.

Musk has his own fears about stalkers and violent randos, which have led him to craft extensive policy to address the issue of people who use public records to reveal the movements of billionaires' private jets. This is an issue for a tiny handful of people, while Twitter's neutered block button imposes additional risk on millions, perhaps tens of millions, of users.

With interop, users could leave Twitter and continue to talk

to the people who mattered to them, but with far more control over the spread of their messages.

Interop is a fast, reliable way to fix, unbrick, improve, and adapt the technology we own. When users can unilaterally alter the way that a product or service works, they don't have to wait around for a regulator to step in, nor do they have to launch a costly lawsuit against a giant firm. They can treat the company's enshittificatory impulses as damage and route around them.

It's not merely that interop provides immediate relief for users—it also imposes immediate *and* lasting costs on companies that choose enshittification. When users engage in adversarial interoperability, the business whose products or services they modify immediately loses a key relationship with that user, and will struggle to *ever* recover that relationship. Once your customer discovers that third-party ink works just as well as the \$10,000-a-gallon official stuff, they're *never* coming back.

Every user can benefit from adversarial interop, but *very few* parties are capable of performing the reverse engineering, scraping, and other guerrilla tactics needed to reap these benefits. To turn interoperability into a check on the enshittificatory impulses of tech executives and their product designers, we have to deputize skilled third parties to assist normie users with their reverse engineering projects. It's not enough to have the right to reverse engineer your car's firmware or Twitter's app—*other* people need to be able to do this on your behalf.

If this sounds obvious, well, it *is*, but it still bears mentioning here, because policymakers all over the world act as though this isn't true.

Though tech and tech-adjacent companies have figured out how to mobilize *all* of IP law against interoperators, one kind of law stands out as the most dangerous impediment to adversarial interoperability: anti-circumvention rules like Section 1201

of the US Digital Millennium Copyright Act (see page 138 for more).

You'll recall that this law prohibits bypassing "access controls" that sit in front of copyrighted works. You can't jailbreak your ebook reader to move your books to a rival device or app without falling afoul of this rule. Likewise, you can't jailbreak your *car* to get it to accept third-party parts without violating DMCA 1201.

This anti-circumvention law was born in the United States, first proposed by Bill Clinton's copyright czar, Bruce Lehman, who tried to get Vice President Al Gore to include it in the "Information Superhighway" initiative that moved control of the internet away from the US military to a multistakeholder system dominated by private firms.

Gore rejected this idea, so in 1996 Lehman did an end run around the US government and went to the United Nations' World Intellectual Property Organization (WIPO), an agency that is the root of nearly all bad global internet law in the same way that Mordor is the root of all evil in Middle-earth. Lehman, along with the Office of the US Trade Representative, talked the world's governments into integrating anti-circumvention into two treaties, the WIPO Copyright Treaty and the WIPO Performances and Phonographs Treaty, collectively known as the Internet Treaties.

In 1998, Congress passed the DMCA as a way of satisfying US legal obligations under the Internet Treaties. This is quite a little maneuver: after one part of the Clinton administration rejected the batshit proposals of another part of the administration, the thwarted party went to the UN, turned the rejected proposal into a treaty obligation, and then came *back* to the United States and convinced Congress that it *had* to adopt this batshit proposal as law. Aaron Sorkin, eat your heart out.

All this skullduggery did not go unnoticed at the time.

Many experts were rightly alarmed by the possibilities for anti-circumvention to metastasize out of the narrow domains it applied to in 1998 (when it was principally used to prevent people from unlocking their DVD player so they could watch videos bought outside the United States) and into any device with a computer chip.

As a sop to these critics, the DMCA instructs the US Copyright Office to solicit proposals for exceptions to the rule, every three years. This is billed as an “escape valve” for “unintended consequences” of DMCA 1201—for example, using the law to block repair of ventilators, cars, or phones.

The Copyright Office has held these proceedings every three years since the turn of the millennium, and while it has granted *many* exemptions, these have been almost totally useless. That is by design: you see, these “triennial exemptions” proceedings are a *scam*.

Under the statute, the Copyright Office collects testimony, data, and rebuttals on problems caused by DMCA 1201. Then, after weighing all the evidence, it is empowered to grant a *use* exemption. For example, if you prove that the App Store unduly restricts your access to desirable iPhone apps, the Copyright Office can grant you the right to bypass the iPhone’s access controls and install apps of your choosing, or even a third-party app store.

That may sound about right, but there’s a *massive* catch: this is a *use* exemption, and it does not include a *tools* exemption.

That means that all the Copyright Office can do is grant individuals or groups—up to every single American—the right to *individually* figure out how to jailbreak their iPhones and install apps of their choosing on them.

As you sit down to begin your round of high-tech hand-to-hand combat with the best security engineers Apple can afford, remember that this exemption does not allow you to discuss your

efforts to jailbreak your phone with anyone else. As you dump the ROMs on your iPhone and go through the assembly language code, symbol by symbol, you can neither post any of that code to the internet (privately or publicly), discuss its meaning, or trade tactical notes on how to defeat it.

As you may recall from page 149, if you break any of these rules, you can face felony prosecution, with a five-year prison sentence and a \$500,000 fine for a first offense. So you'd better play your cards close to your chest.

If this sounds really weird, that's because it's really *stupid*. A use exemption without a tools exemption amounts to a useless ornament, a performance of balance without any actual balance.

The United States didn't just export anti-circumvention law around the world—the Office of the US Trade Representative also exported this *demented* use-only exemption.

In 2001, the EU adopted the European Union Copyright Directive (EUCD), whose Article 6 mirrors the language of the American DMCA 1201. In 2003, Norway implemented the EUCD into its own domestic law. At that time, I was still serving as European director for the Electronic Frontier Foundation, and in that capacity, I was invited to Oslo to debate the new law with the minister responsible for it.

The minister's opening remarks were full of self-praise for the "balanced" approach that Norway had taken to the law. Rather than forcing the Norwegian public to apply for exemptions to the anti-circumvention law, Norway's legislature had baked several exemptions into the law from the get-go. The minister was most proud of an accessibility exemption that allowed blind users to jailbreak their ebooks so that they could run them through text-to-speech tools, Braille printers, and other assistive devices.

Then it was my turn. I asked the minister who was empowered

by his law to conduct the reverse engineering needed to help blind people read their ebooks.

“Why, blind people,” he said.

“So blind people are allowed to decompile and reverse engineer an ebook program like Adobe Reader, look for vulnerabilities in the code, and write exploits that allow them to extract the text of ebooks so they can use them in assistive devices.”

“Yes,” he said.

“Can organizations that represent blind people do this work for their members?”

“No,” he said.

“Can universities do this work on behalf of blind people?”

“No,” he said.

“Can commercial companies sell blind people a tool that moves their ebooks from Adobe Reader format to one that’s compatible with assistive devices?”

“Absolutely not,” he said.

“Can one blind person who figures out how to do this tell another blind person how they did it?”

“No,” he said.

“If a blind person converts an ebook to a format that works with an assistive device, can they give a copy of that compatible file to another blind person?”

“No,” he said.

“So,” I said, “to exercise this exemption, every single blind person in Norway would be expected to individually crack Adobe Reader. They would have to labor in total secrecy, telling no one how they accomplished the work, and no one would be permitted to give them any technical assistance.”

He conceded that this was, indeed, how the exemption in his law worked.

The point of all this is that while interoperability can be a powerful force for disenshittification, and while learning how to get more out of the computers and programs you use is a powerful, fun, and liberating pastime, unless we empower third parties to engage in adversarial interoperability *on behalf of users*, we will not reap its benefit.

These are the kinds of intermediaries we *want*: intermediaries who step into the nonconsensual, abusive relationships we are forced into with powerful vendors. Intermediaries who come to the rescue with cool, useful hacks that let us use technology in the way that benefits us, even if the technology's manufacturer objects.

For regulation to work, it must be administrable. For interoperability to work, it must be *delegatable*. Everyone can benefit from interop, but not everyone can be an interoperator. The problem isn't middlemen: by managing specialized, esoteric, and technical tasks, middlemen can increase participation and access. The problem is *powerful* middlemen. A new, good internet is built on policies that reduce middlemen's power when they act against our interests, and protect them when they act to further those interests.

## The Strange Tale of Beeper Mini

Whatever else billionaires are good at, they sure have a real talent for saying the quiet part aloud. Back in 1989, when the eminently guillotineable hotelier and legendary shitty boss Leona Helmsley was on trial for tax evasion, one of her much-abused maids testified that Helmsley had vouchsafed, “We don’t pay taxes; only the little people pay taxes.” (Sentenced to sixteen years for tax fraud, Helmsley was released after only nineteen months.) Satan took Helmsley to hell in 2007, but her breathtaking act of let-’em-eat-cake hubris was, and still is, typical for the ultrarich.

Take Tim Cook, Apple’s billionaire CEO, who was elevated to replace founder Steve Jobs after he figured out how to move Apple’s manufacturing to Chinese sweatshops without compromising quality. (The answer turned out to be partnering with the electronics giant Foxconn to create factory environments that were so unbearable that the company installed suicide nets to catch workers who had reached the ultimate breaking point.)

In 2022, *Vox Media* reporter LiQuan Hunt asked Tim Cook how he could communicate securely with his mother—an Android user—with Apple’s default iMessage App.

Cook’s answer: “Buy your mom an iPhone.”

iMessage is an “end-to-end encrypted messaging service.” I’ve talked about the end-to-end principle a lot already in this book, but here’s yet another way in which end-to-end is critical to a

healthy internet. A service is end-to-end encrypted when outgoing messages are scrambled by the sender and not unscrambled until they reach their receiver.

We call that scrambling *encryption*, and it's a powerful expression of some extremely esoteric (and very, very cool) mathematics. After years of guerrilla warfare with surveillance-happy governments, we've arrived at a happy juncture where nearly everything you do with a device these days is encrypted by default.

Reach into your pocket and take out your little black distraction rectangle. Open up the camera app. Point it at this page. Press the shutter button. Congratulations, you've just committed copyright infringement. See you in court.\*

Now, in the eyeblink that it took for your phone's sensor to capture an image of the words on this page and store them on its internal drive, it scrambled (encrypted) them so thoroughly that if every hydrogen atom in the universe were transformed into a computer and set to guessing which key was needed to unscramble that picture, we would run out of universe *long* before we ran out of possible keys. So long as the scrambling system is well made, there is no way to guess or derive the key needed to unscramble things that are sent over the internet or stored on the devices used to send or receive those things.

(You can delete the photo now. Or better yet, post it to your group chat or social media account with a note telling people how much you're enjoying this book! Here, I'll provide you with some explanatory text: Greetings, followers of my reader! This is Cory Doctorow writing to you, and your friend has very nearly finished reading my excellent 2025 book, *Enshittification: Why Everything Suddenly Got Worse and What to Do About It*, avail-

\* Just kidding. Despite the ominous and wildly legally incomplete copyright notice at the front of this book, fair use is a thing, and it covers what you just did.

able at finer bookstores everywhere, as well as on monopoly electronic retail sites that should be condemned to the scrap heap of history.)

But just because something is *encrypted*, it doesn't mean that it is *end-to-end* encrypted. Take the wildly popular messaging platform Telegram, which bills itself as an encrypted messaging service. Nearly all of the messages exchanged between Telegram's 950 million users are in group chats, which are not encrypted at all.

Then there's Apple's iCloud service. For years, Apple encrypted traffic between your device and its cloud servers but then stored your data in a format that Apple itself can access. (This is still an option, but Apple now defaults to end-to-end storage, after prolonged, repeated campaigns by privacy and security experts.)

When a service sports end-to-end encrypted messages, that means that only people who can unlock the sender's device or the recipient's device can unscramble those messages. Even if your ISP, your boss, your device maker, your government, or a criminal intercepts that message in transit, all they'll get is a profoundly scrambled string of nonsense that can't be converted back into the message.

This is very cool. It's also very important. Apple's iMessage is a successor to the antiquated short message service (SMS) system, which dates back to the Reagan era but really caught on in the mid-1990s, where it was commonly known as "texting."

Even today, people call sending messages using encrypted services like iMessage "texting," but there is a world of difference between sending an SMS message and using iMessage to send an end-to-end encrypted message.

Broadly speaking, SMS messages have *no* security. They can be trivially intercepted, tampered with, and forged. (One major

advantage of encrypted messaging is that it makes forgery and message-tampering just as impossible as interception.)

SMS messages are playgrounds for all kinds of bad actors who wish to do you serious harm, from the phishers who intercept SMS-based two-factor authentication messages and hijack your crypto wallet, to the identity thieves who forge SMS messages from your loved ones to you. Everything about SMS is unacceptably terrible, right up to SS7, the billing and logistics back end, which allows stalkers, cops, bounty hunters, and anyone else with a little technical knowledge and a few dollars to trace your location in near real time.

So there's a good reason to get everyone the hell off SMS and into some kind of modern, encrypted, secure messaging service.

To its credit, that's exactly what Apple has done. If you're an iPhone user and you send another iPhone user a "text message," by default that is seamlessly transformed into an iMessage\* that is encrypted in your device's storage, encrypted in transit to your friend's device, and encrypted on that device's storage after it is received.

But what if you want to communicate with someone who doesn't use an iPhone? That's about half of Americans, and about 70 percent of mobile users worldwide. Your message goes out over SMS. Terrible, terrible SMS.

This is bad for everyone, including Android users with iPhone-using friends, *and especially* iPhone users with Android-using friends. The fact that there is no iMessage for Android means that there is a fifty-fifty chance that, if you're an American iPhone user, anytime you send a text message, you have *no* protection against interception, forgery, or in-transit alteration. Worse, if you add a *single* Android user to an iMessage group

\* Technically, an "iMessage message."

chat, *all* the messages within that group are sent without *any* protection.

Why would Apple do this? It's not that it's technically challenging to create an Android app that can send and receive iMessages. Think back to page 133 and the inescapable reality that every computer is a Turing-complete, universal von Neumann machine. That means that every program that can run on an iPhone can run on an Android device and vice versa.

The reason to block iMessages on Android, and to expose every Apple customer in the world to completely avoidable, absolutely terrifying security risks, is right there in Tim Cook's zinger to LiQuan Hunt: "Buy your mom an iPhone."

By downgrading the security of Apple customers who have friends who use a rival product, Apple hopes to recruit its customers to serve as high-pressure sales agents for its products.

In other words, Apple is making its service worse for its customers in order to benefit its shareholders. Or, put more plainly, Apple enshittified iMessage.

This is exactly the sort of place where interoperability can play a key disenshittificatory role. By reverse engineering iMessage, an Android developer can make an iMessage-compatible app for Android, and give all mobile users—whether they have an iPhone or an Android phone—the security they deserve.

And that's *just* what happened. In 2024, a teenager named James Gill put the iMessage app up on his metaphorical workbench, pried its metaphorical case open, and figured out what made it metaphorically tick.

This is—to use one of Steve Jobs's favorite phrases—*insanely great*.

It's also extremely funny. Apple argues that all the locks it puts on and around its devices—its ecosystem, its low-level bootloaders, its hardware secure enclaves, its App Store—are there to keep

its users secure, and not just to provide rent-extraction opportunities for a \$3 trillion multinational corporation.

And yet all of this security was swiftly defeated by a teenager! It's a stinging rebuttal to anyone who dismisses adversarial interoperability as a waste of time because no one can possibly hope to win a technical throwdown with a Big Tech company. It's also a sterling affirmation of the truism that one should "never underestimate the determination of a kid who is time-rich and cash-poor."<sup>\*</sup>

Gill's sweet hack did not go unnoticed. One person who took particular interest was Eric Migicovsky, the CEO of Beeper, a company that specialized in interoperable "bridges" between different messaging tools. Beeper had a mixed reputation in the security community thanks to its reliance on a strategy called man-in-the-middle.<sup>†</sup>

Beeper maintained a data center full of Mac Mini desktop computers, running in "headless" mode (that is, without any screens). These headless Macs ran copies of Apple's iMessage desktop software, which received and decrypted iMessages from iPhone users, then re-encrypted them and passed them on via Beeper's own app. This was *not* end-to-end encryption, and it (rightfully) drove privacy and security advocates nuts. As far as they were concerned, Beeper was putting its users in harm's way, lulling them into the false sense of security that comes from *thinking* your messages are secure and private, when in actuality anyone who can pressure, hack, or trick a small, resource-strapped startup into compromising its systems can gain access to all of them.

But Gill's discovery meant that, finally, Beeper *could* offer

<sup>\*</sup> Cory Doctorow, *Little Brother* (Tor Teen, Tom Doherty Associates, 2008).

<sup>†</sup> A more up-to-date, less gendered name for this is *machine in the middle*.

end-to-end messaging for Apple users who wanted to use iMessage to talk to Android users and vice versa. They released a new app, called Beeper Mini, that gave Android users the coveted “blue bubble” (which adorns each party to an iMessage chat who is using an Apple device) and, more important, gave Apple’s customers the privacy and security that Apple had denied them.

A small but vocal minority of Apple users were outraged by this. Apple has mastered the bizarre trick of convincing its customers that the act of purchasing consumer electronics from a \$3 trillion company makes you a member of an oppressed religious minority (they don’t call it the “Cult of Mac” for nothing), and Beeper Mini constituted an act of blasphemy.

These users insisted, and continue to insist, that Apple customers don’t want iMessage clients for Android, that they’re happy only talking to other Apple customers. Meanwhile, the fact that innumerable—billions of—other Apple customers manifestly and demonstrably *do* want to securely communicate with Android users over the default iPhone messaging app is irrelevant. Those people, say the Apple users, are doing it *wrong*.

The argument goes like this: “When you bought an iPhone, you knew—or should have known—that the deal was that you could only use it in ways that Apple permitted. This has been the deal since the first iPhone went on sale, over a decade ago, and if you can’t live with that, you should not have bought an iPhone.”

But there’s a pretty devastating counterargument to this: “When Apple decided to sell iPhones, it knew—or should have known—that selling goods to a customer transfers ownership to that customer. Once I acquire lawful title to an iPhone, it’s none of Apple’s business how I use it, because it’s mine. This has been the deal since private property rights were invented, over a millennium ago, and if Apple can’t live with that, it shouldn’t have sold me an iPhone.”

For weeks, Apple and Beeper Mini played a game of cat and mouse, as Apple tried to patch all the different exploits that Gill and the Beeper team had discovered. Eventually, Beeper Mini threw in the towel; it had been acquired by Automattic, the open-source company that makes WordPress, and had other mice to catch.

Meanwhile, the European Union has ordered giant “gatekeeper platforms” to open up their messaging services to third parties, like Beeper, under the terms of the Digital Markets Act. And Apple experienced some mix of shame (at the negative publicity over the Beeper skirmish) and dread (at the prospect of EU regulation) and voluntarily added support for RCS—a secure messaging protocol that comes standard on Android—to iMessage, giving Apple customers the security and privacy they should have had from the start.

## Repealing the Law of “Felony Contempt of Business Model”

Intermediaries rely on a tangle of overlapping IP laws to usurp and control the relationships of buyers and sellers, service providers and customers, cultural workers and audiences, politicians and voters, and families and communities. It will be the work of decades to pass laws reforming copyright, patent, anti-circumvention, trade secrecy, contract law, trademark, and all the other policies that stand in the way of interoperability as a means of giving users immediate relief from oppressive rent-seeking middlemen.

But that’s not to say we shouldn’t try—and we are trying. One area where interoperability has made enormous progress is right-to-repair laws enacted at the state level.

In the 2010s, repair advocates, organized under the Digital Right to Repair Coalition umbrella, authored model legislation that was introduced in dozens of states, only to be thwarted by a powerful coalition of giant manufacturers, from Big Car to Big Tech. Apple led the charge to kill these bills, backed by everyone from John Deere to GM to Wahl. The latter, the hair-clipper giant, had lately redesigned its clipper blades with spring-loaded booby traps. If you took apart the blade to sharpen it, the housing would fly apart into several pieces, and there was no way to reassemble it short of mailing your clipper back to Wahl and paying for sharpening.

But in the 2020s, the dam broke. It’s hard to say why: perhaps it was the lockdowns and supply-chain shocks that made the

public and lawmakers more alive to the risks of anti-repair design. Maybe people just got fed up with being ripped off.

Whatever the reason, right-to-repair laws have been passing at the state level, amid smart tactics from repair advocates, who have split the anti-repair coalition by introducing domain-specific repair laws, rather than going after across-the-board repair rights.

The turning point came during the 2020 elections, when Massachusetts repair advocates won a commanding majority for a ballot initiative, Question 1, that safeguarded automotive right to repair. Under Question 1's language, automakers would be obliged to provide diagnostic codes and other digital tools to independent mechanics. In the run-up to the election, the big automakers blanketed the Bay State with scare ads about all the dangers drivers would face once anyone could work on your car. One of these ads depicted a shadowy figure following a woman to her home, ending on a freeze frame as she turns over her shoulder and begins to scream. Right to repair will *kill you!*

The automakers' pitch was that they had transformed their products into rolling surveillance platforms that gathered and stored so much information about their owners as to constitute a lethal risk. There's some truth to this: In 2024, Mozilla Labs surveyed the privacy policies and practices of every carmaker and concluded that, from a privacy perspective, no car currently being manufactured was safe. (Mozilla also revealed some of the very weird lies that carmakers told to data brokers about which information they held on drivers, like Nissan, which promised that it could supply data about the *smells* present inside its drivers' cars. Needless to say, Nissan has none of this data—gas chromatographs do not come standard in Nissan's cars. The company was just treating the ad brokers with the same contempt they exhibit for their customers when they spy on them. There is no honor among thieves.)

But the answer to “Your car is a rolling surveillance platform full of so much compromising data that anyone who can access its internal systems could *murder you*” is simple: your car should stop spying on you. That would actually *work*, unlike Big Car’s answer, which is “Data should be accessible only to giant car companies and anyone who will buy it from us.”

The Massachusetts Question 1 automotive repair initiative passed with a *massive* majority (74.97 percent!), but it still hasn’t taken effect, thanks to successful courtroom delaying efforts by Big Car. Even so, the idea of establishing right-to-repair laws spread to other states.

In New York State, an electronics right-to-repair law passed in 2024, only to be neutered by Governor Kathy Hochul in a signing statement that ripped the guts out of it. (Note to New York transit activists who are still salty about Hochul unilaterally diminishing NYC’s hard-fought congestion charge from \$15 to \$9 at the last minute: we feel your pain, and your enemy is our enemy.)

But repair advocates are tenacious, and their tenacity is paying off. In 2024, Colorado passed the nation’s first powered wheelchair right-to-repair law, which is notable for three reasons: First, it actually *passed*, without being assassinated as it crossed the finish line. Second, it addressed the absolute catastrophe that is powered wheelchair repair, a complicated mess composed of terrible federal procurement rules. (Medicare pays for chairs only rated for *indoor* use, and only from the lowest bidder, which practically means one of two private equity-backed monopolists that have gutted their repair divisions.) Third, it simply *banned* the use of parts pairing and other DRM in powered wheelchairs sold in Colorado. States can’t fix DMCA 1201 and its prohibition on reverse engineering, because that’s federal law, but they *can* order companies not to use technologies that enable them to invoke DMCA 1201 within state lines.

Colorado's prohibition on DRM found its way into a 2024 Oregon right-to-repair law, one that covers broad swaths of consumer electronics. The Washington statehouse passed its own version of this law this spring. More state legislatures are teeing up similar rules in the sessions to come.

This sets up a cool dynamic, where every state has its own unique repair law, forcing national companies to follow a complex and confusing patchwork of laws, which has the reliable effect of turning these companies into advocates for a *national* repair law, one that covers every state. These companies would prefer *no* law at all, but if they *must* have a law, they'd like to have it come out of Congress, since they reckon they can corrupt one national legislature more readily than fifty state legislatures.

All this is to say that after more than a decade of trench warfare holding action in the repair wars, things are finally starting to move. And with the European Union passing its own far-reaching right-to-repair legislation, manufacturers are increasingly required to either sell repairable goods all over the world or endure the cost, complexity, and risk of producing different models for the EU market and for everywhere else. So far, the picture is looking very good: When the EU ordered Apple (and everyone else, but Apple is a uniquely bad actor here) to standardize a USB-C charger port, Apple switched *all* its iPhones to USB-C. Apparently, producing a USB-C phone for the EU and a different one for everywhere else is too expensive, even for a company as stubbornly proprietary and rent seeking as Apple.

Other legislatures are still groping their way to repair-friendliness. As a Canadian, I am simultaneously proud and ashamed to say that in November 2024, Parliament passed two bills that provide for far-reaching repair and interoperability rights: C-244 and C-294. (Note to Americans: Your charming custom of putting the nation's top political science graduates

to work for a yearslong apprenticeship consisting primarily of thinking up cute acronyms for their bosses' legislative proposals is not widely practiced elsewhere.)

This is *great* . . . but there's a catch. Canada has its own version of DMCA 1201. Known as Bill C-11, this anti-circumvention law was shepherded through Parliament in 2012 by Heritage Minister James Moore and Industry Minister Tony Clement (the latter of whom is a disgraced sex-pest whose political career ended when he sent pictures of his erect penis to a young woman who turned out to be a pair of extortionists from Côte d'Ivoire).

Bruce Lehman got the DMCA passed in the United States in 1998, when the internet was relatively obscure and few people were paying attention to tech policy questions. But by 2010, we'd had more than a decade of experience with anti-circumvention law, and Canadians were virulently opposed to the introduction of their own Made-in-Canada anti-circumvention law. Clement and Moore consulted on the proposal and were inundated with objections. By the time the consultation ended, 6,138 Canadians had written in to oppose it, while 54 wrote in support. Faced with this total rejection, Moore deployed a shrewd gambit: he dismissed the bill's opponents—me included—as “radical extremists” and said that he would disregard their “babyish” views.

As with DMCA 1201, Bill C-11 comprehensively prohibits the distribution of circumvention devices. (See the discussion of “use exemptions” and “tools exemption” on page 287 for more on this.) That means that Canada's new legislation grants Canadians the right to modify their devices to make them interoperate and in order to repair them, but it denies them the tools they'll need to exercise these rights. Womp womp.

The repair movement is an example of how creating a coalition around a broad issue—repair—that then fights together for narrow victories (wheelchairs, cars, electronics) can break through

the incredible lobbying power of giant monopolists. Working at the state level, repair advocates are creating a patchwork of policies that can only really be satisfied by wholeheartedly supporting repair in every way. They can thus bypass a hostile White House and Congress but still be able to work with federal agencies when those agencies come on board.

I think interoperability's future lies in this strategy. Manufacturers' war on interop tempts them into such baroque, odious scams that we have our pick of wedge issues.

For example, a "right-to-print" campaign could target the ink rip-offs used by printer manufacturers, banning them from selling printers that take measures to block third-party ink, requiring them to provide diagnostic codes needed to fix busted printers, and the unlock codes needed to roll back fake "security updates" that break compatibility with rival ink cartridges.

A "right to unlock" campaign could force manufacturers to provide the keys and codes needed to keep gadgets running if the manufacturer stops supporting them or goes out of business. States could ban manufacturers from locking customers to specific app stores, servers, or other proprietary code and services.

Such campaigns wouldn't just represent bids for narrow sets of rights; they'd be a way to normalize the idea that if you buy something, it's yours, and you should have the final say as to how it works, even if the manufacturer would rather you organized your affairs to its shareholders' benefit. Each victory would radicalize more partisans to the cause of technological self-determination and create a hostile, difficult-to-navigate regulatory environment for would-be enshittifiers.

Best of all, the right to self-help would also create resilient communities, where local businesses build software and provide repair and upgrade services to their neighbors, and create a partisan army for expanding and protecting interoperability.

Ironically, Trump's trade wars have opened a new front in the interoperability wars. Many other countries have adopted anti-circumvention rules patterned after the US DMCA 1201, under pressure from the Office of the US Trade Representative, which made adopting US IP laws a condition of trading with the United States.

During Trump's first term, his trade negotiators ripped up the North American Free Trade Agreement (NAFTA), which had been in place since 1994, and replaced it with the United States–Mexico–Canada Agreement (USMCA). Under the USMCA, both Canada and Mexico are obliged to pass and enforce anti-circumvention laws, and in exchange, both countries get tariff-free access to US markets.

When Trump threatened to impose a 25 percent tariff on goods from Mexico and Canada, leaders in both countries mooted their own retaliatory tariffs on US goods. Canadians liked the sound of giving Americans a black eye, but it's a sure bet that once they find themselves paying *far* higher prices for the US goods they rely on, they'll lose their enthusiasm. If there's one political lesson from 2024's wave of elections in which incumbent parties were enthusiastically voted out of power, it's that voters do not like politicians who preside over a rise in prices.

Rather than imposing retaliatory tariffs on Trump's America, Canada could—and should—repeal its anti-circumvention law, and empower Canadian companies to make interoperable goods and services, from third-party printer cartridges, to independent app stores for phones and games consoles, to universal diagnostic tools for cars and tractors. That way, Canadians would pay *less* for the apps, repairs, parts, and services associated with their digital technologies, and America's most profitable companies would be directly punished with competitors who attacked their

most profitable lines of business, the enshittified after-market services and junk fees that really screw us all.

The final edits for this book were delivered in early June, just days after the US Court of International Trade ruled that most of Trump's tariffs were illegal, and just days before the DC circuit court's deadline for briefs for Trump's appeal of the decision. If Trump loses that appeal, he's vowed to take his case to the Supreme Court, which has grown so bizarre and dysfunctional that it's hard to guess what will happen next.

But even in the event that Trump is prohibited from carrying on with his tariffs, even if he has a public change of heart and promises to do away with *all* of his tariffs forever, the rest of the world should not and will not believe him.

Trump has forever shattered the international system of trade, and, in so doing, he has destroyed the US trade representative's most effective tool for getting other countries to pass pro-enshittification laws: the threat of tariffs for noncompliance.

There is no reason for any country, anywhere, to keep anti-circumvention (that is, pro-enshittification) laws on their books. The first country that dares to abolish these laws could set in motion a revolution in technology, one that treats the billions in monopoly rents that US Big Tech has extracted from the rest of the world as a disposable rocket stage that boosts its domestic tech sector into a long-term, stable orbit as a global powerhouse of dis-enshittification tools that the rest of us will greedily buy and use.

The audience for these tools is truly global, and it includes Americans, who, after all, were the first victims of Big Tech's scams and privacy invasions. If Canada can export reasonably priced pharmaceuticals to Americans, then Canada (or some other country) could also export the tools of technological self-determination to any American with a credit card and an internet connection.

Happy Liberation Day, everybody!

## Restoring Labor

William Gibson famously said, “The future is here. It’s just not evenly distributed.” This is usually interpreted to mean that sharp-eyed observers can find little bits and bobs of gleaming new technology seeded around their surroundings, like a kid on a solar-charged e-bike bombing down a gravel road with a cargo box full of COVID vaccines in a region where no one has running water or grid electricity.

But I know Bill, and there’s no way that his unevenly distributed futures are exclusively utopian. Gibson is a man who is uniquely and brilliantly attuned to all the ways that technology can go horribly, lavishly wrong.

Here’s how I think the future’s uneven distribution goes: I think all the worst technologies appear first among the least socially powerful among us, and then work their way up the privilege gradient until we’re all struggling under them.

I call this the “shitty technology adoption curve.” If you’re a bright tech entrepreneur with a terrible idea that will make people’s lives miserable, you can’t just inflict it on someone like me, a middle-aged, middle-class mouthy white guy. I’ll scream bloody murder.

So you start with prisoners. Asylum seekers. People in mental institutions. Parolees. Then it’s schoolkids, people on welfare, gig workers. Then it’s college kids, interns, Medicare recipients, blue-collar workers, bottom-rung white-collar workers. At each stage,

all the rough edges of the terrible new technology are sanded down on the bodies of its victims, and the depredations that can't be softened are instead normalized, one group at a time.

Eventually, the shitty technology comes for us all, working its way past middle-class writers and white-collar workers, all the way up to the C-suite. Twenty years ago, if you found yourself eating your meals under the unblinking eye of a CCTV camera, it was because you were an inmate at a supermax prison. Today, all it signifies is that you were unwise enough to buy a “smart” home camera from Apple, Google, or (God help you) Facebook.

Tech workers enjoyed decades of absolutely top-tier workplace conditions. A tech industry “campus” had many perks: free gourmet meals, day-care facilities, gyms, laundry services—all the mom-for-hire comforts that were lampooned in shows like *Silicon Valley*. Tech bosses didn't lavish these extras on tech workers out of affection: it came out of a cold-blooded calculation that tech workers were very hard to replace, and in enormous demand, so they had to be kept happy or they might defect to a rival.

But tech workers aren't the only workers tech bosses employ—indeed, they represent a tiny slice of a typical tech business. From Amazon's warehouse workers and delivery drivers to Facebook's overseas content moderators to Apple's Chinese factory workers, the largest tech workforce labors under some of the *worst* conditions of *any* workers in *any* sector.

Amazon's warehouses have the highest rate of on-the-job injuries—including serious injuries, even maimings—of its industry. As discussed on page 120, Amazon drivers are put on quotas so punishing that they piss in bottles and defecate in bags. Their eyes and mouths are constantly monitored by “AI” cameras, and they are disciplined for not looking where the camera

thinks they should be, or for singing along to the radio (“distracted driving”).

The reason Jeff Bezos and Andy Jassy treat Amazon coders well and treat Amazon drivers and packers horribly is not that they are sentimentally attached to the one group and contemptuous of the other. The reason Amazon coders get to show up for work with pink mohawks, facial piercings, and black T-shirts with weird slogans their bosses don’t understand is that their bosses are afraid of them.

The future of those coders is here; it’s just not evenly distributed yet. If you want to know how Amazon will treat its coders once they can be readily replaced, just look at Amazon warehouse workers and drivers. They’re the early adopters of Amazon’s preferred labor conditions. There’s no reason coders can’t piss in bottles.

For a man with a dick-shaped rocket, Jeff Bezos sure has an abiding hatred of our kidneys.

Apple CEO Tim Cook has a reputation for being a kind of cuddly tech boss who stands out from the pack. But the reason Apple’s board picked Cook to replace cofounder Steve Jobs after he juice-cleansed his way into an early cancer death wasn’t Cook’s sunny disposition.

As I discussed on page 291, Cook’s signature achievement prior to his elevation to CEO, the deed that led to his accumulation of more than \$2 billion in personal wealth, was figuring out how to offshore Apple’s production to factories in China. This involved establishing labor oversight and discipline in those remote Chinese factories that was so overwhelming and brutal that Foxconn, Apple’s primary contractor, had to install suicide nets around the factories in “iPhone City” to catch workers who leaped to their deaths rather than face another day on the job.

We don’t have to speculate about how Tim Cook treats

workers he's not afraid of. The suicide nets have settled the matter. This is what Apple's tech workers can look forward to, once Tim Cook is no longer worried about replacing them.

The bad news is that tech has resolved its labor scarcity problem. As I noted earlier, the US tech sector fired 260,000 workers in 2023. In the first half of 2024, another 100,000 tech workers joined their unemployed colleagues on the breadline.

The scarcity that was at the root of tech workers' power has ended, and their power has evaporated. Scarcity-based labor power is always temporary, and bosses do everything they can to hasten its end, from demanding a halt to COVID relief checks in a bid to force more workers into the labor market, to hiring undocumented immigrants or children, to offshoring.

Throughout labor history, there's only ever been one mechanism that working people could use to protect their pay and working conditions, through times of labor scarcity and labor supply: unions.

Unionization has been in retreat for forty years—the same period during which antitrust law was in its induced coma. The same people who killed antitrust also killed unions: the neoliberal economists who have served as court sorcerers to presidents—Republican and Democrat—since Reagan.

And just as antitrust is enjoying a global revival, so, too, are unions. The favorability numbers for unions among Americans have attained heights not seen in generations, and more American workers than ever want to join unions.\*

Paradoxically, union membership is still falling. That's down to bad union leaders—the kinds of union leaders you'd expect to find occupying leadership roles after decades of union collapse.

\* "From Businesses and Banks to Colleges and Churches: Americans' Views of U.S. Institutions," Pew Research Center, February 2024.

These are the union bosses who signed off on “two-tier” contracts that reserved union benefits for the most senior workers in the shop, while still requiring new hires to pay dues to a union that negotiated contracts that denied those workers any protections. If you wanted to design a union contract that systematically destroys solidarity among workers, you could not do any better than this.

American unions have bank balances that are at historic peaks, but they spend less on union organizing every year. This *must* change.

America’s biggest unions squandered a historic opportunity under Joe Biden, whose National Labor Relations Board was more sympathetic to workers than any NLRB since the New Deal. The fact that American labor entered the second set of Trump years with *fewer* unionized workers than existed at the start of the Biden years is grotesque. The labor leaders who sat out a once-in-a-generation opportunity to unionize millions of Americans *begging* to join up are worse than useless. We need to occupy our unions and get rid of these bastards.

That’s happening. A little. Since the COVID pandemic, some of America’s biggest, most corrupt, most stagnant unions have held their first free and fair leadership elections in living memory. The most notable success story here is the UAW, which, as its website notes, is “one of the largest and most diverse unions in North America.” No longer just an autoworkers’ union, the organization has members in a broad array of economic sectors.

The story of how the UAW finally threw out its corrupt, barnacle-suctioned old guard and elevated the firebrand Shawn Fain to its presidency in 2023 is instructive. UAW reformers helped organize an unlikely shop: Harvard’s grad students, who struggle to survive in a precarious and brutal workplace, with an employer sitting on untold billions. (Not for nothing is Harvard

referred to as “a hedge fund with an inconvenient university attached to it.”) The newly unionized Harvard kids memorized the entire UAW rulebook, analyzing it and planning strategy. At the leadership conference in 2023, these new UAW members served as a defensive line for the reformers. Every time the old guard tried a parliamentary trick to either call or delay a vote, or shut down a meeting or a line of questioning, one of these Harvard kids would pop up from the audience to give a chapter-and-verse explanation of why the move was illegal, over and over, until the UAW found itself holding the first fair election in decades.

When the dust settled, Shawn Fain was president and he led the union to an unprecedented simultaneous strike against all of the Big Three automakers, shutting down US car production. After six weeks on the line, all three employers had capitulated, and the autoworkers had new contracts.

These contracts are noteworthy not merely for the protections they offer to workers—just as interesting is the fact that these contracts all expire in 2028.

In fact, Fain has called on *all* US unions bargaining for a new contract to set a 2028 expiry date. That way, every union in the United States will be able to go on strike simultaneously: a general strike. This is a very clever hack around the Taft-Hartley Act’s prohibition on sympathy striking, and the fact that the strike is set to arrive in the midst of the next presidential election is especially important.

Organized labor has a long history of successfully resisting fascist and cryptofascist regimes. (There’s a reason fascists attack unions as soon as they take power.) The current labor surge dates back to the first Trump administration, when teachers across the United States walked off the job in a wave of #RedForEd strikes that won historical gains for teachers and their communities, with

contracts that reached far beyond the economic welfare of teachers and into key justice issues for the communities they served.

For example, the Los Angeles teachers' strike not only won wage and working-conditions concessions for teachers; it also won significant gains for human rights (a ban on ICE patrols scooping up parents at the school gates) and environmental justice (money to put a green space on the grounds of, or in the immediate vicinity of, every L.A. school). What's more, the teachers who were unified by that strike also turned out door-knockers and organizers who delivered swing seats to the Democrats in 2018, securing a congressional majority.

Unions get stuff done, even in the midst of authoritarian chaos and crackdowns. If teachers can use labor organizing to secure gains for their students' families and communities, tech workers can use labor organizing to secure their users' interests. Disenfranchisement can be a union demand.

To the extent that tech workers have addressed these issues in their workplace, it has been through social movements, not labor organizing. Social movements do important work; I've devoted most of my life to them. But social movements tend to thrive under liberal regimes, even when those regimes let down their goals.

Think of how Black Lives Matter and Occupy arose under Barack Obama. His administration was hardly a friend to working people, but it didn't threaten daily survival the way the Trump administration did. People who tried to form social movements under Trump—like the Women's March—found themselves splitting their time between just trying to get through the day and trying to hold Trump's feet to the fire.

Labor organizing produces institutions, solidarity, and mutual aid—everything from strike pay to communications infrastruc-

ture. Rebuilding worker power and bringing it to the tech sector is a big project, but support for unions and worker interest in joining unions has never been higher. The future is there for unions, if we want it.

Not every union is well managed, and union leaders can undermine their members' interests in many ways. It's not just the naked corruption of the old guard at the UAW.

In 2022, the Communications Workers of America (CWA)—which had made excellent inroads organizing tech workplaces—endorsed the controversial merger of Microsoft (a convicted monopolist) with the gigantic and notoriously brutal Activision Blizzard (an unconvicted monopolist). The union did so after Microsoft promised “nonaggression” toward organizers seeking to sign up the downtrodden workers of the games industry, whose workplace depredations are legendary.

This was a gross miscalculation. The Microsoft/Activision Blizzard merger significantly reduced competition in the already concentrated games industry—a massive industry that out-grosses movies, music, and TV *combined*.

CWA leaders assumed that Microsoft would keep its word. This was a naive assumption indeed—Microsoft is too big to fail, which means it's too big to care. Within months of the merger's completion, Microsoft had taken an axe to Blizzard's ranks, mass-firing workers, including those who were undergoing union drives. Womp womp.

Unions don't just represent the workers who pay their dues; they represent *labor*, in solidarity, against the forces of capital. To effectively support their members, unions can't confine themselves to fighting the employer—they have to fight *corporate power* itself.

Unionizing tech workers is a big lift, but tech labor organizers—

like the people doing excellent work at Tech Solidarity and the Tech Workers Coalition—aren't on their own. There's a huge wave of unionization waiting to happen, at all kinds of workplaces, and each successful union drive and strike helps every drive and strike that comes after.

In 2024, the legendary union organizer Jane McAlevey died of cancer. McAlevey was a devastatingly effective union organizer. She was trained by organizers who came down in a direct line from the activists working in the years when unionization was criminalized and union organizers faced violent retaliation, prison, and even assassination.

McAlevey never tired of reminding workers that the legal support for unions, including the National Labor Relations Act, came *after* years of ultimately successful union organizing. Labor law exists because unions demanded it. Labor law didn't make unions—first we got unions, *then* we got labor law.

In the first week of his second term, Donald Trump effectively shuttered the NLRB, violating procedures by firing a Democratic board member named Gwynne Wilcox, leaving the NLRB without a quorum, unable to make new rules or pursue new investigations or enforcement actions. He also killed all *existing* NLRB enforcement actions and investigations, effectively mothballing the agency.

But Trump made a mistake. He thinks that by getting rid of the referee, he can halt the game. But all he's done is get rid of the *rules*. The NLRB didn't just limit what bosses could do to workers—it limited what workers could do to *bosses*. The era before the NLRB was a time when bosses scurried from their mansions to their fancy restaurants to their opera boxes surrounded by armed guards. It was a time of bombings, arson, and firefights. The aphorism “War is politics by other means” (a loose translation

of the military theorist Carl von Clausewitz's words) has a corollary: Politics is war by other means. The labor wars were turned into a long peace thanks to the NLRB. Now it's war. Again.

We did this in living memory, right around the time we came up with antitrust law and smashed the empires of the likes of John D. Rockefeller. It's no coincidence that these two accomplishments happened in parallel. Both unions and trustbusting are examples of working people using democratic means to rein in the undemocratic, autocratic power of corporations and the ultrarich.

It's true that, on the way, the wealthy have used antitrust law to target workers: over and over again, bosses sued their workers for forming unions on the grounds that this was a form of price-fixing for wages that violated antitrust law. Often, these bosses prevailed, despite the fact that this theory had no connection to the actual text of the laws.

Antitrust in the United States has *always* been targeted at corporate *power*. This has been true since the year dot. Senator John Sherman, he of the Sherman Act, famously said in support of his bill: "If we will not endure a king as a political power we should not endure a king over the production, transportation, and sale of any of the necessities of life. If we would not submit to an emperor we should not submit to an autocrat of trade, with power to prevent competition and to fix the price of any commodity."

Indeed, the history of antitrust law essentially consists of Congress sitting down every decade or two to pass a new antitrust law explaining in extremely plain language that it intends for antitrust to be used against corporations, but not their workers. In the memorable words of Democratic congressman Thomas Konop in 1914, "We are aiming at the gigantic trusts and combinations of capital and not at associations of men for the betterment of their condition. We are aiming at the dollars and not at men."

Konop was speaking in favor of the Clayton Act, a successor to the Sherman Act that was largely motivated by willful judicial misinterpretations of existing law. Judges misapplied the Sherman Act to crush a Pullman Porters strike led by Eugene V. Debs in 1894 and a Danbury, Connecticut, hatters' unionization drive in 1902.

The drafters of the Clayton Act took enormous pains to make it clear that they were "aiming at the dollars and not at men," and that the law did not apply to union organizing or union action. The Clayton Act explicitly permits workers to form unions, call for boycotts, and organize sympathy strikes. Despite this, the courts allowed bosses to use the Clayton Act to shut down 2,100 strikes in the 1920s.

This so infuriated Congress that it passed *another* law, 1932's Norris-La Guardia Act, whose congressional record includes a spitting-mad Fiorello La Guardia fulminating on the floor about judges who "willfully disobeyed the law . . . emasculating it, taking out the meaning intended by Congress, making the law absolutely destructive of Congress's intent." The final text of Norris-La Guardia explicitly repudiated every argument judges used to apply the Sherman and Clayton Acts to labor action, and despite this, in 1942, a federal court decided that since the fishermen in the case *Columbia River Packers v. Hinton* were selling "commodities" (as opposed to labor), it could apply Norris-La Guardia to smash a strike.

This continued through the ages—all the way up to 1999, when the FTC used antitrust law to attack truckers in the port of Los Angeles.

It's doubtless cold comfort for workers whose labor grievances are steamrolled by antitrust law to be told that the law was misapplied, but that doesn't make it untrue. And law need not be misapplied. By 2016, workers were able to get judges to actually

read the law and defend their rights, when, for example, jockeys in Puerto Rico got Judge Sandra Lynch of the First Circuit Court of Appeals to reverse a Clayton Act decision against the jockeys, who had been ordered to pay fines to their bosses as a penalty for organizing a union. (The lower court had even allowed the jockeys' bosses to go after their workers' *wives* for damages.) Lynch correctly determined that the Clayton Act expressly *protected* the jockeys' right to organize.

A corrupt administration or a corrupt judge will always find a reason to attack workers. That's why worker power always starts with *workers*, not with the law. Solidarity will get you through periods of legal attacks on unions more than the law will get you through periods of no solidarity.

But when administrations and the judiciary *are* on the side of labor, strong antitrust laws that attack corporate power at its root, that attack John Sherman's "autocrats of trade," are a powerful force to reduce the power of corporations, which makes it easier for labor to come out on top.

# There's Bad News and There's Good News

This is an unprecedented moment for the war on corporate power. While previous waves of resistance to “autocrats of trade” have occurred in nations or even regions in years gone by, there has never been a *global* movement like the one that is surging today.

All over the world, there is muscular action underway to restore competition, regulation, interoperability, and labor power, which is good, because at the same time, all over the world, we are experiencing an unprecedented wave of enshittification, too.

## The Bad News

We are living at the confluence of two long-term trends that used to run in parallel and that are now reinforcing each other, with disastrous results that just keep getting worse.

First, there is the trend to market consolidation across *every* sector, from automobiles to white goods, from groceries to meat-packing, from energy to sea-freight, and beyond. Sector by sector, the global economy has collapsed into inbred cartels. These cartels are insulated from competition, they capture their regulators, and they lord their power over their workers. In other words, they are ripe for the enshittification practices of price gouging, deception, and out-and-out fraud.

The only saving grace here is that the cartels operate mostly in hard goods industries, which means that they can't take advantage of the flexibility that digital platforms use to twiddle their customers and sleaze their way through endless rounds of Darth Vader MBA deal-altering.

But that's changing—due to the second trend.

The Trump toady, tech authoritarian, and cryptocurrency hustler Marc Andreessen once famously quipped that “software is eating the world.” Andreessen was (as usual) wrong. Software's effects are primarily focused at the other end of the world's alimentary canal: software isn't *eating* the world; it's enshittifying it.

A better prophet to listen to is, as ever, William Gibson, each of whose quips is worth a dozen Andreessen aphorisms. (See page 307, where I discuss “The future is here. It's just not evenly distributed.”) From Gibson's 2007 novel, *Spook Country*, we get the ominous observation that “cyberspace is everting.” In other words, cyberspace (another Gibson coinage) is turning inside out—the phenomena that once only took place *inside* computers are now happening out here, in meatspace, where we keep our meaty bodies.

The “Internet of Things”—the world of “smart,” networked devices that was touted in the early 2000s—has decayed into the “Internet of Shit,” as one anonymous social media account dedicated to chronicling the terrible world of “smart” appliances has it.

The digitization of every industry opens up new opportunities for twiddling and, with it, intensifying enshittification. Enshittification is coming for *everything*.

Recall the example of grocery stores implementing electronic shelf labels (page 128). When Jeff Bezos, owner of Amazon Fresh (an online grocery store), wants to hike the prices of eggs based on a data-driven hunch that you will pay extra for them, he just moves a slider bar and the eggs are all magically repriced.

Jeff Bezos is also the owner of Whole Foods, a grocery store that is made out of stubborn atoms that we insert our meatbodies into like cavemen. Up until recently, if Jeff Bezos had wanted to reprice everything in a Whole Foods as you wandered the aisles, he would have needed an army of rollerblading teenagers armed with pricing guns.

But add in electronic shelf labels, and everything in the Whole Foods gets hooked up to a slider bar just like the goods for sale in an Amazon Fresh—no teenagers required.

Recall, too, that Norwegian grocers, who lead the world in electronic shelf labels, already reprice their goods *more than two thousand times per day*. They claim that this is done to provide discounts (for example, making milk cheaper as it nears its expiry date), but we all know how this works. Think of your grocery loyalty card (or these days, app), which started off as a way to get a discount when you shopped, but—as competition dwindled—turned into an essential, as the prices of everything in the grocery store went up and the only way to get the regular price was to surrender your privacy and use a store card. The store cards don't provide a discount anymore (if they ever did)—rather, you have to pay a premium for privacy.

It's not just groceries. Cyberspace is everting everywhere. Remember the discussion of automotive right to repair (page 300)? Your car is a rolling surveillance platform that gathers so much information on you that the carmakers themselves warn that anyone who gains access to your car could actually *murder* you.

But all that computation isn't just a way to spy on you—it's also a way to rip you off. Tesla pioneered the idea of a car that had features you couldn't access unless you paid a monthly subscription or onetime unlock fee. Some Tesla automation features (the deceptively named “self-driving” system) have to be bought as monthly subscriptions. Even worse, in some Teslas the *bat-*

*tery* will no longer power your car after it reaches 50 percent discharge unless you pay for it every month. The battery still has a charge; it just refuses to deliver that charge to the car.

Once Tesla opened the door, everyone else got in on the game. Companies like BMW and Mercedes want to rent you the seat heater in your car on a monthly basis, or force you to subscribe in order to access the automatic high-beam dimmers that toggle to driving lights when a car is oncoming.

The story of autoenshittification is also a Shitty Technology Adoption Curve case study: The first drivers to be exposed to remote-control kill switches and overrides for their cars were poor people who took out subprime auto loans. These loans—which come with ultrahigh interest rates, onerous limits on where you are allowed to drive, and remote kill switches that immobilize the car if you miss a payment—were issued by the trillion-dollar load to the poorest, most desperate people in America. Like the subprime loans that triggered the Great Financial Crisis of 2008, these loans were designed to fail, with low “teaser rates” that gave way precipitously to “balloon rates” that borrowers couldn’t possibly pay. And like the banks that offered subprime mortgages, the lenders that originated these loans packaged them up as bonds and sold them off to investors, incentivizing the issuance of loans destined to fail, because when they did, the loan originators (mostly used-car dealers) would no longer be holding them.

Subprime cars are rolling surveillance platforms that could be partially or completely disabled by a distant, uncaring corporation. Hackers who gain access to dealers’ computer networks are able to brick whole fleets of cars at a time. Lenders who are impatient over late payments can activate a secondary stereo system in the car and blare repayment demands through speakers that can’t be silenced or even have their volumes lowered.

The first and second decades of this century saw the proliferation and refinement of these features in clunkers that were routinely repossessed and resold out from under drivers who had no social clout and no chance of recourse when they were treated unfairly.

Now that these features have been refined and normalized, the rest of us have to live with them. All new cars sold today come with surveillance technology that feeds your private information to data brokers. Their diagnostic systems and internal networks are designed to extract rent from you by blocking third-party service and parts. Luxury cars' features are rented, not sold, and the money you invest in after-market improvements to your car is lost because those improvements vanish as soon as title to the car changes.

My own Kia Niro has an app that my family is expected to pay a monthly fee to use. Because we don't pay this fee, we lose remote access to the car's systems—we can't start the air conditioning or heating a few minutes before we leave the house, can't remotely unlock the door or start the ignition without the fob (which costs \$500 or more to replace), can't locate the car if it's stolen or if we forget where we parked it.

But just because *we* can't access our car's network, that doesn't mean *Kia* can't do so. This network from which we are excluded continues to hum along in the background, nonconsensually gathering data on us that is sold to data brokers and will eventually leak onto the dark net.

Cars, bassinets, sous-vide gadgets, insulin pumps—they're all turning into inkjet printers, the most extractive and depressing category of goods imaginable. Printers themselves are getting progressively worse, with HP now routinely tricking its customers into signing up for ink "subscriptions" whose terms of service

allow HP to data-mine the documents you print on them and also brick your printer when the company decides it's time for you to buy a new one.

Cyberspace is everting. The twiddling that was once the exclusive domain of virtual services you access through a screen is now commonplace in physical systems of the world. You routinely insert your body into eminently enshittifiable computers—like a house with a “smart” thermostat—and you are likewise expected to wear these enshittification targets about your body (like the phone in your pocket) or even *inside* your body, like your implanted defibrillator.

That is the bad news.

## The Good News

Now the *good* news.

Remember James Boyle's idea of the word *ecology* as a talisman that catalyzed the formation of a coalition that fused thousands of issues into a single issue (page 254)?

The modern antitrust movement is one part of a broader coalition that crosses borders, ideology, and issues. Antitrust is part of the movement against inequality, corruption, pollution, labor abuses, and discrimination. Antitrust enforcement is surging in the west, the east, the north, and the south.

Long before the United States started to seriously tackle Big Tech, European enforcers were handing out stonking fines and passing big, ambitious regulations. There are geopolitical reasons for this, but this isn't merely down to modern geopolitics.

The fact that EU enforcers could bring action against US companies was no coincidence. European competition law was

modeled on US antitrust law. American technocrats working for the Marshall Plan after World War II installed lightly modified versions of American competition law in the statute books of European nations. After all, the rise of fascism in Europe depended on the support of large German and Italian corporations that saw in fascism an opportunity to fuse their power with the power of the state, to eliminate competition, and to win gigantic war profits. Curbing corporate power was key to preventing the re-emergence of fascism.

So when EU enforcers decided to take on Big Tech, they had a lot of tools at hand—existing legislation that had simply been ignored since the neoliberal turn.

But international enforcers have an advantage that goes beyond a common set of laws, and a common cause in regulating Big Tech. They also enjoy a common set of facts that can be mobilized in cases against multinational tech firms.

The fact that there are broad similarities between the competition laws of the UK, the EU, Japan, South Korea, and other countries means that conduct that violates the law in, say, the UK also likely violates the laws in those other countries.

And since tech firms run the same sleazy enshittification playbook in countries all over the world, a successful case from one country can be filed in many others, relying on the facts and arguments that were developed the first time around.

That's a dynamic that's already playing out. In 2021, the British Parliament passed a bill creating the Digital Markets Unit, a seventy-engineer-strong, tech-focused department of the Competition and Markets Authority (see page 229). The DMU is the best-staffed technical competition unit in the world. Whereas most competition regulators struggle to attract and retain top tech talent who can help them understand the tactics and lies of

tech companies, the DMU is practically drowning in savvy engineers who can cut right through the nonsense and lay out the wrongdoing in pitiless and precise detail.

There was only one fly in the ointment: the DMU was created in the midst of one of the most chaotic periods in British parliamentary history, when the messiness of Brexit saw one prime minister after another defenestrated in a series of constitutional crises in which bill after bill died on the order paper, without receiving a hearing or a vote.

Thus it was that a second bill, intended to give the DMU special enforcement powers that could turn all that engineering firepower into action, failed to pass for three years. (The Digital Markets, Competition & Consumers Act finally became law in 2024.)

This failure to give the DMU enforcement powers could have rendered it a lame duck at best, an expensive boondoggle at worst. But that's not how things played out. The DMU used its investigative powers to compel the participation of the largest tech companies in a series of market studies on topics like the ad-tech market and the mobile computing market, yielding four-hundred-page bricks of damning, footnoted, irrefutable evidence of how Big Tech was rooking the public, small businesses, and governments.

While the DMU wasn't able to act on these insights, it didn't have to. After all, the scams that Big Tech runs in the UK are virtually identical to the scams it had run in the EU.

The EU's enforcers in the European Commission (EC) face the opposite problem of their counterparts in the DMU. While the DMU enjoyed a vast bounty of investigative expertise but an embarrassing poverty of enforcement powers, the EC had all the enforcement powers it needed—but it labored under a punishing shortage of technical advisers who could help it wield those powers.

In a heartwarming show of post-Brexit trans-Channel cooperation, the EC used the UK DMU's market studies as blueprints for enforcement actions in Europe that saw US tech giants like Apple and Google hit with fines running to *billions* of euros. The EC also relied heavily on the DMU's studies in crafting new laws in the form of the Digital Markets Act and Digital Services Act.

But the international cooperation didn't end there. The EU's successful Apple case inspired enforcers in South Korea and Japan—two other countries with broadly similar antitrust laws, thanks to the US Marshall Plan technocrats—to bring their own cases against Apple. Enforcers in both countries were able to recycle the exhibits, internal documents, testimony, and arguments of their EU counterparts to build cases that would otherwise have been prohibitively expensive.

Of course, it didn't hurt that both Japan and South Korea have their own important tech sectors that have been devastated by US-based tech monopolies, which produced a lot of political will for these enforcement actions.

American tech giants commit the same crimes everywhere, including in countries that are too small and/or poor to run their own enforcement actions against them. There's no reason that Japan needs to be the last stop in Apple's long ordeal through the world's regulatory wood chippers. Countries in the global south, in particular, could both nurture a domestic tech sector and bring in much-needed dollars by suing and fining US tech giants.

And now it's Trump's turn. His famously chaotic governance style and self-contradictory bluster make it hard to predict what Trump will do about competition, antitrust, interoperability, and labor law. While it's a sure bet that parts of the Trump agenda will be hostile to workers and friendly to oligarchic firms, it's far from certain that it will be *uniformly* so.

Elements of the Trumpian coalition have spoken in favor of

both labor rights and trustbusting. Biden had to deliver some wish-list items to the corporate wing of the Democrats—like the lifetime appointed federal judge whose son was employed by Microsoft, who proceeded to rule against Lina Khan’s FTC and its attempt to block the disastrous Microsoft/Activision Blizzard merger. Trump will deliver far *more* benefit to his party’s much larger and more powerful corporate wing, but he can’t completely deny the pro-labor, anti-monopoly wing of his party. It’s just too powerful. In the first days of the second Trump administration, his DOJ filed a suit to block the merger of two giant US corporations: HP and Juniper Networks. The anti-monopoly elements in Trump’s coalition will mostly not get their way, because they are not the most powerful bloc in Trump’s power base.

But how powerful are they? Remember that Trump’s vice president, JD Vance, has sung Lina Khan’s praises, singling her out as the best of Biden’s agency heads. Trump’s initial pick for attorney general, Matt Gaetz, calls himself a “Khanservative” and publicly lauded the Biden antitrust enforcers’ ambitious agenda and many victories. Gaetz’s time as prospective AG was short-lived, but it ended because he has been credibly accused of sexually trafficking underage girls—not because his views on antitrust are anathema to the GOP consensus.

And of course, the Google antitrust case *started* under the first Trump administration—and Trump also sued to block the disastrous AT&T/Time Warner merger. Of course, both of these crackdowns were motivated by resentment more than policy: Trump attacked Google as symbolic punishment for the conspiracy theory that Big Tech shadow bans conservatives, and his campaign against Time Warner was payback for unfavorable coverage on CNN.

The fact that Trump’s antitrust actions in his first administration were impurely motivated doesn’t mean that these companies

were innocent. The Google case—carried forward by Biden’s DOJ under the leadership of Jonathan Kanter—resulted in a stunning victory. A federal judge struck down the case against the AT&T/Time Warner merger, but that’s because the judge ignored the text of the law in favor of the precedents set by Chicago-pilled judges who’d been brainwashed at the Manne seminars. (Recall from page 234 that 40 percent of federal judges attended these “continuing education” seminars, which indoctrinated them with pro-monopoly legal theories.)

Time Warner and Google were guilty as hell—as are *all* the monopolists and cartels in the time of late-stage capitalism. Forty years of antitrust non-enforcement has yielded a poison crop of outsized, crooked, inbred companies that are *all* guilty of violating the law.

Combine these facts—powerful antitrust elements in the Trump coalition, Trump’s own propensity for vindictive prosecutions of companies that are insufficiently deferential to his agenda, and a crowded field of companies that have *all* committed multiple violations of antitrust law—and you get a perfect recipe for a fair bit of antitrust enforcement in the second Trump term.

This enforcement will be corrupt in the sense that Trump will be picking the companies that he, personally, hates the most, rather than the companies whose lawbreaking represents the greatest threat to the American public. But it will *not necessarily* be corrupt in the sense that Trump will bring cases against innocent companies. Nearly *all* the big companies are guilty. The corrupt part isn’t prosecuting the companies; rather, the corruption is in which companies he *won’t* prosecute.

Of course, antitrust enforcement will only be a minor side-show in the Trump antitrust agenda. Trump ran on a belligerent isolationism, with high tariffs and an outright trade war against countries whose companies compete with the United States.

As he carries this agenda out—as much as his coalition will permit him to, anyway—he will help build the case for antitrust enforcement and interoperability remedies outside the United States. Whatever deference large powers like the EU have shown to US Big Tech in hopes of maintaining a good working relationship with America will last only as long as Trump’s “America First” agenda doesn’t convince Europeans that they have nothing to gain from maintaining friendly terms with the United States.

Trump’s vow to expand the use of cryptocurrency will only accelerate this phenomenon. Cryptocurrencies are near-perfect vehicles for wild speculation, money laundering, and scams. Expanding their centrality to the US economy will precipitate the kinds of crises that previous speculative bubbles caused, such as when exotic mortgage derivatives gave rise to the Great Financial Crisis of 2008.

Amid the instability of an isolationist, authoritarian United States lashing out at its enemies and the economic chaos that will arise from turning the US economy into a cryptocurrency casino, there will be motive, means, and opportunity for other countries to develop their own tech tools, networks, clouds, social media, and messaging.

## Conclusion: Is Enshittification Just Capitalism?

A confession: I am no true believer in markets as the best arbiter of how our society should work, who should be in charge of it, and how its productive capacity should be organized. Like other leftists, I am deeply suspicious of capitalism, not least because so many self-professed “capitalists” seem hell-bent on abolishing capitalism and replacing it with feudalism (see page 194).

I understand the temptation to look at all this verbiage about enshittification, throw your hands up, and say, “What do you expect? Capitalism *always* produces these crises of production. *Enshittification* is just a swearsy euphemism for *capitalism*.”

But this is dead wrong. There are meaningful differences between the internet as it stands today—the enshitternet—and the old, good internet we once had.

The enshitternet is a source of pain, precarity, and immiseration for the people we love. The indignities of harassment, scams, disinformation, surveillance, wage theft, extraction, and rent seeking have always been with us, but they were a minor sideshow on the old, good internet and they are the everything and all of the enshitternet.

The old, good internet was not designed or operated by better people. Many of the same bosses who run the enshitternet today presided over the services we once loved and relied upon. The leaders of tech companies have demonstrated time and again

that they lack anything like executive function. There's no way these guys were patiently running a long con, waiting until the perfect moment to spring a trap on us.

No, the Adderall-soaked masters of the universe are doing what they've always done: showing up for work every morning and going directly to the giant ENSHITTIFICATION lever installed in the C-suite and yanking on it as hard as they can.

The difference is that the lever used to be stuck. It was gummed up by competition, by regulation, by interoperability, and by tech workers' power and conscience.

Once competition and regulation were neutered, once interoperability was banned in favor of "felony contempt of business model," once tech workers were cowed and precaritized, the lever started to move very freely indeed.

So those same bosses, with the same moral and psychological flaws, doing the same thing they always have, are producing a wildly different outcome. The enshittification lever that was once stuck fast can now be moved with a fingertip, all the way to 100.

This has real, material consequences for our comrades in the struggle for a better world. The internet that spawned Occupy and Black Lives Matter has become profoundly hostile to the ongoing maintenance of radical political movements and is inimical to the founding of new ones.

That really matters. Not because the internet is the most important issue facing us today. Far from it. Compared with the climate emergency, genocide, inequality, corruption, democratic backsliding, authoritarianism, and the sustained racist, homophobic, misogynist, and transphobic attacks on our comrades, sisters, and brothers, the internet is just a sideshow.

But for all that the internet is far less important to these other fights, it is nevertheless *extremely relevant* to these struggles. The internet is the terrain upon which these fights will be waged. It is

the communications medium that we will use to organize to save our species and planet from their imminent eradication. These other fights are more important to the internet, but we can't win them without a free, fair, and open internet.

An internet, in other words, that is very similar to that old, good internet we once had, but one that corrects its defects—the inscrutable technical details that kept our normie friends from joining the party.

A new, good internet is one that combines the old, good internet's ethic of technological self-determination with the greased-skids simplicity of Web 2.0 that allowed all our normie friends to join the party.

Audre Lorde was far smarter than I am about nearly everything, but when she wrote “The master's tools will never dismantle the master's house,” she was manifestly wrong. The master's tools were used to *build* that house in the first place—that makes them the *ideal* tools to take it to bits and rebuild it to shelter us.

The capitalism of twenty years ago made space for a wild and woolly internet, a space where people with disfavored views could find one another, offer mutual aid, and organize.

The capitalism of today has produced a global, digital ghost mall, filled with botshit, crapgadgets from companies with consonant-heavy brand names, and cryptocurrency scams.

We *can* reverse the enshittification of the internet. We can halt the creeping enshittification of every digital device.

We can build a better, enshittification-resistant digital nervous system, one that is fit to coordinate the mass movements we will need to fight fascism, end genocide, and save our planet and our species.

Martin Luther King Jr. once said, “It may be true that the law cannot make a man love me, but it can stop him from lynching me, and I think that's pretty important, also.”

And it may be true that the law can't force corporate sociopaths to conceive of you as a human being entitled to dignity and fair treatment, and not just an ambulatory wallet, a supply of gut bacteria for the immortal colony organism that is a limited liability corporation.

But it *can* make that exec fear you enough to treat you fairly and afford you dignity, even if he doesn't think you deserve it.

And I think that's pretty important.

## Acknowledgments

This book started in 2023 as a series of essays on my Pluralistic.net blog, one of which caught the eye of Gideon Lichfield, who republished it on Wired.com, which kicked off the first wave of interest beyond my own readership.

In late 2023, the American Dialect Society named *enshittification* their Word of the Year, and then Nóra Ó Murchú asked me to come to Berlin and give the Marshall McLuhan Lecture at the Canadian embassy for the Transmediale festival. After I published the transcript of that talk on Pluralistic, Matt Vella at the *Financial Times* reprinted it in the weekend magazine, and then Stefan von Holtzbrinck and Jochen Wegner picked it up for *Die Zeit*.

Next, Brooke Gladstone and her colleague Katya Rogers from *On the Media* were kind enough to feature enshittification in a three-part series on their show. That prompted a flurry of interviews, podcast appearances, invitations to submit articles, and so many other opportunities to talk about these ideas to wider and wider audiences.

I'm so thankful for everyone who helped me get this critique over the transoms of so many people, who in turn spread the word and—more important—the ideas. My colleagues, both past and present, at the Electronic Frontier Foundation helped me develop this critique and supported me while I refined it and delivered it.

Other colleagues from the wider digital rights movement were critical as well.

Over the past half decade, I've been lucky to connect with the modern antitrust movement, "neo-Brandeisians" like Matt Stoller, Barry Lynn, Lina Khan, Cristina Caffarra, Dina Srinivasan, Zephyr Teachout, Will Hayter, Tim Wu, Rebecca Slaughter, David Dayen, Michelle Meagher, Jonathan Kanter, Alvaro Bedoya, Cori Crider, Rohit Chopra, and many others. It's an honor to serve in these trenches with you all.

I'm also keenly grateful to the heterodox economists who've welcomed me into their midst, such as Stephanie Kelton, Steve Keen, L. Randall Wray, Patricia Pino, and Christian Reilly.

I wouldn't be who I am without my family: my parents, Roz and Gord, who taught me that some fights you fight because you *must*, not because you have any reasonable expectation of winning (my mother is also hands-down the best proofreader I've ever had, and she caught and fixed several typos in the book you are reading right now); my wife, Alice Taylor, who is my best friend, sounding board, and wisest adviser; our daughter, Poesy, who is brilliant and talented and helps me stay relevant.

Sean McDonald, my editor at Farrar, Straus and Giroux's MCD, gave me invaluable feedback and made this book infinitely better. Rodrigo Corral designed the *banging* cover. Janet Renard gave this book a thorough and thoughtful copyedit. Ben Brooks shepherded it through production. Steve Weil masterminded the publicity campaign and collaborated with my brilliant team at Wunderkind PR, Elena Stokes, Brianna Robinson, and Kayla Slusser.

I am blessed with many brilliant and generous readers who have supported me in innumerable ways, from foisting my books on others to backing my weirdo Kickstarters. Two readers, though, have made a gigantic difference to my daily writing:

Loren Kohnfelder, who took pity on me and wrote the Python scripts I use to publish my blog; and Gregory Cherlin, who emails me twice per month with corrections for all my typos.

Of course, I also collaborate with many other kinds of writers, thinkers, and doers. There are lawyers like Jamie Boyle and Jennifer Jenkins, Lawrence Lessig, and Rebecca Giblin. There are technologists like Ken Snider, who keeps my infra running, and bunny Huang, who makes me smarter about technology every time we talk. There are media producers like Acey Rowe and Matt Meuse at the CBC. There are my audio production comrades, Gabrielle de Cuir and Stefan Rudnicki at Skyboat Media and John Taylor Williams at Wryneck Studio.

Then there are all the web writers: Mark Frauenfelder, Molly White, Ed Zitron, Brian Merchant, the 404 Media crew, Cat Valente (“Stop Talking to Each Other and Start Buying Things” is a must-read), and so many others.

The longer I think about this, the more names I come up with. I’m going to stop now, but I’ll leave you with one final word: *enshittification*.

Specifically, I am giving you *explicit permission* to use this word in a loose sense, whenever you think it makes sense to do so. As I wrote in my essay “Dirty Words Are Politically Potent”:

The fact that a neologism is sometimes decoupled from its theoretical underpinnings and is used colloquially is a *feature*, not a bug. Many people apply the term “enshittification” very loosely indeed, to mean “something that is bad,” without bothering to learn—or apply—the theoretical framework. This is *good*. This is what it means for a term to enter the lexicon: it takes on a life of its own. If 10,000,000 people use “enshittification” loosely and inspire 10 percent of their number to look up the longer,

more theoretical work I've done on it, that is one million normies who have been sucked into a discourse that used to live exclusively in the world of the most wonkish and obscure practitioners. The only way to maintain a precise, theoretically grounded use of a term is to confine its usage to a small group of largely irrelevant insiders. Policing the use of "enshittification" is worse than a self-limiting move—it would be a self-inflicted wound.

## A Note About the Author

Cory Doctorow is a blogger, journalist, and activist. For more than twenty years, he has worked with the Electronic Frontier Foundation on campaigns to safeguard and further our human rights online. He was coeditor of the weblog *Boing Boing* for nineteen years and now maintains a daily(ish) newsletter at Pluralistic.net. He has written more than thirty books, including nonfiction books, many science fiction novels, collections of short stories and essays, young adult novels, graphic novels, and even a picture book. Born in Toronto, he now lives in Burbank, California. He was awarded an honorary doctorate in laws by York University and an honorary doctorate in computer science by the Open University. He has been inducted into the Canadian Science Fiction and Fantasy Association Hall of Fame and was awarded the Sir Arthur C. Clarke Award for Imagination in Service to Society. He holds visiting professorship and research appointments at MIT, the University of North Carolina, Cornell University, and the Open University.

