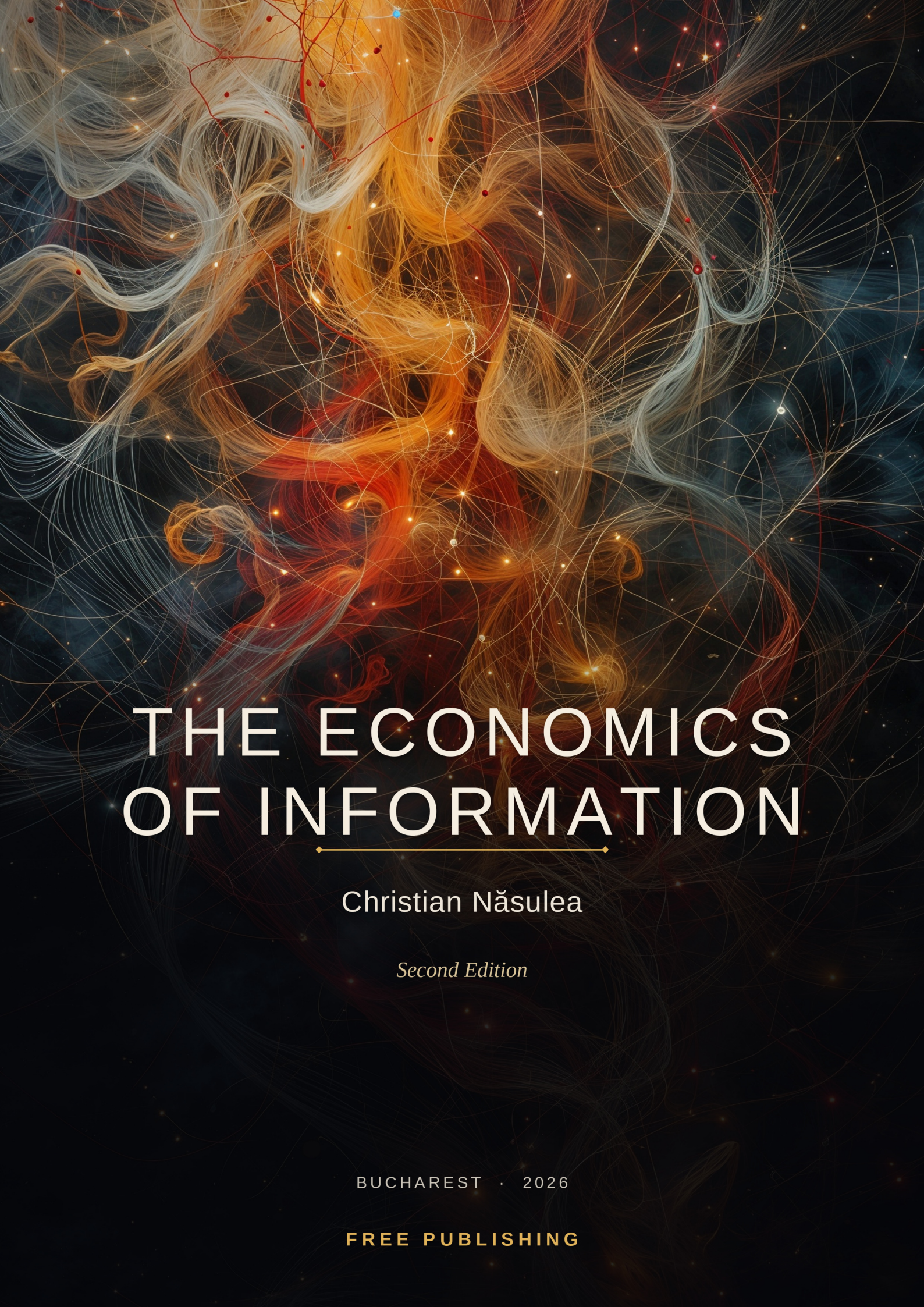




THE ECONOMICS OF INFORMATION

Christian Năsulea

Second Edition

BUCHAREST · 2026

FREE PUBLISHING

THE ECONOMICS OF INFORMATION

Christian Năsulea

Second Edition

The Economics of Information

Author: Christian Năsulea

Second Edition

ISBN 978-630-95499-1-4

Copyright © 2023, 2026 Christian Năsulea

Published by FREE Publishing

Republicii 202, Comarnic, Prahova, Romania

editurafree.ro / freepublishing.eu

Direct all inquiries to contact@editurafree.ro

This book is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0), unless otherwise required or stated. To view a copy of this licence, visit creativecommons.org/licenses/by-nc-sa/4.0/

The chapter-opening photographs are licensed from Adobe Stock and are not covered by the Creative Commons licence. They may not be reused outside this book without a separate licence.

Contents

How to Use this Textbook.....	4
Part I. How Information Shapes Markets.....	6
1. Markets and Price Signals.....	7
2. Information Asymmetry.....	14
3. The Principal-Agent Problem.....	20
4. Game Theory.....	24
Part II. Technology and the Organisation of Work.....	30
5. Platforms and the Sharing Economy.....	31
6. Blockchain and Smart Contracts.....	38
7. Robots, RPA, AI and the Future of Work.....	44
8. Crowdsourcing.....	51
9. Outsourcing.....	56
Part III. The Rules of the Digital Economy.....	61
10. Intellectual Property.....	62
11. Big Data, Privacy, and GDPR.....	67
12. Social Media and Fake News.....	72
13. Big Tech vs Big Government.....	77
Glossary.....	82
Answers to Self-check Questions.....	86
References.....	92

How to Use this Textbook

This textbook accompanies the Economics of Information course taught at the Faculty of Business Administration in Foreign Languages at the Bucharest University of Economic Studies. It is written for students who attend the lectures and take part in the group work, and it is meant to deepen that experience rather than replace it. Each chapter explains a concept in plain language, illustrates it with a worked example or a real case, and points to further reading for those who want to go further.

The chapters can be read in order or dipped into as the course progresses. Wherever a chapter relies on an idea introduced elsewhere in the book, the connection is made explicit in the text, so that the same few principles, scarcity, incentives, trust, and the uneven distribution of information, are seen at work across very different settings, from automation and online platforms to privacy law and intellectual property.

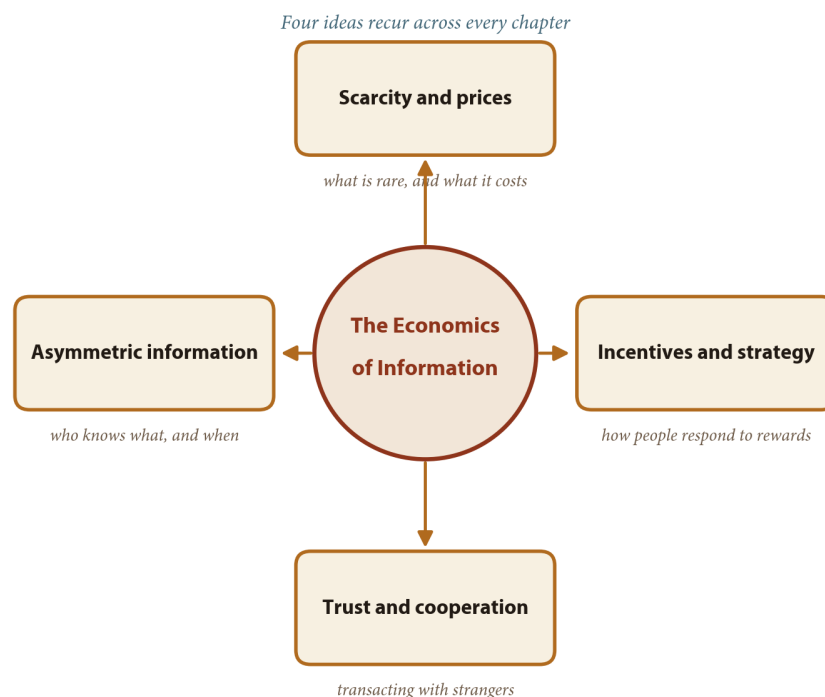


Figure 1. The four ideas that recur across every chapter of the book.

The book is organised in three parts. Part I sets out the core ideas of the economics of information: how prices carry knowledge, what happens when information is unevenly shared, how delegation creates agency problems, and how strategic interaction shapes outcomes. Part II applies these ideas to the technologies and arrangements that are changing how exchange and work are organised: platforms, blockchain, automation and artificial intelligence, crowdsourcing, and outsourcing. Part III turns to the rules: intellectual property, data protection, the regulation of online speech, and the contest between the largest technology firms and the states that govern them. Throughout, market failures are weighed against government failures, because neither markets nor states are perfect, and the useful question is always which imperfection is the smaller in a given case.

Each chapter opens with a short list of learning objectives and closes with a summary box headed “In brief.” The body of the chapter is written to be read as continuous prose; the summary box gathers the main points in list form for quick revision before a seminar or an exam. Treat the box as a checklist of

what you should be able to explain in your own words, not as a substitute for the explanation itself. At the back of the book you will find a glossary of key terms, with their Romanian equivalents, and short answers to the self-check questions that end each chapter.

A word of caution about the further reading. Not every item listed is meant to be accepted at face value. A few have been included precisely because they contain weak arguments or logical fallacies, so that the full range of opinion on a contested question is represented. Reading critically, weighing the evidence, and noticing when a claim outruns what its author has actually shown, is one of the central skills this course tries to develop. The economics of information is, in the end, about how we come to know things, and how easily we can be misled.

This is the second edition. The conceptual core of the course is unchanged, but the regulatory landscape and the technology have moved quickly since the first edition, and every chapter has been updated to reflect recent developments. The text reflects the state of affairs in October 2026. Students and colleagues at other institutions are welcome to use these materials. Useful examples and constructive feedback are always appreciated and will be credited in future editions.

Part I. How Information Shapes Markets

The four chapters of Part I set out the ideas on which the rest of the book relies. They explain how prices carry knowledge that no one could gather centrally, what goes wrong when one side of a transaction knows more than the other, why delegating a task always costs something, and how people reason when the outcome depends on what others do. Each idea is introduced with everyday examples so that it can be recognised again later, in very different settings.



1. Markets and Price Signals

Learning objectives

- Explain how prices transmit dispersed knowledge, and why Hayek saw this as the central function of markets.
- Use supply, demand, and elasticity to predict how prices and quantities respond to change.
- Explain why search costs let the same good sell at different prices, and how information goods are priced.
- Compare market failure with government failure and explain why both must be weighed.

A market is any setting in which buyers and sellers come together to exchange goods, services, or resources, whether a physical farmers' market or an online auction running across continents. What makes markets remarkable is not the exchange itself but the coordination they achieve. No one plans how much bread a city needs, yet bread appears in roughly the right quantity each morning. The mechanism that performs this quiet miracle is the price, and understanding prices as carriers of information is one of the deepest ideas in economics.

Prices are signals. A price compresses an enormous amount of dispersed knowledge, how scarce a resource is, how much consumers value it, how costly it is to produce, into a single number that everyone can see and act on. The economist Friedrich Hayek argued that this is the central function of a market: no planner could ever gather and process all the local knowledge held by millions of individuals, but the price system transmits the relevant part of it automatically. When tin becomes scarce, its price rises, and users around the world economise on tin without ever knowing why, simply because it has become more expensive. The price did the communicating.

The familiar machinery of supply and demand describes how these signals form. Holding other things equal, higher demand pushes prices up and higher supply pushes them down, and the two pressures settle at an equilibrium, the market-clearing price at which the quantity buyers want exactly matches the

quantity sellers offer. That price then guides behaviour on both sides. When a price rises because demand is strong or supply is short, it signals producers to make more and consumers to use less; when it falls, it signals the reverse. In this way resources flow, without central direction, toward the uses people value most.

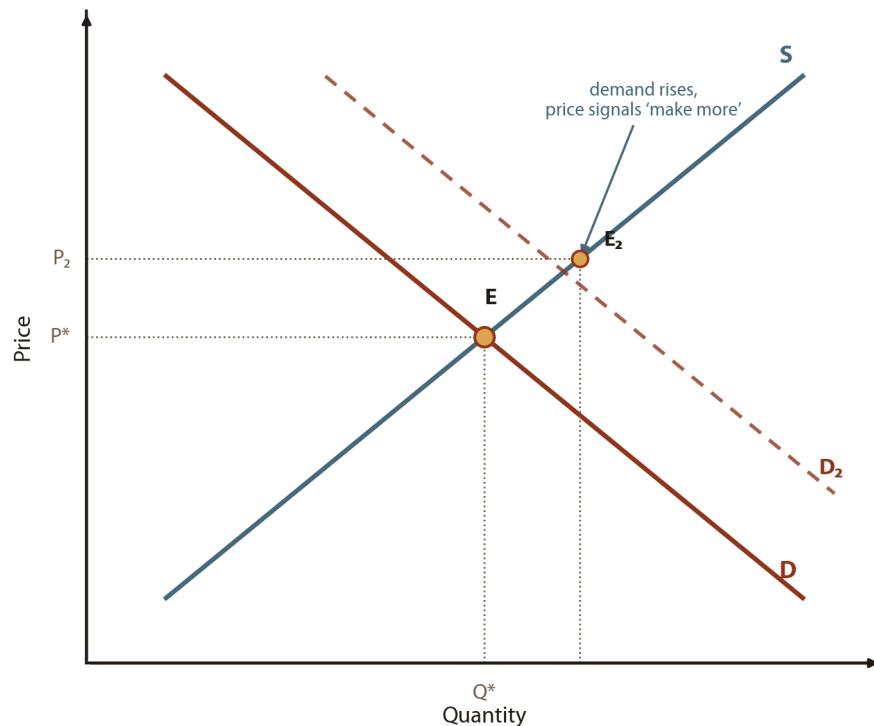


Figure 2. Supply, demand, and the price signal: a rise in demand lifts the equilibrium price.

Competition is what keeps the signal honest. In a competitive market individual firms are price takers, too small to set the price and obliged to accept what the market offers, and competition drives prices down toward the cost of production, squeezing out waste. How sharply quantities respond to price is captured by elasticity: where demand is elastic, a small price change causes a large change in quantity, and where it is inelastic, quantity barely moves. Elasticity matters for everything from how a tax is shared between buyers and sellers to how a firm should price to maximise revenue.

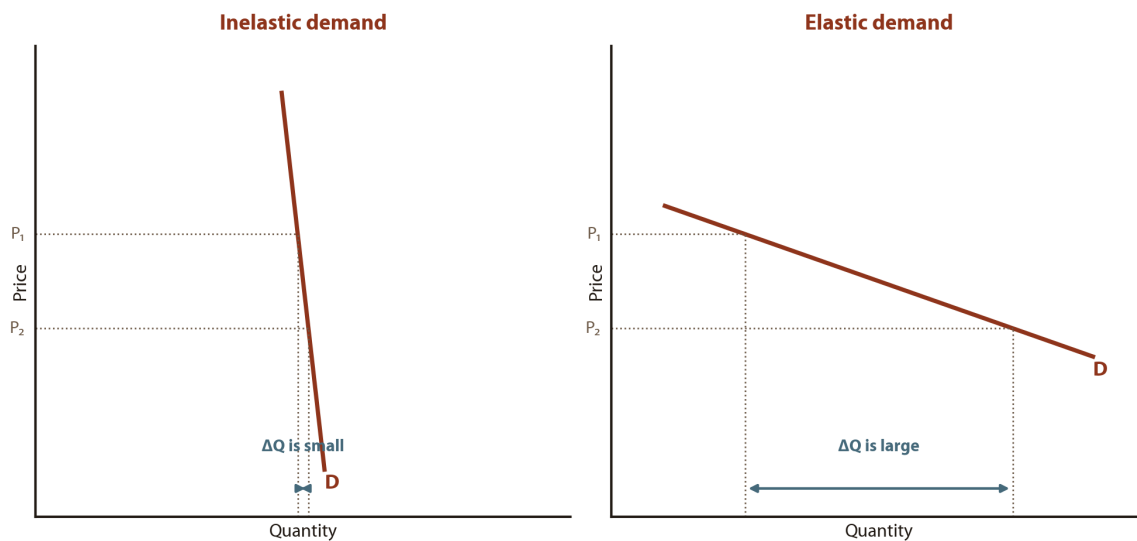


Figure 3. Elastic and inelastic demand: how sharply quantity responds to a change in price.

Markets can also fail, and the failures usually trace back to information or to costs that escape the price. Externalities, such as pollution, impose costs on third parties that the price does not capture, so the market produces too much of the harmful activity. Public goods, such as national defence, will be undersupplied because no one can be made to pay for what they can enjoy for free. And information asymmetries, the subject of Chapter 2, can distort or destroy markets outright. These failures are the standard economic justifications for government intervention, though intervention has its own costs and failures, a tension that runs through later chapters on regulation. Markets, finally, never float free of institutions; they are shaped by laws, courts, regulators, and trade rules that determine how information flows and how contracts are enforced.

Government failure deserves the same scrutiny as market failure. Intervention is carried out by people who face incentives and information problems of their own. A regulator rarely knows as much about an industry as the firms it oversees, which is Hayek's knowledge problem in a new setting. Politicians respond more readily to organised interests than to dispersed ones, so a policy whose benefits are concentrated on a few and whose costs are spread thinly across many can survive long after it has stopped serving its stated purpose. Rent controls that shrink the supply of rental housing, agricultural subsidies that outlive the crises that justified them, and licensing rules that shield incumbents from competition are standard examples. The comparison that matters is therefore never an imperfect market against a perfect government, but one imperfect institution against another, and the chapters that follow keep asking which imperfection is the smaller in each case.

Search Costs and Price Dispersion

Hayek's price system works only if people can see the prices, and in practice they cannot see them all, because finding out what different sellers charge takes time and effort. George Stigler made this the starting point of a 1961 article that is often regarded as the founding paper of the economics of information. Because search is costly, buyers stop searching once the expected saving from one more enquiry falls below the cost of making it, and so the same good sells at different prices in different shops even in a competitive market. Price dispersion, in other words, is not a sign that a market has failed; it is a measure of how expensive it is to be informed.

The theory makes a sharp prediction: anything that lowers the cost of search should narrow price dispersion and push prices down. Price-comparison websites, online marketplaces, and apps that list fuel prices along a route do exactly this. The internet has not abolished dispersion, however. Sellers

respond by making comparison harder, through complicated tariffs, add-on fees, and frequent small price changes, a reminder that information can be obscured as well as revealed. The same logic explains much of the value of brands, advertising, and reputation, which save buyers the cost of searching by telling them where reliable quality can be found, an idea developed in Chapter 2.

Price Differentiation

One of the most visible uses firms make of information about customers is price differentiation, also called price discrimination: charging different prices to different buyers for essentially the same good, according to what each is willing to pay. Far from being unusual, it is everywhere, and a cinema ticket is a perfect tutorial. Children pay less, because families are price-sensitive and a lower price brings them in; adults pay the standard fare; seniors receive a discount that recognises a fixed income and fills seats that might otherwise stay empty. The same film at a quiet weekday matinee costs less than at a Saturday evening show, spreading demand across the day and capturing both the bargain-hunter and the customer who insists on prime time. Members pay less through a loyalty scheme that secures repeat business and a steady revenue stream, while a premium format such as IMAX or 3D commands a higher price from those who want the enhanced experience.

Each of these is a way of sorting customers by willingness to pay and charging each group accordingly, which lets the seller serve more of the market and earn more than a single uniform price would allow. The digital economy has supercharged the practice. With detailed data on individual behaviour, firms can move toward personalised and dynamic pricing, adjusting offers in real time and, in principle, tailoring a price to each shopper. This raises sharper fairness and privacy concerns than a cinema's age-based discount, and regulators have begun to respond: consumer-protection rules in the EU now require disclosure when a price has been personalised using automated processing, and competition authorities have opened inquiries into so-called surveillance pricing. Price differentiation, in short, sits exactly at the meeting point of this course's themes, information, markets, and the uses and abuses of knowing your customer.

Information Goods

Much of what the digital economy sells is information itself: software, music, films, news, databases, and online services. These information goods have an unusual cost structure. The first copy is expensive to produce, because it embodies all the research, writing, coding, or filming, but every further copy costs almost nothing to make and distribute. High fixed costs and near-zero marginal costs change the rules of pricing. Selling at marginal cost, the textbook competitive outcome, would mean giving the product away and never recovering the cost of making it, so producers of information goods must price according to what customers are willing to pay rather than according to what an extra copy costs.

Carl Shapiro and Hal Varian, in their influential book *Information Rules*, described the two main ways in which firms do this. The first is versioning: offering the same underlying product in several versions, a basic and a premium tier, a delayed and an instant one, a home and a professional edition, so that customers sort themselves by willingness to pay, exactly as with the cinema tickets above. The second is bundling: selling many goods together for a single price, as streaming services and software suites do, which works because customers who value individual items very differently tend to value the bundle as a whole more similarly. Information goods are also experience goods, whose quality can be judged only after consumption, which is why free trials, previews, and reviews matter so much, and they are easy to copy, which is why intellectual property, discussed in Chapter 10, carries so much weight in this part of the economy.

In brief

- Prices are signals. A price condenses dispersed knowledge about scarcity, value, and cost into one number everyone can act on.
- Supply and demand find equilibrium. The market-clearing price matches quantity supplied to quantity demanded and guides resources to their most valued uses.
- Competition disciplines prices. Price-taking firms are pushed toward cost, and elasticity governs how strongly quantities respond.
- Markets can fail. Externalities, public goods, and information asymmetries justify, but do not guarantee, beneficial intervention.
- Price differentiation sorts by willingness to pay. Age, time, loyalty, and format discounts let sellers serve more of the market and capture more value.
- Data sharpens and complicates it. Personalised and dynamic pricing raise fairness and privacy concerns that regulators are starting to address.

Case study: surge pricing and the shortage debate

Few ideas in economics are as easy to state and as hard to accept emotionally as the claim that prices should rise when things are scarce. The clearest modern illustration is surge pricing on ride-hailing apps. When demand spikes, after a concert lets out, during a downpour, on New Year's Eve, the price of a ride climbs, sometimes steeply. Economically, this is the price system doing exactly what this chapter describes. The higher price rations the limited supply of cars toward the riders who value them most at that moment, and at the same time it signals drivers, who can see where surge is highest, to head toward the shortage. Supply rises, demand moderates, and the market clears far faster than it would at a fixed fare, where the result of a shortage is simply that no cars are available at any price.

Yet surge pricing provokes genuine anger, and the anger is instructive. People feel that charging more in a moment of need is unfair, even exploitative, especially when the need is acute, getting home safely late at night, or reaching a hospital. The economist's reply, that the alternative to a high price is not a low price but no service at all, is logically strong and emotionally unpersuasive, and a manager who ignores the fairness reaction will pay for it in reputation. This is the same tension introduced by price differentiation: a mechanism that is efficient can still be perceived as unjust, and in a world of online outrage perception has real commercial consequences.

The debate turns sharpest during genuine emergencies, where it collides with the law. When a hurricane approaches or a pandemic strikes, the price signal would ordinarily send bottled water, generators, masks, and hand sanitiser rushing toward the affected area and tell buyers to take only what they truly need. During the early months of the COVID-19 pandemic in 2020, soaring prices for masks and sanitiser did exactly that, drawing in new suppliers, but they also triggered public fury and a wave of enforcement under anti-price-gouging laws that cap price rises during declared emergencies. Those laws express a real value, that no one should profiteer from a disaster, but they carry a real cost, because by holding prices below the market-clearing level they can produce empty shelves, hoarding, and queues, the classic symptoms of a shortage that the price was trying to prevent.

There is no tidy resolution, and that is the point of the case. Prices are extraordinarily effective at coordinating dispersed decisions and allocating scarce resources, which is the lesson of Hayek and the heart of this chapter. But prices are not the only thing societies care about; fairness, dignity, and protection of the vulnerable matter too, and sometimes they justify overriding the signal even at a cost in efficiency. The educated analyst's job is not to worship the price mechanism or to dismiss it, but to understand precisely what it does, what it leaves out, and what is gained and lost when we choose to interfere with it.

Review and practice

Discussion questions

1. Hayek argued that no planner could replace the price system. What exactly does a price know that a planner cannot?
2. Surge pricing is efficient but widely resented. Should ride-hailing apps be allowed to raise prices during emergencies? Argue both sides.
3. Is personalised pricing, charging each customer their own tailored price, a clever use of information or an unfair one? Where would you draw the line?

Exercises

1. Demand for a good rises while its supply is fixed. Trace, step by step, what happens to the price and how that price reallocates the good among buyers.
2. A cinema charges different prices by age, by time of day, and by format. For each, identify the customer characteristic it is exploiting and explain why.
3. Explain how an anti-price-gouging law can create the very shortage it was meant to prevent.

Self-check

- What information does a price transmit?
- Define the market-clearing price.
- Name three causes of market failure.
- What is price elasticity, and why does it matter for how a tax is shared?
- Give two examples of government failure, and explain why it should be compared with market failure.
- Why does costly search allow the same good to sell at different prices?
- Why are information goods often sold in versions or bundles?

Further Reading

- Assad, S., Clark, R., Ershov, D., & Xu, L. (2024). Algorithmic pricing and competition: Empirical evidence from the German retail gasoline market. *Journal of Political Economy*, 132(3), 723-771.
<https://doi.org/10.1086/726906>
- Bichler, M., Knörr, J., & Maldonado, F. (2023). Pricing in nonconvex markets. *Information Systems Research*, 34(2), 652-675.
<https://doi.org/10.1287/isre.2022.1139>
- Brown, Z. Y., & MacKay, A. (2023). Competition in pricing algorithms. *American Economic Journal: Microeconomics*, 15(2), 109-156.
<https://doi.org/10.1257/mic.20210158>
- Chen, L. (2019). Retailers' differentiation strategy and pricing in the rental market of digital content. *Journal of Theoretical and Applied Electronic Commerce Research*, 14(3), 61-75.
<https://www.mdpi.com/0718-1876/14/3/22>
- Coyle, D. (2021). *Cogs and monsters: What economics is, and what it should be*. Princeton University Press.
- Hayek, F. A. (1945). The use of knowledge in society. *The American Economic Review*, 35(4), 519-530.
<https://www.jstor.org/stable/1809376>
- Shapiro, C., & Varian, H. R. (1999). *Information rules: A strategic guide to the network economy*. Harvard Business School Press.
- Stigler, G. J. (1961). The economics of information. *Journal of Political Economy*, 69(3), 213-225.
<https://doi.org/10.1086/258464>



2. Information Asymmetry

Learning objectives

- Distinguish adverse selection from moral hazard and give an example of each.
- Explain how signalling, screening, and reputation help markets overcome hidden information.
- Assess how digital platforms have both reduced and relocated information asymmetry.
- Evaluate regulatory remedies, including the risk of regulatory capture.

At the heart of the economics of information lies a simple observation with far-reaching consequences: in most transactions, the two sides do not know the same things. The seller of a used car knows whether it has hidden faults; the buyer does not. The borrower knows how risky the venture really is; the lender can only guess. This imbalance, where one party holds more or better information than the other, is called information asymmetry, and it can distort or even destroy markets that would otherwise work well.

It helps to distinguish two moments at which asymmetry bites. Before a deal is struck, the problem is hidden information, which economists call adverse selection. The classic illustration is George Akerlof's "market for lemons." Suppose buyers cannot tell good used cars from bad ones, the lemons, and so are willing to pay only an average price. At that price, owners of genuinely good cars are unwilling to sell, since they know their car is worth more, so they withdraw. With the good cars gone, the average quality on the market falls, buyers revise their offers down further, and still more decent cars leave. In the limit the market can unravel entirely, even though buyers and honest sellers would both gladly trade if only quality could be observed. The same logic explains why the sickest people are keenest to buy insurance and why lenders fear that the most eager borrowers are the riskiest.

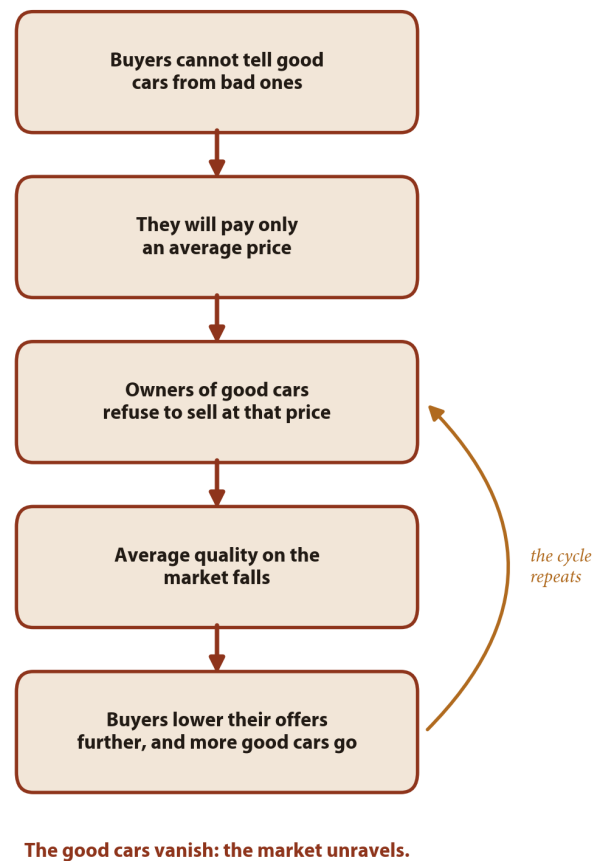


Figure 4. How information asymmetry can unravel the market for used cars.

After a deal is struck, the problem becomes hidden action, or moral hazard. Once someone is insured, they bear less of the cost of carelessness and may take risks they would otherwise avoid; once an employee is paid a fixed salary, the employer cannot fully observe how hard they work. In each case one party cannot monitor the other's behaviour, and so the other's incentives quietly change. Adverse selection is about who you end up trading with; moral hazard is about how they behave once you have.

Markets do not simply surrender to these problems; they evolve devices to overcome them. The first is signalling, in which the better-informed party takes a costly action to credibly reveal what it knows. A job applicant invests years in a degree partly to signal ability to employers who cannot directly observe it; a manufacturer offers a long warranty to signal that it expects its product to last; a firm builds a brand precisely so that its name becomes a believable promise of quality. For a signal to work it must be cheaper for the high-quality type to send than for the low-quality type to fake, otherwise everyone would send it and it would convey nothing.

The mirror image is screening, in which the less-informed party designs choices that lead the other side to sort itself. An insurer offers a menu of policies, one with a high deductible and low premium, another with a low deductible and high premium, knowing that low-risk customers will tend to choose the first and high-risk customers the second, thereby revealing through their choice what the insurer could not directly see. Reputation systems, certifications, mandatory disclosure, and product labelling all work in related ways, shrinking the information gap so that trade can resume.

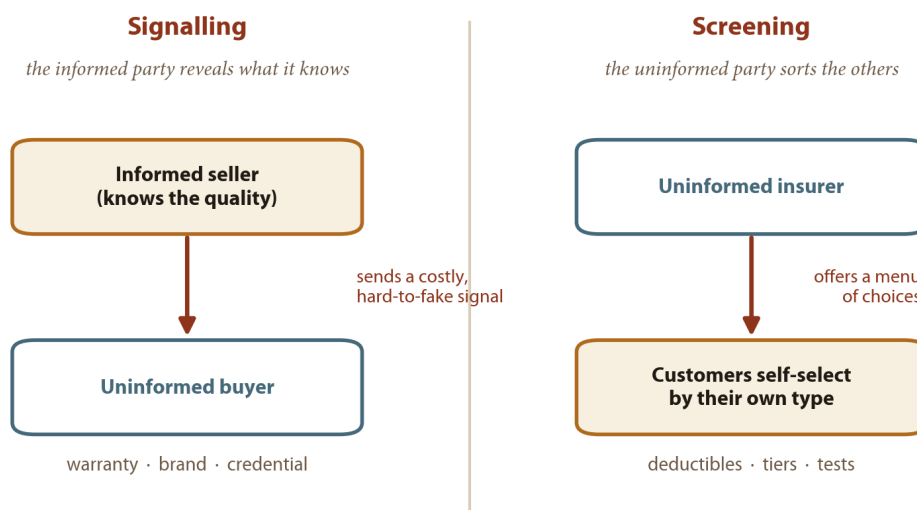


Figure 5. Two ways markets overcome information asymmetry: signalling and screening.

The digital economy has transformed this ancient problem in two opposite directions at once. On one hand, online reviews, ratings, verified histories, and escrow services have dramatically reduced the asymmetries that once made it dangerous to buy from a stranger, which is exactly why platforms, the subject of Chapter 5, invest so heavily in them. On the other hand, large firms now often know far more about us than we know about them. They observe our behaviour in fine detail, infer our willingness to pay, and shape what we see, while their algorithms remain opaque to us. The result is not the disappearance of information asymmetry but its relocation, and much of the regulation discussed later in this book, from consumer protection to data rights to algorithmic transparency, is an attempt to redress the new imbalance.

Regulation is the other familiar answer to information asymmetry, and it deserves the same critical eye as the market remedies. Mandatory disclosure, product standards, and professional licensing can protect uninformed buyers, but the regulator is itself an uninformed party, often knowing less about an industry than the firms it supervises, and it faces incentives of its own. George Stigler argued in 1971 that regulation is frequently acquired by the industry it governs and designed mainly for that industry's benefit, a process known as regulatory capture. Occupational licensing illustrates the risk. Presented as a guarantee of quality, it can also work as a barrier that keeps competitors out and prices up: a 2015 report prepared for the White House found that more than a quarter of American workers needed a licence to do their jobs, a share that had risen roughly five-fold since the 1950s, with little consistent evidence that the spread of licensing had improved quality. Credit-rating agencies offer a second warning. When American regulators began, from 1975, to write the ratings of officially recognised agencies into financial rules, they turned a handful of firms into gatekeepers on which many investors were effectively required to rely, which weakened the reputational discipline that should have kept the agencies careful, and their ratings of mortgage securities failed badly before the crisis of 2008 described in Chapter 3. Rules can close information gaps, but they can also create new ones, and their record has to be judged case by case, just like the market's.

In brief

- Asymmetry is the norm. In most transactions one party knows more than the other, and that imbalance can distort or destroy a market.
- Adverse selection: hidden information. Before trading, unobservable quality can drive good products out, as in Akerlof's market for lemons.
- Moral hazard: hidden action. After trading, a party that is shielded from consequences may change its behaviour where it cannot be monitored.
- Signalling. The informed party reveals what it knows through costly, hard-to-fake actions such as warranties, credentials, or a brand.
- Screening. The uninformed party offers choices that lead the other side to sort itself, as with insurance menus and deductibles.
- The digital twist. Reviews and ratings shrink old asymmetries, but firms now often know more about us than we do about them.

Case study: the used-car market and the war on lemons

George Akerlof built his famous model on the used-car market, and that market remains the clearest place to watch information asymmetry both cause a problem and call forth its own solutions. The difficulty is simple to state. A seller knows whether a car has been reliable or troublesome; a buyer, looking at two cars that appear identical, cannot tell a sound vehicle from a hidden wreck. Fearing the worst, the buyer offers only a middling price, which is too low to tempt the owners of genuinely good cars to sell. As they withdraw, average quality falls, buyers lower their offers again, and in the extreme the market for good used cars can collapse even though buyers and honest sellers would both like to trade. The word lemon, American slang for a defective car, gave the model its name.

What is striking is that the real used-car market has not collapsed, because over time it evolved a whole toolkit of the devices this chapter describes, aimed squarely at closing the information gap. Dealers offer warranties, a costly promise that signals confidence in the car, since a seller who expected the vehicle to fail would not offer to pay for repairs. Manufacturers run certified pre-owned programmes, putting their brand behind a used car after an inspection and thereby lending it the reputation the individual seller lacks. Buyers, for their part, can pay an independent mechanic to inspect a car before purchase, a form of screening that turns hidden information into observable fact.

The most powerful modern remedy is the vehicle-history report. Services that aggregate accident records, service histories, ownership changes, and odometer readings let a buyer see much of what was once known only to the seller, and their very existence changes behaviour, because a seller who knows the history can be checked has less room to misrepresent it. Reputation does similar work: a dealer who depends on repeat business and online reviews has a strong incentive not to sell lemons, since a single exposed deception can cost far more in lost custom than the deception gained. Online marketplaces extend this further, attaching ratings and feedback to sellers so that trust can accumulate and travel.

The case is worth dwelling on because it generalises. The lemons problem is not really about cars; it is about any market where quality is hidden, from insurance and lending to freelance labour and second-hand goods online. And the response is always some combination of the same instruments: signalling by the informed party, screening by the uninformed party, and reputation systems that make honesty pay. Markets do not passively suffer information asymmetry. Where there is value to be unlocked by overcoming it, they tend, over time, to invent the institutions that do so, which is one of the more hopeful lessons in the economics of information.

Review and practice

Discussion questions

1. In the market for lemons, why can honest sellers of good cars be driven out, and what does that tell us about trust in markets more generally?
2. A university degree is partly a signal of ability. If employers could measure ability directly and cheaply, would degrees lose their value? What would that imply about what students are really buying?
3. Online reviews have shrunk old asymmetries, yet firms now know more about us than we do about them. On balance, is the information relationship between buyers and sellers better or worse than before the internet?

Exercises

1. Give one real example each of signalling and of screening that you have encountered as a customer, and explain in each case why it works.
2. An insurer offers two policies: high premium with a low deductible, and low premium with a high deductible. Explain which customers each is designed to attract and how this sorts risk.
3. Choose an online marketplace and list every feature it uses to overcome the information asymmetry between buyers and sellers.

Self-check

- What is the difference between adverse selection and moral hazard?
- For a signal to be credible, what must be true of its cost?
- Define screening and give an example.
- Why does a strong brand reduce information asymmetry?
- What is regulatory capture, and why does it matter for remedies against information asymmetry?

Further Reading

- Akerlof, G. A. (1970). The market for “lemons”: Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84(3), 488-500.
<https://www.jstor.org/stable/1879431>
- Bergemann, D., Bonatti, A., & Gan, T. (2022). The economics of social data. *The RAND Journal of Economics*, 53(2), 263-296.
- Bergh, D. D., Ketchen, D. J., Orlandi, I., Heugens, P. P. M. A. R., & Boyd, B. K. (2019). Information asymmetry in management research: Past accomplishments and future opportunities. *Journal of Management*, 45(1), 122-158.
<https://doi.org/10.1177/0149206318798026>
- Einav, L., Finkelstein, A., & Fisman, R. (2023). *Risky business: Why insurance markets fail and what to do about it*. Yale University Press.
- European Union. (2019). *Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/dir/2019/771/oj>
- Spence, M. (1973). Job market signaling. *The Quarterly Journal of Economics*, 87(3), 355-374.
<https://doi.org/10.2307/1882010>
- Stigler, G. J. (1971). The theory of economic regulation. *The Bell Journal of Economics and Management Science*, 2(1), 3-21.
<https://doi.org/10.2307/3003160>
- U.S. Department of the Treasury Office of Economic Policy, Council of Economic Advisers, & U.S. Department of Labor. (2015). *Occupational licensing: A framework for policymakers*. The White House.
https://obamawhitehouse.archives.gov/sites/default/files/docs/licensing_report_final_nonembargo.pdf
- Zhao, M., Wang, S., & Xia, T. (2025). The social welfare effect of e-commerce product reputation information asymmetry from the perspective of network externality. *PLOS ONE*, 20(1), Article e0313852.
<https://doi.org/10.1371/journal.pone.0313852>



3. The Principal-Agent Problem

Learning objectives

- Identify the principal, the agent, and the hidden action in a relationship of delegation.
- Explain why the problem requires both divergent interests and information asymmetry.
- Break agency cost into its components and design contracts that narrow the gap.
- Apply principal-agent reasoning to government through public choice theory.

The principal-agent problem is the information asymmetry of Chapter 2 seen from inside a relationship of delegation. Whenever one party, the principal, hires another, the agent, to act on its behalf, it gains the agent's time, skill, or reach but loses something too: it can no longer be sure the agent is acting in the principal's interest rather than the agent's own. Shareholders delegate to managers, employers to employees, patients to doctors, citizens to elected officials, and in every case the same tension appears.

The problem has two ingredients, and it requires both. The first is a divergence of interests. Principal and agent share some goals but not all of them, and where their interests part company the agent has reason to favour its own. The second is information asymmetry. The agent typically knows more than the principal about the task, about its own effort, and about its own intentions. If interests were perfectly aligned, the asymmetry would not matter, because the agent would do what the principal wants anyway. If information were perfect, the divergence would not matter, because the principal could simply observe and insist. It is the combination, conflicting interests plus hidden action, that creates the difficulty. Hidden action is the moral hazard of Chapter 2, now built into a lasting relationship.

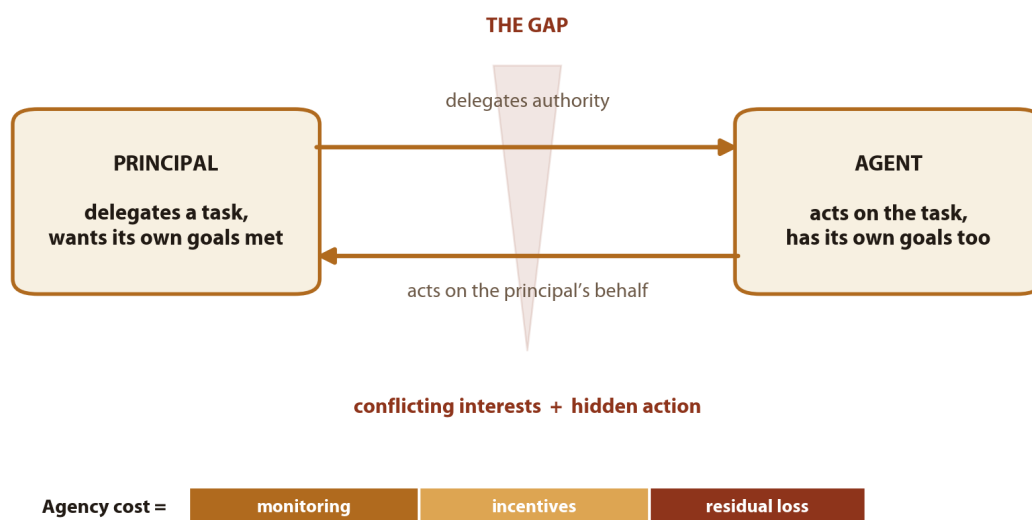


Figure 6. The principal-agent relationship and the gap that creates agency costs.

From this root grow several familiar troubles. The principal often cannot observe how much effort the agent is really putting in, so the agent may shirk. Principal and agent may differ in their appetite for risk, with a salaried employee preferring safety and an owner willing to gamble for a higher return. They may also weigh time differently, the agent chasing short-term gains that flatter this quarter's numbers at the expense of the principal's long-run health. Monitoring can reduce these problems but is costly and never complete, and even a watched agent may be hard to judge.

Because perfect monitoring is impossible, the practical response is to design incentives so that the agent, in pursuing its own interest, also serves the principal's. This is what performance-related pay, commissions, bonuses, equity stakes, and deferred compensation are for: they tie the agent's reward to outcomes the principal cares about. The catch is that incentives are blunt instruments. Reward a salesperson purely on volume and they may push unsuitable products; reward a manager purely on the share price and they may cut the investment that secures the firm's future. A poorly designed incentive does not eliminate the conflict; it merely redirects the agent's ingenuity toward gaming the measure. Some loss almost always remains, what the literature calls the residual loss, and the sum of monitoring costs, incentive costs, and that residual loss is the price of delegation, the agency cost.

The same logic applies with full force to government, which is one reason this book treats state action with the same scepticism as market outcomes. Citizens are principals and elected officials their agents; legislators, in turn, are principals to the officials who carry out their laws. Each link has the two ingredients that create agency costs. Interests diverge, because politicians want to be re-elected and officials may prefer larger budgets and quieter lives, and information is asymmetric, because voters cannot follow most of what is decided in their name. Since a single vote almost never changes an outcome, it is rational for most people to remain largely uninformed about policy, a condition economists call rational ignorance, while small, organised groups with a great deal at stake follow every detail. This insight, developed by James Buchanan and Gordon Tullock in *The Calculus of Consent* and recognised with Buchanan's Nobel Prize in 1986, is the foundation of public choice theory. It explains why public programmes, like private bonus schemes, can drift away from the purposes for which they were designed, and why constitutional limits, transparency, and competition between jurisdictions matter as much as good intentions.

Case study: the real-estate agent and the financial crisis

Start with the everyday version. Suppose you want to sell your house and you hire an agent to represent you. You, the principal, want the highest possible price. The agent earns a percentage commission, so the agent also wants a high price, which makes it tempting to assume your interests are aligned. They are aligned only partly, and the gap is where the problem lives.

Put numbers on it. Imagine the house would fetch about three hundred thousand if you are willing to wait a couple of months, but only two hundred and eighty thousand if you insist on selling within a week. Holding out for the higher price is worth twenty thousand to you. To the agent, on a commission of, say, two and a half per cent, that same twenty thousand is worth only about five hundred, while a quick sale frees them to collect their fee now and move on to the next client. The agent's incentive to put in the extra effort, and bear the extra risk, of holding out for the best offer is therefore far weaker than yours, even though, on paper, you are on the same side. Worse, the agent knows things you do not: how strong the interest really is, whether an offer is truly the best available, how hard they are actually working on your behalf. The conflict of interest is compounded by information you cannot observe.

The fix is to redesign the contract so that the agent's reward tracks yours more closely. A bonus for selling above an agreed target, or a commission that rises steeply with the final price, sharpens the agent's incentive to chase the offer you would prefer. No contract closes the gap completely, which is why some residual loss almost always remains, but a well-designed one narrows it.

Now scale the same structure up, and it explains a catastrophe. In the years before the financial crisis of 2008, the people who originated, packaged, rated, and traded mortgage-backed securities were agents acting for others: for shareholders, for clients, and ultimately for the wider economy. Many were paid large bonuses tied to short-term volume and short-term profit, while the long-term risks they created fell on someone else, the firm, its shareholders, taxpayers, and borrowers. Loan officers were rewarded for writing mortgages, not for whether they were repaid; traders were rewarded for this year's profit, not for the tail risk they accumulated; and because each agent bore little of the downside of their own decisions, the system as a whole took on far more risk than any principal would have chosen. The agency problem that costs a homeowner twenty thousand at the negotiating table is, structurally, the same problem that, multiplied across an industry and badly governed, helped bring the global financial system to the brink.

Review and practice

Discussion questions

1. Why are aligned interests not enough on their own to remove the agency problem, and why is information asymmetry not enough on its own either? Why does it take both?
2. Performance pay is meant to align an agent with a principal. Give a case where it backfired, and explain exactly what went wrong.
3. The financial crisis of 2008 has been called a giant principal-agent failure. Is that a fair description, or does it let individuals off the hook too easily?

Exercises

1. Using the estate-agent example, recompute the agent's extra commission and the seller's extra proceeds if the commission rate were five per cent instead of two and a half. Does the conflict of interest shrink?
2. Design an incentive contract for a salesperson that rewards sales volume without encouraging the sale of unsuitable products.
3. Identify the principal, the agent, and the hidden action in three relationships of your choice, for example patient and surgeon, shareholders and chief executive, or voter and politician.

Self-check

- Define agency cost and name its three components.
- Why can a principal rarely observe the agent's effort directly?
- What is residual loss?
- Give two ways a contract can better align an agent with a principal.
- Why might voters be rationally ignorant, and what follows for how governments behave?

Further Reading

- Bebchuk, L. A., & Tallarita, R. (2022). *The perils and questionable promise of ESG-based compensation* (ECGI Law Working Paper No. 671/2022). European Corporate Governance Institute.
https://www.ecgi.global/sites/default/files/working_papers/documents/theperilsandquestionablepromiseofesgbasedcompensationecgi.pdf
- Buchanan, J. M., & Tullock, G. (1962). *The calculus of consent: Logical foundations of constitutional democracy*. University of Michigan Press.
- Coates, J. C. (2023). *The problem of twelve: When a few financial institutions control everything*. Columbia Global Reports.
- Cohen, S., Kadach, I., Ormazabal, G., & Reichelstein, S. (2023). Executive compensation tied to ESG performance: International evidence. *Journal of Accounting Research*, 61(3), 805-853.
<https://doi.org/10.1111/1475-679X.12481>
- European Union. (2017). *Directive (EU) 2017/828 as regards the encouragement of long-term shareholder engagement (Shareholder Rights Directive II)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/dir/2017/828/oj>
- Greenstone, M., He, G., Jia, R., & Liu, T. (2022). Can technology solve the principal-agent problem? Evidence from China's war on air pollution. *American Economic Review: Insights*, 4(1), 54-70.
<https://doi.org/10.1257/aeri.20200373>
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305-360.
[https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)



4. Game Theory

Learning objectives

- Describe a game by its players, strategies, and payoffs, and classify it by type.
- Analyse the prisoner's dilemma and identify a Nash equilibrium.
- Explain how repetition and reputation can sustain cooperation.
- Recognise the limits of game theory as a predictive tool.

Game theory is the study of decisions whose outcomes depend not only on what you do but on what others do in response. It is, in a phrase, the science of strategy. Whenever the best move for one player depends on the anticipated moves of others, competing firms, bargaining governments, bidders at an auction, ordinary economics is not enough, and we need a framework for reasoning about mutual expectations.

Every game has three basic ingredients. The players are the decision-makers, whether individuals, firms, or countries. The strategies are the courses of action available to each player. The payoffs are the outcomes that result from the particular combination of strategies all the players choose. Crucially, your payoff depends on others' choices as well as your own, which is what makes the analysis strategic rather than merely individual.

Games come in contrasting types, and recognising the type is half the analysis. In cooperative games players can make binding agreements; in non-cooperative games they cannot, and must rely on self-interest holding the outcome together. In simultaneous games players move at the same time, without seeing each other's choice, as in a sealed-bid auction; in sequential games they move in turn and can react, as in chess or a price war. In zero-sum games one player's gain is exactly another's loss, so the pie is fixed; in non-zero-sum games the players' interests are partly aligned, and cooperation can leave everyone better off or conflict leave everyone worse.

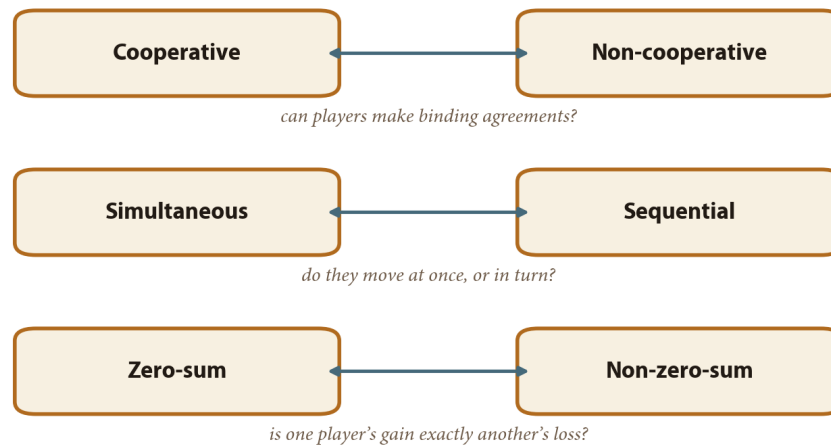
Three ways to classify a game

Figure 7. Three ways to classify a game.

The most instructive single game is the prisoner's dilemma. Two suspects are interrogated separately. Each is offered a deal: betray the other and go free while the other takes the heavier sentence; if both betray, both are punished moderately; if both stay silent, both get only a light sentence. Whatever the other does, each is individually better off betraying, so two rational players both betray and both end up worse than if they had cooperated. The dilemma captures countless business and social situations, from price wars and advertising arms races to overfishing and pollution, in which individually rational choices produce a collectively poor result. Its most hopeful lesson is that when the game is played repeatedly, the shadow of future encounters can sustain cooperation, because betrayal today invites retaliation tomorrow, which is one reason long-term business relationships behave so differently from one-off deals. The same mechanism underlies the reputation systems of Chapter 2 and the ratings that platforms use to make strangers trustworthy (Chapter 5): they turn what would be a one-off encounter into something closer to a repeated game, because a seller's behaviour today is visible to tomorrow's buyers.

		Prisoner B	
		Stay silent	Confess
Prisoner A	Stay silent	-1, -1 <i>both get a light sentence</i>	-3, 0 <i>A is betrayed</i>
	Confess	0, -3 <i>B is betrayed</i>	-2, -2 <i>both betray: Nash equilibrium</i>

Each does better by confessing, so both confess and both lose.

Figure 8. The prisoner's dilemma: individually rational choices, a collectively poor outcome.

The central solution concept is the Nash equilibrium, named after John Nash. It describes a combination of strategies in which no player can do better by unilaterally changing course, given what everyone else is doing. At a Nash equilibrium each player's strategy is a best response to the others', so the situation is self-enforcing and stable. In business terms it resembles a settled market in which no firm sees an advantage in changing its current price or product, given its rivals' choices. A game can have one such equilibrium, several, or none in pure strategies, and identifying it is often the key to predicting how a strategic situation will resolve.

Managers use these ideas constantly, if not always by name. In an oligopoly of a few large firms, each must anticipate that a price cut will be matched, which can deter the cut or trigger a damaging price war; game theory clarifies when each is likely. In auctions, the right bidding strategy depends on the rules and on what rivals are expected to bid. In negotiations over mergers, supplier contracts, or labour, understanding the other side's options and outside alternatives is decisive. And firms use strategic reasoning to deter entry, to build reputations, and to choose when cooperation serves them better than rivalry.

Game theory is powerful but not a crystal ball. Real players are not perfectly rational; they misjudge, act on emotion, and operate with incomplete and often wrong information. Real situations are messier than tidy models, with many players, shifting rules, and outcomes that unfold over time. The value of game theory is less in delivering exact predictions than in disciplining how we think: it forces us to put ourselves in the other side's position, to anticipate responses rather than assume a static world, and to see where our own incentives may be leading us astray.

In brief

- Strategy under interdependence. Game theory analyses decisions whose payoffs depend on the choices of others, not yours alone.
- Three ingredients. Players, strategies, and payoffs define any game.
- Know the type. Cooperative or not, simultaneous or sequential, zero-sum or not: the type shapes the analysis.
- The prisoner's dilemma. Individually rational choices can yield a collectively bad result, though repetition can sustain cooperation.
- Nash equilibrium. A self-enforcing outcome in which no player can gain by changing strategy alone.
- A discipline, not an oracle. It improves strategic thinking but is limited by irrationality, complexity, and imperfect information.

Case study: price wars and the bargaining table

Game theory earns its keep in two very different business settings, and it is worth seeing both. The first is the price war, which is a prisoner's dilemma in disguise. Imagine two airlines competing on the same route. If both hold their fares, both earn a healthy margin. If one cuts its fare while the other holds, the cutter fills its planes and steals the market. So each reasons that, whatever the rival does, it is better off cutting, and both cut. The result is a Nash equilibrium in which fares are driven down toward cost and both airlines earn far less than if they had simply held, exactly the collectively poor outcome the dilemma predicts. The same logic plays out in supermarket price wars, mobile-data plans, and advertising arms races, where everyone spends more and no one gains a lasting edge.

The most important insight is what changes when the game is repeated. Airlines do not meet once; they compete on the same routes day after day, year after year. In a repeated game, a fare cut today invites retaliation tomorrow, and the threat of a sustained war can be enough to keep both firms disciplined without any explicit agreement. This is why long-lived rivals often settle into a stable, if fragile, truce, and also why competition authorities watch such industries closely, because the line between tacit, lawful restraint and illegal collusion can be thin.

The second setting is explicit bargaining, and trade negotiations are the textbook example. In the talks that produced the Trans-Pacific Partnership, many countries bargained at once, each with its own goals on market access, intellectual property, labour, and environmental standards, and each one's best move depended on what the others would accept. Negotiators used strategic reasoning to anticipate responses, to sequence their concessions, to build coalitions of countries with aligned interests, and to find the trade-offs where enough parties could gain to say yes. Understanding each side's alternatives, what it would do if the talks collapsed, was the key to knowing who held leverage.

The episode also shows that strategic situations keep evolving, so the analysis is never finished. The United States, a driving force in the original deal, withdrew in 2017; the remaining eleven countries renegotiated it as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, which entered into force in 2018; and the United Kingdom later acceded, joining in 2024. Each move rewrote the payoffs for everyone else and triggered a fresh round of calculation. Whether the game is a price war or a treaty negotiation, the lesson is the same: you cannot choose well by looking only at your own options, because the outcome depends on the choices of others, who are reasoning about you in turn.

Review and practice

Discussion questions

1. Why do two rational firms in a price war both end up worse off, and why might the same two firms avoid the war if they expect to compete for many years?
2. Is a Nash equilibrium always a good outcome for the players? Use the prisoner's dilemma to support your answer.
3. Game theory assumes players are rational. Where does that assumption most mislead, and does it make the theory useless or merely incomplete?

Exercises

1. Draw the payoff matrix for two airlines choosing to hold or to cut their fares. Invent plausible payoffs, then identify the Nash equilibrium.
2. Classify three real strategic situations along each of the chapter's axes: cooperative or non-cooperative, simultaneous or sequential, and zero-sum or non-zero-sum.
3. Using the TPP and CPTPP example, explain how one player leaving a negotiation changes the payoffs for everyone who remains.

Self-check

- Name the three ingredients of any game.
- Define a Nash equilibrium in your own words.
- Why can repetition sustain cooperation in a prisoner's dilemma?
- State one major limitation of game theory in the real world.

Further Reading

Axelrod, R. (1984). *The evolution of cooperation*. Basic Books.

<https://www.basicbooks.com/titles/robert-axelrod/the-evolution-of-cooperation/9780465005642/>

Dixit, A. K., & Nalebuff, B. J. (2008). *The art of strategy: A game theorist's guide to success in business and life*. W. W. Norton.

<https://wwnorton.com/books/9780393337174>

Gneezy, U. (2023). *Mixed signals: How incentives really work*. Yale University Press.

Klein, T. (2021). Autonomous algorithmic collusion: Q-learning under sequential pricing. *The RAND Journal of Economics*, 52(3), 538-558.

Milgrom, P. R. (2021). Auction research evolving: Theorems and market designs. *American Economic Review*, 111(5), 1383-1405.

<https://doi.org/10.1257/aer.111.5.1383>

Osborne, M. J. (2003). *An introduction to game theory*. Oxford University Press.

<https://global.oup.com/ushe/product/an-introduction-to-game-theory-9780195128956>

Part II. Technology and the Organisation of Work

Part II applies those ideas to the technologies and business models that are changing how goods, services, and labour are exchanged: platforms that sell connections, ledgers that try to replace trusted intermediaries, software that automates tasks, crowds that supply ideas and effort, and global networks of suppliers. The same questions return in every chapter: who knows what, whose interests are aligned, and what makes cooperation between strangers possible.



5. Platforms and the Sharing Economy

Learning objectives

- Explain how multi-sided platforms create value through cross-side network effects.
- Explain why platform markets tend to tip and what keeps them contestable.
- Link a platform's trust infrastructure to signalling, screening, and reputation.
- Outline the EU and Romanian rules that now govern platforms and platform work.

A platform is a business whose product is a connection. Rather than making a good and selling it, a platform brings two or more groups together and makes it easier, cheaper, and safer for them to transact: hosts and guests, drivers and riders, advertisers and audiences, developers and users. This sounds modest, but it has turned out to be one of the most powerful business models of the digital age, and it behaves in ways that the economics of a traditional firm does not prepare us for.

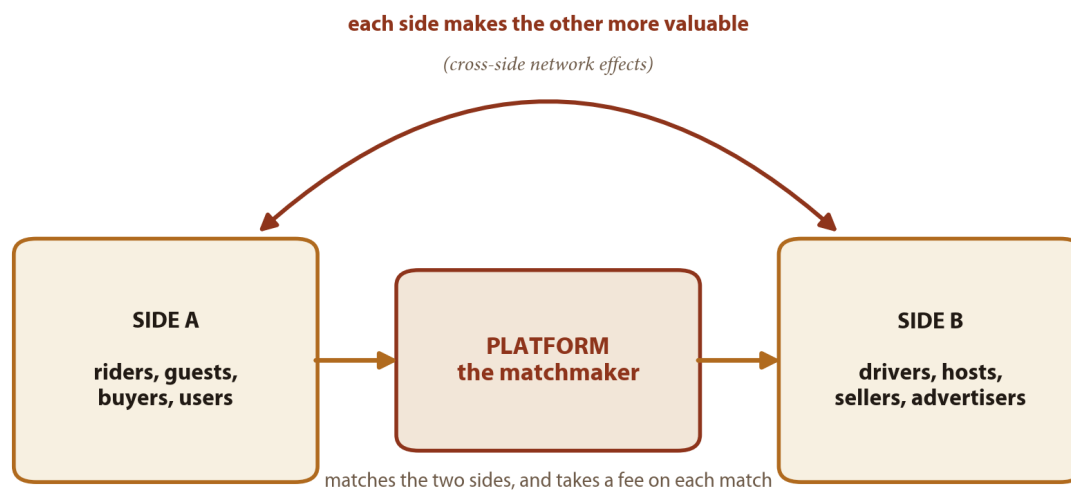


Figure 9. A platform as a multi-sided market, connecting two sides and taking a fee on each match.

The engine of a platform is the network effect. A telephone is useless if no one else has one and valuable when everyone does; the value of the device rises with the number of other users. Platforms work the same way. A ride-hailing app is more useful to riders when more drivers are available, and more useful to drivers when more riders are looking, so each side makes the other more valuable. Economists call this a cross-side network effect, and it creates a hard problem at the start, the so-called chicken-and-egg problem: neither side wants to join until the other is already there. Getting through that cold start, often by subsidising one side heavily, is the central challenge of launching a platform and the reason so many fail before reaching critical mass.

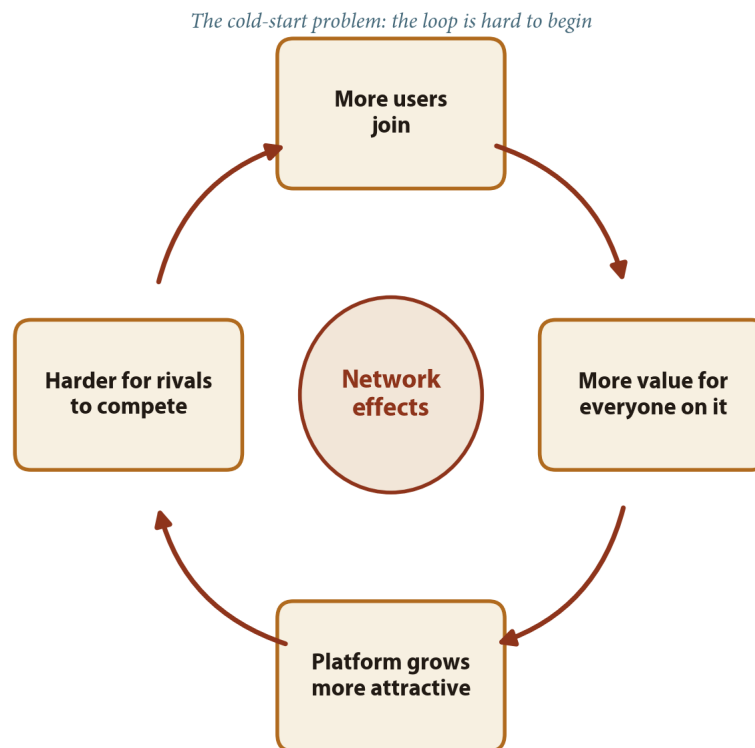


Figure 10. The network-effects flywheel, and the cold-start problem that makes it hard to begin.

Once a platform clears that hurdle, the same network effects work in its favour and can tip a market toward a single dominant player. Each new user makes the platform more attractive to the next, raising a barrier that competitors struggle to clear even with a better product, because what users value is partly the presence of everyone else. This is why platform markets often look monopolistic or close to it. The tendency is real but not absolute. Users can belong to several platforms at once, a habit known as multi-homing, and dominance can erode quickly when a platform stops serving its users well, so incumbency is an advantage rather than a guarantee.

Because a platform asks strangers to transact, trust is its most important and most fragile asset. The sharing economy in particular, the renting of homes, cars, tools, and time among people who do not know one another, only works because the platform manufactures enough trust to substitute for personal acquaintance. Ratings, reviews, identity verification, secure payments, insurance, and dispute resolution are not add-ons; they are the core product. A platform that loses control of trust, through fraud, fake reviews, or unsafe encounters, can unravel no matter how strong its network.

In the language of Part I, this trust infrastructure is a set of familiar remedies for information asymmetry. Ratings and reviews are a reputation mechanism that counters adverse selection (Chapter 2); identity checks, deposits, and vetting are forms of screening; and the prospect of a bad review disciplines behaviour after the deal is struck, turning a one-off encounter between strangers into something closer to the repeated game of Chapter 4, in which cooperation can be sustained.

Platforms create value by lowering the cost of finding and completing a transaction and by improving the quality of the match between the two sides. They capture a share of that value through commissions, subscriptions, advertising, or by monetising the data the transactions generate. That data is itself a competitive asset: it lets a platform match more precisely, price dynamically in response to real-time demand, and improve the experience in ways a newcomer cannot easily replicate. Managing a multi-

sided market means constantly balancing the interests of groups that do not always agree, since a change that pleases riders may anger drivers, and a fee that suits sellers may drive away buyers.

Platforms have run repeatedly into regulation, especially where they enter sectors that were already heavily regulated for good reasons, such as transport, lodging, and labour. In the European Union two instruments now shape the field directly. The Digital Services Act sets obligations for online platforms around illegal content, transparency, and the protection of users, with the heaviest duties falling on the very largest. The Digital Markets Act designates the biggest platforms as gatekeepers and imposes rules intended to keep their markets open to competitors. A third instrument speaks to the sharing economy's labour question: the Platform Work Directive, adopted in 2024, introduces a rebuttable presumption that a platform worker is an employee where the platform exercises control over the work, and it requires transparency about the algorithms that assign, rate, and discipline workers. Member states must bring it into national law by December 2026, which will reshape how delivery and ride-hailing platforms operate across the bloc.

Romania offers a local illustration of how regulation of platforms tends to arrive in stages. Ride-hailing operated in a legal grey zone until Government Emergency Ordinance 49/2019, later approved by Law 204/2019, created a separate regime for alternative transport, requiring platforms to obtain a technical permit and drivers to hold a professional certificate and a clean criminal record. The long dispute that preceded and followed these rules, with taxi operators pressing for restrictions on their new rivals and the platforms warning that further limits would drive them out, is a reminder that regulating a new market is also a contest between incumbents and entrants, and that the rules which emerge reflect that contest as well as the public interest. Like every member state, Romania must also bring the Platform Work Directive into national law by December 2026.

Finally, platforms generate externalities, effects that fall on people who are not party to the transaction. Some are positive, such as better use of idle assets and access to services in places traditional providers ignored. Others are contested: short-term rentals have been blamed for pushing up rents and hollowing out neighbourhoods, and gig work has raised questions about security and rights. A serious manager, and a serious student, has to weigh both sides rather than treating the platform model as either an unambiguous good or an unambiguous threat.

In brief

- Platforms sell connections. They match two or more groups and profit by reducing the cost and risk of transacting between them.
- Network effects are the engine. Each side makes the other more valuable, which creates a cold-start problem and, once solved, a tendency toward dominance.
- Dominance is strong but contestable. Multi-homing and the risk of losing users keep even large platforms disciplined.
- Trust is the core product. Ratings, verification, payments, and insurance substitute for personal acquaintance and are essential, not optional.
- Regulation has caught up. The EU's DSA, DMA, and 2024 Platform Work Directive now govern content, competition, and gig-worker status.
- Mind the externalities. Effects on housing, congestion, and labour fall on third parties and belong in any honest assessment.

Case study: Airbnb and the limits of a platform

Airbnb began in 2008 with a small, almost comic idea: its founders rented out air mattresses on their living-room floor to offset the rent on a San Francisco apartment. Within a decade it had become one of the largest accommodation businesses in the world, without owning a single room. That is the platform model in its purest form. Airbnb does not supply lodging; it connects people who have space with people who need it, and it makes money by taking a fee on each booking. Everything that makes the business work sits in the connection rather than the asset.

Its growth was driven by the network effects described in this chapter. Every new host made the platform more useful to travellers by widening choice, and every new traveller made it more attractive to hosts by raising the chance of a booking, so each side pulled the other in. Airbnb solved the hard problem at the centre of the sharing economy, persuading strangers to let other strangers sleep in their homes, by manufacturing trust where personal acquaintance was absent. Verified profiles, two-sided reviews, secure in-app payment, messaging, and host guarantees together substituted for the reputation a local guesthouse would have built over years. The result expanded the supply of lodging, gave travellers cheaper and more local options, and forced incumbent hotels to compete harder on price and experience.

The same growth produced externalities that fell on people who never used the platform. In cities with strong tourist demand, landlords found that letting a flat to visitors night by night could earn more than renting it to residents, and as units shifted from the long-term to the short-term market, critics blamed Airbnb for raising rents and hollowing out residential neighbourhoods. Because these costs landed on third parties, they were exactly the kind of problem a market price does not capture, and the response came through regulation. New York effectively curtailed short lets with strict registration rules in 2023; Barcelona moved to phase out tourist-apartment licences; and in 2024 the European Union adopted a regulation to standardise short-term-rental data so that local authorities could actually enforce their own limits.

Airbnb's arc is a compact lesson in platform economics. It shows how network effects and a trust infrastructure can build a vast business out of other people's assets, and it shows how the externalities of that business eventually catch up with it. Ride-hailing followed a parallel path: Uber used an app, dynamic pricing, and a large pool of drivers treated as independent contractors to outcompete traditional taxis, and it too ran into the limits of the model, this time over labour, as the United Kingdom's Supreme Court ruled in 2021 that its drivers were workers entitled to minimum pay and holiday rights, and the EU's 2024 Platform Work Directive pushed the whole sector toward clearer protections. In both cases the platform did not fail; it matured, and society negotiated the terms on which it would be allowed to operate.

Review and practice

Discussion questions

1. Why do platform markets so often tip toward a single winner, and what, if anything, stops the winner from charging whatever it likes?
2. Airbnb expanded the supply of lodging but is blamed for raising rents. How should a city weigh these effects when deciding whether to restrict short-term lets?
3. The Platform Work Directive presumes a gig worker is an employee where the platform controls the work. Does this protect workers or strip away the flexibility many of them chose? Make the strongest case on each side.

Exercises

1. Pick a platform you use and identify its two or more sides, the cross-side network effects between them, and the specific features it uses to manufacture trust.
2. Explain how you would solve the cold-start problem for a new home-cleaning marketplace, including which side you would subsidise first and why.
3. Classify three platforms by whether their users multi-home, and use that to predict how secure each platform's dominance is.

Self-check

- Can you define a cross-side network effect?
- Why is trust infrastructure described as the platform's core product rather than an add-on?
- What do the DSA, the DMA, and the Platform Work Directive each regulate?
- Give one positive and one negative externality of the sharing economy.
- How do ratings and reviews relate to the ideas of signalling, screening, and repeated games?

Further Reading

- European Commission. (n.d.). *The Digital Services Act package*. Shaping Europe's Digital Future.
<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
- European Union. (2022). *Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/reg/2022/1925/oj>
- European Union. (2024). *Directive (EU) 2024/2831 on improving working conditions in platform work*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/dir/2024/2831/oj>
- Government of Romania. (2019). *Ordonanța de urgență nr. 49/2019 privind activitățile de transport alternativ cu autoturism și conducător auto*. Monitorul Oficial al României.
<https://legislatie.just.ro/Public/DetaliiDocument/215598>
- Lehdonvirta, V. (2022). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. MIT Press.
- McIntyre, D. P., Srinivasan, A., Afuah, A., Gawer, A., & Kretschmer, T. (2021). Multisided platforms as new organizational forms. *Academy of Management Perspectives*, 35(4), 566-583.
- Rietveld, J., & Schilling, M. A. (2021). Platform competition: A systematic and interdisciplinary review of the literature. *Journal of Management*, 47(6), 1528-1563.
<https://doi.org/10.1177/0149206320969791>
- Schor, J. (2016). Debating the sharing economy. *Journal of Self-Governance and Management Economics*, 4(3), 7-22.
<https://greattransition.org/publication/debating-the-sharing-economy>
- Suciu, M. C., Năsulea, D. F., & Năsulea, C. (2020). Smart city innovation within the sharing economy. *Proceedings of the International Conference on Business Excellence*, 14(1), 1147-1157.
<https://doi.org/10.2478/picbe-2020-0107>
- Sutherland, W., & Jarrahi, M. H. (2018). The sharing economy and digital platforms: A review and research agenda. *International Journal of Information Management*, 43, 328-341.
<https://doi.org/10.1016/j.ijinfomgt.2018.07.004>



6. Blockchain and Smart Contracts

Learning objectives

- Explain how a distributed ledger and its consensus mechanism create trust without an intermediary.
- Weigh the benefits and dangers of self-executing smart contracts.
- Decide when a blockchain adds value over a conventional database.
- Describe how the EU's MiCA regulation governs crypto-assets.

Blockchain is best understood by the problem it tries to solve. Whenever two parties who do not trust each other want to keep a shared record, money owed, ownership of an asset, the history of a shipment, they have usually relied on a trusted third party to hold the authoritative copy: a bank, a registry, a clearing house. Blockchain proposes a different arrangement, in which the record is held in identical copies by many participants and kept in agreement by a set of rules rather than by a single custodian. It is, in short, an attempt to create trust without a trusted intermediary.

Seen through the lens of Part I, the attraction is easy to understand. An intermediary is an agent with interests of its own (Chapter 3), able to charge for its position, to make mistakes, or to be corrupted, and a consensus mechanism is a set of rules designed so that honest behaviour is each participant's best response (Chapter 4). Whether code can really replace the intermediary, and at what cost, is the question this chapter tries to answer.

Technically, a blockchain is a distributed ledger. Transactions are gathered into blocks, each block is cryptographically linked to the one before it, and the whole chain is replicated across a network of computers. Two properties follow. The ledger is decentralised, so no single party controls it, and it is effectively immutable, because altering a past record would require redoing the cryptographic work on every subsequent block across most of the network at once. What keeps the copies in agreement is a consensus mechanism. The best-known, proof of work, has participants compete to solve hard puzzles and is notoriously energy-hungry. The main alternative, proof of stake, instead selects validators in

proportion to the assets they pledge; when Ethereum switched to proof of stake in 2022 it cut its energy use by roughly ninety-nine per cent, which has reshaped the environmental debate around the technology.

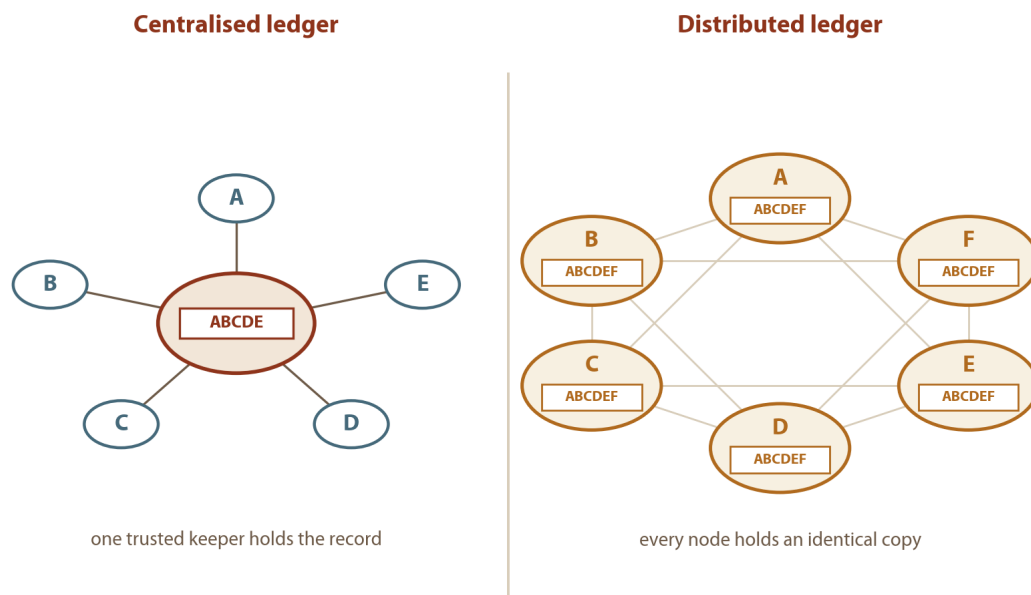


Figure 11. A centralised ledger versus a distributed one.

Smart contracts extend the idea from recording transactions to executing agreements. A smart contract is a program stored on the blockchain that runs automatically when its conditions are met: if a payment arrives, release the asset; if a deadline passes, refund the deposit. Because it runs on the ledger, it executes exactly as written, without a clerk or a court to interpret it, which removes intermediaries and the delays and costs they impose. The same property is also its greatest danger. Code that is immutable is immutable when it is wrong, and a bug cannot simply be patched after the fact. The most famous early lesson came in 2016, when an attacker drained tens of millions of dollars from a smart-contract investment fund by exploiting a flaw in its code, exposing the tension in the slogan that on a blockchain the code is the law.

For business, the honest assessment is that blockchain adds genuine value in a specific situation: when several parties who do not fully trust each other need to share a single authoritative record, and when no neutral intermediary is available or the intermediary is slow, costly, or capturable. Cross-border payments, trade finance, supply-chain provenance, and land registries all fit that description in principle. Where a trusted intermediary already exists and works well, a conventional database is usually simpler, faster, and cheaper, and the blockchain adds cost and complexity for little gain. Distinguishing the cases where the technology earns its keep from the cases where it is merely fashionable is the single most useful skill a manager can bring to it.

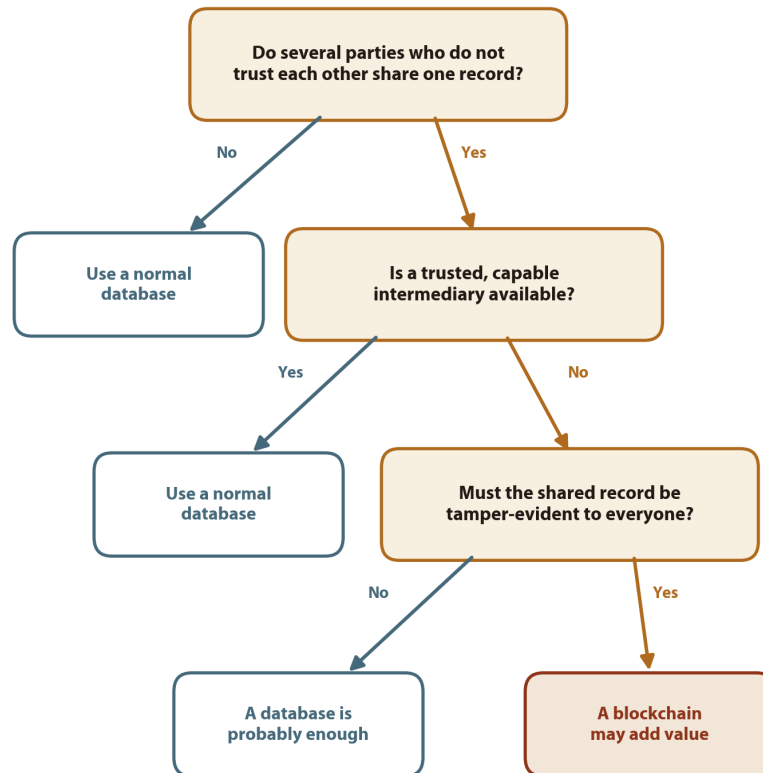


Figure 12. When does a blockchain add value? A decision tree.

The practical obstacles are real. Public blockchains have historically struggled to process transactions quickly and cheaply at scale, though newer designs have improved this. Implementations require scarce technical expertise. Many incompatible blockchains exist, so making them work together is itself a problem. And the speculative excesses of the sector have done lasting reputational damage. The collapse in 2022 of the Terra stablecoin and then of the FTX exchange, which entered bankruptcy that November amid allegations of fraud, wiped out enormous sums and made clear that the absence of intermediaries does not remove the need for sound governance and honest accounting.

Regulators have responded by building frameworks. The European Union's Markets in Crypto-Assets regulation, known as MiCA, became the first comprehensive regime of its kind. Its rules for stablecoins applied from mid-2024 and the rules for crypto-asset service providers from the end of 2024, with a transitional window for existing firms running into 2026. MiCA requires service providers to be authorised, imposes reserve and disclosure rules on stablecoin issuers, and has already pushed non-compliant tokens off regulated European venues. The United States moved separately, passing dedicated stablecoin legislation in 2025. The direction of travel is clear: the technology is being brought inside the regulatory perimeter rather than left outside it, which is likely to favour serious applications over speculative ones.

In brief

- Trust without an intermediary. A blockchain keeps a shared, replicated record in agreement through rules rather than a single custodian.
- Decentralised and immutable. Past records cannot be quietly altered; consensus mechanisms keep copies in agreement, with proof of stake far less energy-hungry than proof of work.
- Smart contracts cut out the middleman. Self-executing code removes intermediaries but executes its mistakes just as faithfully as its intentions.
- Value is situational. Blockchain helps when distrustful parties need one shared record and no good intermediary exists; otherwise a database is usually better.
- Hype carried real costs. The 2022 collapses of Terra and FTX showed that removing intermediaries does not remove the need for governance.
- Regulation has arrived. The EU's MiCA framework now governs crypto-assets and is bringing the sector inside the regulatory perimeter.

Case study: Georgia's blockchain land registry

For most of its post-Soviet history, the Republic of Georgia struggled with a land-registration system that was slow, opaque, and vulnerable to corruption. Records were held in ways that officials could quietly alter, ownership could be disputed or even forged, and the resulting uncertainty discouraged investment and eroded public trust in the state itself. Secure property rights are a precondition for a functioning market economy, because no one will build on, lend against, or improve land they cannot be sure they own, so the weakness of the registry was not a mere administrative inconvenience but a brake on the whole economy.

In 2016 Georgia's National Agency of Public Registry partnered with the technology firm Bitfury to address the problem with a blockchain. The design was deliberately modest and, for that reason, instructive. The substantive registry continued to run on conventional government systems, but a cryptographic fingerprint, a hash, of each land record and each transaction was published to a blockchain anchored to the Bitcoin network. Because that fingerprint is effectively impossible to alter after the fact, anyone could later verify that a given record had not been tampered with since it was registered. The blockchain was not asked to be the database; it was asked to do the one thing it does uniquely well, provide tamper-evidence, and nothing more.

The benefits followed from that narrow role. Citizens, banks, and officials gained a way to confirm that a title was genuine and unchanged, which made fraud far harder and rebuilt confidence in the register. Transactions became faster and cheaper to verify, and the project drew international attention as one of the earliest real deployments of blockchain in public administration, frequently cited as a model for other governments.

The honest lesson, however, is more measured than the early headlines suggested, and it is the lesson this chapter most wants students to take away. Georgia did not replace its institutions with a blockchain; it used a blockchain to make one specific institution harder to corrupt, while leaving the rest of the system in place. Several other countries that announced more ambitious blockchain land registries, attempting to move the entire registry on-chain, have seen mixed or disappointing results, precisely because they asked the technology to solve problems, such as resolving disputed claims or digitising messy historical records, that are really about law, administration, and politics rather than cryptography. The Georgian case is valuable not because it proves blockchain can run a government, but because it shows how to match the tool to the single trust problem it actually solves.

Review and practice

Discussion questions

1. “Blockchain is a solution looking for a problem.” Where is that judgement fair, and where is it unfair?
2. If a smart contract executes a bug faithfully and someone loses money as a result, who, if anyone, should bear the loss?
3. Did the 2022 collapses of Terra and FTX discredit the technology itself, or only the speculation that grew up around it?

Exercises

1. For three proposed uses, a national land registry, a coffee supply chain, and an internal company database, decide in each case whether a blockchain or an ordinary database is the better tool, and justify your choice.
2. Explain to a non-technical manager, in a short paragraph, why proof of stake uses far less energy than proof of work.
3. Outline what MiCA requires of a crypto exchange that wants to serve customers in the EU.

Self-check

- What problem is a blockchain fundamentally trying to solve?
- What makes a blockchain immutable, and why is that both a strength and a danger?
- When does a blockchain add real value over a conventional database?
- What is MiCA, and what does it govern?

Further Reading

Comuzzi, M., Grefen, P., & Meroni, G. (2023). *Blockchain for business: IT principles into practice*. Routledge.

<https://www.routledge.com/p/book/9781032342467>

European Union. (2023). *Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA)*. Official Journal of the European Union.

<https://eur-lex.europa.eu/eli/reg/2023/1114/oj>

Harvey, C. R., Ramachandran, A., & Santoro, J. (2021). *DeFi and the future of finance*. Wiley.

Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, 103(2), 153-174.

<https://doi.org/10.20955/r.103.153-74>

Suciu, M. C., Năsulea, C., & Năsulea, D. F. (2019). Towards developing a friendlier regulatory framework for blockchain-based businesses. *Theoretical and Applied Economics*, Special Issue, 15-24.

<https://www.researchgate.net/publication/335755763>

Suciu, M. C., Năsulea, C., & Năsulea, D. (2020). Knowledge decentralization in the age of blockchain: Developing a knowledge-transfer system using digital assets. In F. Matos, V. Vairinhos, I. Salavisa, L. Edvinsson, & M. Massaro (Eds.), *Knowledge, people, and digital transformation* (pp. 261-274). Springer.

https://doi.org/10.1007/978-3-030-40390-4_17

Taherdoost, H. (2023). Smart contracts in blockchain technology: A critical review. *Information*, 14(2), Article 117.

<https://doi.org/10.3390/info14020117>



7. Robots, RPA, AI and the Future of Work

Learning objectives

- Distinguish mechanical automation, RPA, generative AI, and agentic AI.
- Analyse the effects of automation at the level of tasks rather than whole jobs.
- Identify the ethical risks of automated decisions and the agency problem of delegating to algorithms.
- Outline the phases of the EU AI Act as amended by the 2026 Digital Omnibus.

Few questions provoke more anxiety, or more wishful thinking, than what automation will do to work. The honest answer is that automation does not simply abolish jobs; it changes what jobs consist of, which tasks command a wage, and which skills are scarce. To think clearly about the future of work we need to separate three technologies that are often lumped together: ordinary mechanical automation, robotic process automation, and artificial intelligence.

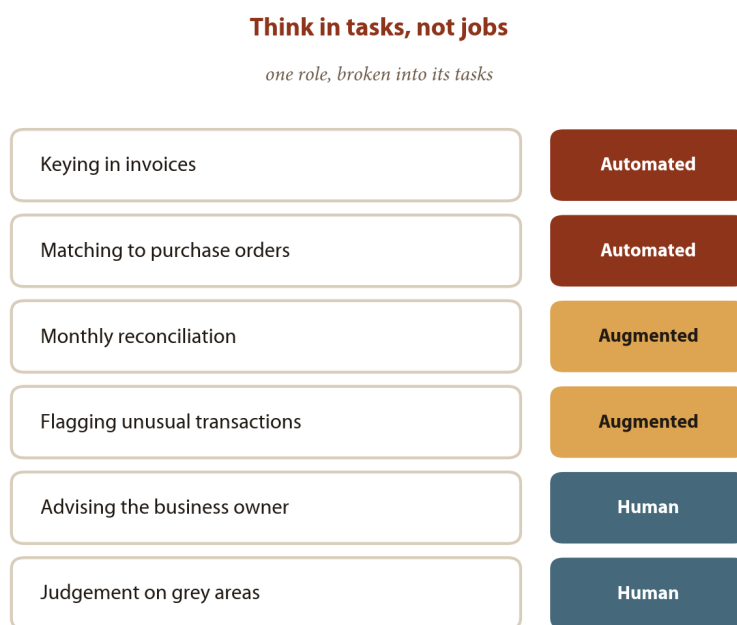
Robotic process automation, usually shortened to RPA, is the least glamorous and, for most firms, the most immediately useful. An RPA tool is a piece of software that mimics the keystrokes and clicks a human clerk would perform: it logs into systems, copies figures from one screen to another, checks one record against another, and follows a fixed set of rules. It does not understand what it is doing, and it breaks the moment the underlying forms change. Within its narrow lane, however, it is fast, tireless, and accurate, which is why it took hold first in high-volume back-office work such as invoicing, payroll, and claims handling.

RPA is also one of Romania's best-known contributions to the global technology industry. UiPath was founded in Bucharest in 2005 by Daniel Dines and Marius Tîrcă, under the name DeskOver, and took its present name in 2015. It grew into one of the world's leading RPA companies, and its listing on the New York Stock Exchange in April 2021 raised about 1.3 billion dollars, one of the largest software flotations in American history. Its path, from a small Bucharest start-up to a global platform that now combines

software robots with AI agents, follows the same evolution this chapter describes, from rule-following automation towards systems that learn.

Artificial intelligence is a broader and more slippery term. The systems that have reshaped expectations since 2022 are large generative models that produce text, images, code, and audio, and that can be steered with ordinary language rather than programming. More recently, so-called agentic systems have begun to chain such models together with tools and memory so that they can carry out multi-step tasks with limited supervision. Where classical RPA follows a script, these systems generalise from patterns in data, which makes them powerful in unstructured situations and, at the same time, less predictable and harder to audit.

The effect on jobs is best understood at the level of tasks rather than whole occupations. Most jobs are bundles of tasks, some routine and some not. Automation tends to absorb the routine, codifiable parts first. This produces three movements at once. Some roles that are almost entirely routine are displaced. New roles appear that did not exist before, from prompt design and model evaluation to the oversight of automated pipelines. And a great many existing roles are augmented, with workers handing the repetitive portion of their work to a machine and spending more of their time on judgement, exceptions, and dealing with people. The net effect on employment in any given sector depends on which of these movements dominates, and that is an empirical question, not something that can be settled from first principles.



The routine tasks are automated first; judgement and people stay human.

Figure 13. A job, broken into its tasks: which are automated, which augmented, and which stay human.

Because the routine layer is the first to go, the skills that gain in relative value are the ones machines still handle poorly. Empathy, persuasion, creative framing, the ability to define a problem rather than solve a pre-defined one, and sound judgement under uncertainty all become more valuable, not less. So does a basic technological literacy. Few workers need to build models, but almost everyone now needs to understand what these tools can and cannot reliably do, how to check their output, and where their failure modes lie. Because the technology keeps moving, the single most durable skill is the disposition to keep learning.

Automation also forces ethical questions into the open. Models trained on historical data can reproduce and amplify the biases in that data, with real consequences when they are used to screen job applicants, price insurance, or allocate credit. Automated decisions can be opaque, leaving the people affected by them with no meaningful explanation and no clear route to challenge a result. And the gains and losses from automation are rarely shared evenly. Responsible adoption means treating these as design problems to be addressed, not as unavoidable side effects to be excused.

Delegating a task to an algorithm also creates a principal-agent relationship of a new kind (Chapter 3). The system pursues the objective it was given, which may differ in subtle ways from what its owner actually wants, and its reasoning can be as hard to observe as an employee's effort. The familiar remedies of monitoring, testing, and carefully designed objectives apply, and so does the familiar warning that an agent rewarded for hitting a measure will find ways of hitting the measure rather than serving the purpose behind it.

Regulators have moved from principles to binding rules. The European Union's Artificial Intelligence Act, the first comprehensive law of its kind, takes a risk-based approach: it bans a small set of practices outright, imposes heavy obligations on systems classified as high risk, and requires lighter transparency measures for everything else, including a duty to label AI-generated content. Its obligations arrive in phases. The prohibitions applied from February 2025 and the rules for general-purpose AI models from August 2025. Most of the transparency obligations, including the labelling of AI-generated content, followed in August 2026, with a grace period until December 2026 for systems already on the market. The requirements for high-risk systems were due at the same time, but in 2026 the EU amended the Act through a package known as the Digital Omnibus on AI, agreed in May and in force since July. It postponed the rules for stand-alone high-risk systems to December 2027 and those for AI built into regulated products to August 2028, and it softened the AI-literacy duty that had applied since February 2025: instead of every provider and deployer having to ensure that its staff are AI-literate, the Commission and the member states must now support them in building that literacy. The episode is a reminder that even landmark legislation keeps being adjusted as it meets practice, and that firms planning around regulatory deadlines face an uncertainty of their own. Any firm deploying AI that touches people in the EU still has to map its systems against these categories, whatever its own location.

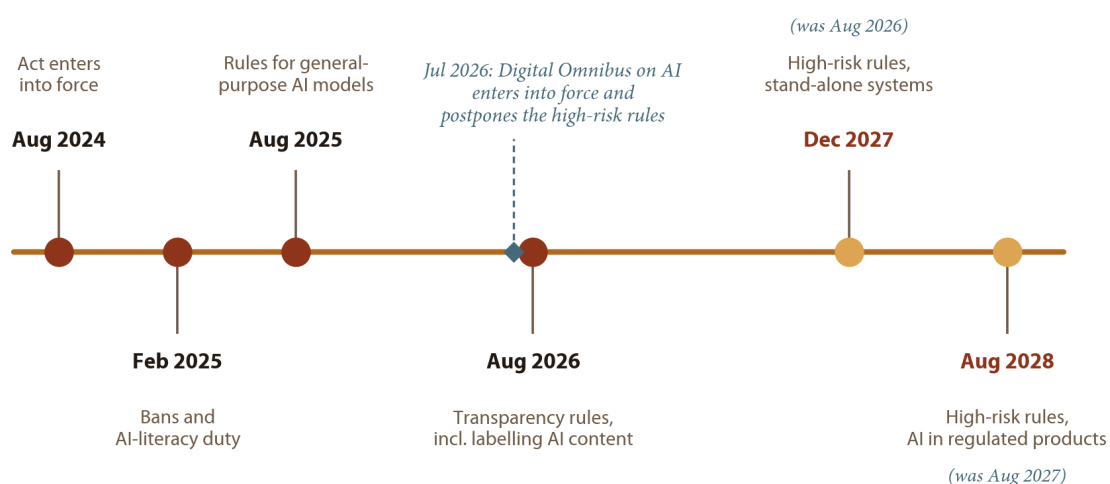


Figure 14. The phased application of the EU AI Act, as amended by the 2026 Digital Omnibus on AI, which postponed the high-risk rules.

The strategic lesson for managers is that adopting these tools is the easy part. The value comes from integrating them into how work is actually organised: redesigning processes around the new division of labour between people and machines, retraining staff for the tasks that remain human, and putting in place the oversight that keeps an automated system honest. Firms that treat automation as a bolt-on technology tend to be disappointed; those that treat it as a redesign of the work itself tend to capture the gains.

In brief

- Three distinct technologies. Mechanical automation, rule-following RPA, and pattern-learning AI differ in flexibility, predictability, and the kinds of work they affect.
- Think in tasks, not jobs. Automation displaces some roles, creates others, and augments many; the net effect on employment is an empirical question that varies by sector.
- Scarcity shifts to human skills. Judgement, creativity, communication, and a disposition to keep learning rise in relative value as routine tasks are automated.
- Ethics is a design problem. Algorithmic bias, opacity, and uneven gains must be addressed deliberately, not treated as inevitable.
- Regulation is now binding. The EU AI Act applies in phases from 2025 to 2028, after the 2026 Digital Omnibus postponed its high-risk rules, and reaches any firm whose AI affects people in the EU.
- Integration beats adoption. Value comes from redesigning processes and oversight around people and machines, not from buying a tool.

Case study: robotic process automation in a finance back office

Consider a large company, a utility, a retailer, or a manufacturer, that receives in the order of fifty thousand supplier invoices every month. Before automation, a team of clerks handled each one by hand: opening the email or scanning the paper, keying the details into the finance system, matching the invoice against the relevant purchase order and goods-received note, checking that it was not a duplicate, chasing the right manager for approval, and finally scheduling payment. The work was slow, repetitive, and easy to get wrong. Invoices sat in queues for days, early-payment discounts were missed, late-payment penalties crept in, and a meaningful share of staff time went into correcting keying errors rather than doing anything a person is uniquely good at.

Robotic process automation attacks exactly this kind of work. A software robot is configured to reproduce the clerk's steps: it collects each incoming invoice from a shared mailbox or supplier portal, and a document-understanding model reads the supplier name, invoice number, date, totals, tax, and individual line items, even when the layout varies from one supplier to the next. The robot then performs the three-way match against the purchase order and the goods-received note, queries the ledger to confirm the invoice has not already been paid, and applies the company's rules. Anything that reconciles cleanly and falls below a set value is approved automatically; anything above the threshold, or with a discrepancy, is routed to the right person with the relevant documents already attached. Once approved, the robot files the payment instruction, notifies the supplier and the requester, and writes a complete log of every action.

The gains are large and measurable. Invoices that once took several days now clear in minutes when they match, the share processed without any human touch, the straight-through rate, climbs steadily as the rules are refined, keying errors fall close to zero, and the cost of processing each invoice drops sharply. Just as important, the audit trail is now complete and consistent, which makes the finance function easier to control and to audit. The clerks are not simply removed; the most routine part of their work is, and they are redeployed to handle the exceptions the robot flags, to manage supplier relationships, and to investigate the disputes that genuinely need judgement.

The case also shows the limits of the technology, which is why it belongs in a chapter about thinking clearly. The robot follows rules and breaks the moment an underlying screen or form changes, so it needs monitoring, maintenance, and clear ownership; treated as a one-off installation it quietly decays. Pairing brittle rule-following with a flexible document-reading model is what makes the modern version robust, and it is a small, concrete illustration of the chapter's central point: the value comes not from buying an automation tool but from redesigning the process, and the division of labour between people and machines, around it.

Review and practice

Discussion questions

1. “Automation does not abolish jobs, it changes them.” Do you find this reassuring or evasive? Argue both sides, using tasks rather than whole occupations as your unit of analysis.
2. Which is the more serious danger when an AI system is used to screen job applicants: that it may be biased, or that no one can explain its decisions? Defend your ranking.
3. The EU AI Act bans a few uses outright and regulates others only lightly. Is a risk-based approach the right way to govern a fast-moving technology, or will it always lag the frontier?

Exercises

1. Take a job you know well and list its main tasks. Sort each into likely automated, likely augmented, and likely unaffected, then describe how the role as a whole would change.
2. A firm processes 40,000 invoices a month at an average of nine minutes each by hand. If automation cuts handling time to one minute on the 70 per cent that reconcile cleanly and leaves the rest unchanged, how many staff-hours a month does it save?
3. Draft a one-page responsible-adoption checklist a manager should apply before rolling out an AI hiring tool, covering bias, transparency, and human oversight.

Self-check

- Can you distinguish RPA, generative AI, and agentic AI, and give an example of each?
- Why is automation’s effect on total employment described as an empirical question rather than a matter of principle?
- Which human skills rise in relative value as routine tasks are automated, and why?
- Can you name the main phases of the EU AI Act’s timeline?
- Why is delegating a task to an AI system a kind of principal-agent problem?

Further Reading

- Acemoglu, D., Autor, D., Hazell, J., & Restrepo, P. (2022). Artificial intelligence and jobs: Evidence from online vacancies. *Journal of Labor Economics*, 40(S1), S293-S340.
<https://doi.org/10.1086/718327>
- Acemoglu, D., & Johnson, S. (2023). *Power and progress: Our thousand-year struggle over technology and prosperity*. PublicAffairs.
- Acemoglu, D., & Restrepo, P. (2019). Automation and new tasks: How technology displaces and reinstates labor. *Journal of Economic Perspectives*, 33(2), 3-30.
<https://doi.org/10.1257/jep.33.2.3>
- Agrawal, A., Gans, J., & Goldfarb, A. (Eds.). (2019). *The economics of artificial intelligence: An agenda*. University of Chicago Press.
<https://www.nber.org/books-and-chapters/economics-artificial-intelligence-agenda>
- Arntz, M., Gregory, T., & Zierahn, U. (2020). Digitization and the future of work: Macroeconomic consequences. In K. F. Zimmermann (Ed.), *Handbook of labor, human resources and population economics* (pp. 1-29). Springer.
https://doi.org/10.1007/978-3-319-57365-6_11-1
- European Commission. (n.d.). *Timeline for the implementation of the EU AI Act*. AI Act Service Desk.
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act>
- European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- European Union. (2026). *Regulation (EU) 2026/1744 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/reg/2026/1744/oj>
- National Academies of Sciences, Engineering, and Medicine. (2024). *Artificial intelligence and the future of work*. The National Academies Press.
<https://doi.org/10.17226/27644>
- Syed, R., Suriadi, S., Adams, M., Bandara, W., Leemans, S. J. J., Ouyang, C., ter Hofstede, A. H. M., van de Weerd, I., Wynn, M. T., & Reijers, H. A. (2020). Robotic process automation: Contemporary themes and challenges. *Computers in Industry*, 115, Article 103162.
<https://doi.org/10.1016/j.compind.2019.103162>
- Webb, M. (2019). *The impact of artificial intelligence on the labor market* [Working paper]. SSRN.
<https://doi.org/10.2139/ssrn.3482150>



8. Crowdsourcing

Learning objectives

- Define crowdsourcing and classify its main forms.
- Weigh its advantages against its risks, above all quality control.
- Explain how reputation, peer review, and redundancy manage hidden quality and effort.
- Discuss the fairness of the crowd labour that trains artificial intelligence.

Crowdsourcing turns a crowd into a workforce. Instead of relying only on its own employees or contracted suppliers, an organisation invites a large, usually online group to contribute ideas, content, labour, or money. The premise is that a sufficiently large and varied crowd can supply knowledge, creativity, and effort that no single team possesses, and the internet makes assembling such a crowd cheap and fast for the first time in history.

Its appeal rests on four advantages. Diversity is the first: a wide and varied pool brings perspectives and skills an internal team would lack. Cost-efficiency is the second, since tapping the crowd can be far cheaper than conventional research or development. Speed is the third, with feedback, solutions, or funds arriving quickly. And the fourth is innovation, because opening a problem to outsiders invites the unexpected, out-of-the-box solution that insiders, steeped in the usual way of doing things, might never reach.

Crowdsourcing takes several recognisable forms. Idea generation gathers proposals for new products or solutions. Micro-tasking breaks a large job into tiny pieces distributed to many people, the model pioneered by Amazon's Mechanical Turk. Crowdfunding raises capital in small amounts from many backers through platforms such as Kickstarter and Indiegogo. Open innovation invites outsiders into a firm's research and development. And distributed data collection enlists volunteers to gather or classify information, as citizen-science projects do.

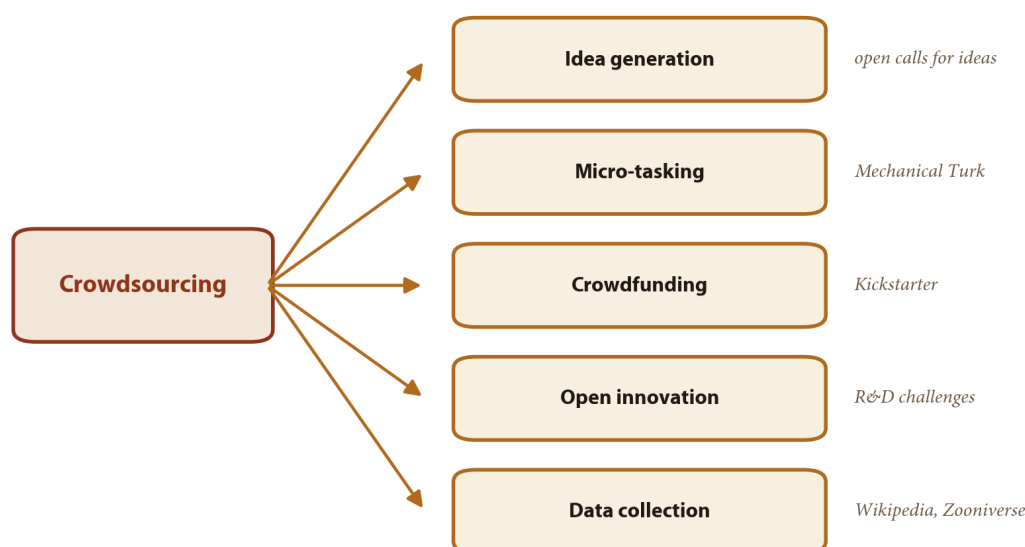


Figure 15. Five forms of crowdsourcing.

The model has real risks. Quality control is the central one: contributions from an open crowd vary enormously and must be filtered and verified. Ownership of what the crowd produces raises intellectual-property questions that should be settled in advance. Sustaining participation requires understanding what motivates contributors, which is rarely money alone, recognition, enjoyment, learning, and a sense of community often matter as much or more, and coordinating a dispersed, anonymous crowd is a genuine communication challenge. There is an ethical dimension too. When crowdsourcing shades into paid micro-work, the people doing it deserve fair compensation and transparent treatment rather than exploitation disguised as participation.

That ethical question has become unexpectedly central, because crowdsourcing now sits at the foundation of modern artificial intelligence. The systems discussed throughout this book are trained and refined on vast amounts of human labour: crowds of workers label images, transcribe audio, rank model outputs, and flag harmful content, and the technique of reinforcement learning from human feedback, in which people rate a model's answers to teach it what is helpful, is a form of crowdsourcing at industrial scale. Much of this work is low-paid and psychologically taxing, which has pushed the fairness of crowd labour from a side issue to a defining one. At the same time, generative AI is beginning to flow back into the crowd, as volunteer communities such as Wikipedia debate how to handle AI-generated contributions without eroding the human judgement that made them trustworthy. As the economy grows more interconnected, the power, and the responsibilities, of the crowd will only grow with it.

The promise and the risks of crowdsourcing both have roots in Part I. The promise is Hayek's insight from Chapter 1: useful knowledge is dispersed among many people, and the challenge is to find a mechanism that draws it together. The risks are information and incentive problems. An organisation cannot directly observe the quality or the effort behind each contribution, a principal-agent problem (Chapter 3) multiplied across thousands of anonymous agents, which is why successful projects rely on reputation scores, peer review, and redundancy, the same devices that overcome information asymmetry in Chapter 2.

In brief

- The crowd as workforce. Organisations source ideas, labour, content, or funds from a large online group rather than only from staff and suppliers.
- Four advantages. Diversity, cost-efficiency, speed, and a greater chance of unexpected innovation.
- Several forms. Idea generation, micro-tasking, crowdfunding, open innovation, and distributed data collection.
- Manage the risks. Quality control, intellectual-property rights, contributor motivation, and coordination all need deliberate attention.
- Ethics matter. Paid crowd work demands fair pay and transparency, not exploitation.
- It powers AI. Data labelling and human feedback are crowdsourcing at scale, making the fairness of crowd labour a defining issue.

Case study: Wikipedia

When Wikipedia launched in 2001, the idea sounded absurd. An encyclopedia that anyone on the internet could edit, written by unpaid volunteers with no central authority vetting their work, seemed destined to drown in error, vandalism, and nonsense. Two decades later it is one of the most visited websites in the world and, for most everyday purposes, a remarkably reliable reference, assembled almost entirely by a crowd. It is the purest large-scale demonstration of the promise, and the problems, set out in this chapter.

Wikipedia works because it harnesses every advantage of crowdsourcing at once. Its diversity is global, so an obscure subject that no single editorial board could cover finds someone, somewhere, who knows it. Its cost is astonishingly low, since contributors are volunteers and the project is run by a non-profit foundation. Its speed is extraordinary, with articles on breaking events taking shape within minutes as many hands add and correct in parallel. And it taps motivations that have nothing to do with money: the pleasure of sharing knowledge, the status earned within the community, and a genuine sense of common purpose.

It also shows how the risks of crowdsourcing can be managed rather than wished away. Quality control, the obvious danger, is handled not by a gatekeeper at the entrance but by the crowd itself: edits are visible and reversible, every change is logged, disputed pages can be locked, and a culture of citing sources lets readers and editors check claims. The result is a system that is self-correcting in the aggregate even though any single edit may be wrong. The other devices the chapter names appear too, in the volunteer administrators who resolve disputes, the bots that revert obvious vandalism, and the norms that hold a dispersed, anonymous community together.

Wikipedia is far from alone, and the other classic examples each highlight a different facet of the model. Waze and OpenStreetMap build live maps from the real-time reports of their users; Kickstarter and similar platforms raise capital in small amounts from many backers to finance projects that traditional funders would never touch; and Zooniverse lets volunteers help scientists classify galaxies or identify wildlife in camera-trap images. That last example points directly to the chapter's most current theme, because the same human classification that powers citizen science is exactly what now trains artificial intelligence. Fittingly, Wikipedia's community is itself debating how to handle AI-generated contributions without eroding the human judgement that made it trustworthy in the first place, the latest chapter in a long experiment in what crowds can build together.

Review and practice

Discussion questions

1. Why does Wikipedia work despite letting almost anyone edit it, and what would have to change for it to fail?
2. A great deal of AI is trained on low-paid crowd labour. Is this a fair exchange, exploitation, or something in between?
3. Should volunteer communities such as Wikipedia accept AI-generated contributions? What do they risk either way?

Exercises

1. For a problem of your choice, design a crowdsourcing approach: choose the type, idea generation, micro-tasking, crowdfunding, open innovation, or data collection, and explain how you would handle quality control and motivation.
2. List the non-monetary motivations that sustain an open-source project, then rank them by how reliable you judge each to be.
3. Explain how reinforcement learning from human feedback is, in effect, a form of crowdsourcing.

Self-check

- Define crowdsourcing.
- Name the four advantages it offers.
- What is the central risk of crowdsourcing, and how does Wikipedia manage it?
- How does crowdsourcing underpin modern artificial intelligence?
- Which ideas from Part I help explain both the promise and the risks of crowdsourcing?

Further Reading

European Union. (2024). *Directive (EU) 2024/2831 on improving working conditions in platform work*. Official Journal of the European Union.

<https://eur-lex.europa.eu/eli/dir/2024/2831/oj>

Howe, J. (2008). *Crowdsourcing: Why the power of the crowd is driving the future of business*. Crown Business.

<https://www.penguinrandomhouse.com/books/192616/crowdsourcing-by-jeff-howe/>

Muldoon, J., Graham, M., & Cant, C. (2024). *Feeding the machine: The hidden human labour powering AI*. Canongate Books.

Murgia, M. (2024). *Code dependent: Living in the shadow of AI*. Picador.

Ponti, M., & Seredko, A. (2022). Human-machine-learning integration and task allocation in citizen science. *Humanities and Social Sciences Communications*, 9, Article 48.

<https://doi.org/10.1057/s41599-022-01049-z>

Vermicelli, S., Cricelli, L., & Grimaldi, M. (2021). How can crowdsourcing help tackle the COVID-19 pandemic? *R&D Management*, 51(2), 183-194.

<https://doi.org/10.1111/radm.12443>



9. Outsourcing

Learning objectives

- Explain the make-or-buy decision through transaction costs, following Coase and Williamson.
- Classify the main types of outsourcing and the motives behind them.
- Manage a vendor relationship as a principal-agent problem.
- Assess how geopolitics, tariffs, and artificial intelligence are changing where work is done.

Outsourcing is the decision to have someone else do part of your work. Rather than perform every function in-house, a firm contracts a third party, at home or abroad, to handle certain processes, from running payroll to writing software to staffing a call centre. The logic is the logic of specialisation and the division of labour that has driven economic growth for centuries, applied to the modern firm and stretched across the globe by cheap communication.

Why do firms do anything in-house at all? Ronald Coase asked this question in 1937, and his answer still frames the outsourcing decision. Using the market is not free. Finding a supplier, negotiating terms, writing a contract, and checking that it is honoured all cost time and money, costs that Coase called the costs of using the price mechanism and that are now known as transaction costs. A firm exists because, for some activities, directing work internally is cheaper than buying it in the market, and it grows until the cost of organising one more activity inside equals the cost of buying it outside. Oliver Williamson later showed which activities tend to stay inside: those that require investments specific to one relationship, that are hard to describe fully in a contract, and that recur often, because these are where a supplier could most easily take advantage of the buyer once the investment has been made. Outsourcing decisions are, in effect, judgements about transaction costs, and the falling cost of communication and coordination explains much of the growth of outsourcing.

Firms outsource for several reasons that usually appear in combination. Cost reduction is the most cited, as work can be moved to regions where it can be done more cheaply. Focus is a subtler and often more

important motive: by delegating peripheral tasks, a company can concentrate its attention and capital on the core activities where it truly creates value. Outsourcing also buys access to specialised skills and technology a firm does not possess, provides scalability so that operations can expand or contract with demand without heavy fixed commitments, and can spread certain operational risks across partners.

The work outsourced falls into broad families. Business process outsourcing covers functions such as customer service, human resources, and finance. Information-technology outsourcing covers software development and the running of IT infrastructure. Knowledge process outsourcing covers higher-value, expertise-intensive work such as research, analytics, and legal services. The further up this ladder a task sits, the more the relationship depends on trust and capability rather than mere cost.

None of this is free of difficulty. The quality of outsourced work may fall short of expectations. Distance, culture, and time zones can breed miscommunication. Over-reliance on a single vendor creates dependency and exposes the firm to disruption. Sharing sensitive data with a third party raises security and intellectual-property risks. And the headline savings are often eroded by hidden costs of transition, training, and management. There are ethical dimensions too: outsourcing to places with weak labour protections raises real questions about working conditions, and shifting work abroad can cost jobs at home, with social and political consequences that firms cannot simply ignore. Managing all this well demands careful vendor selection, clear contracts with measurable performance standards, and an active, collaborative relationship rather than a transaction tossed over a wall. Sometimes the right answer is to reverse course, bringing work back in-house, known as insourcing, or moving it to a different vendor.

Every outsourcing contract is also a principal-agent relationship of the kind described in Chapter 3. The client is the principal and the vendor the agent; their interests overlap but do not coincide, since the vendor gains by economising on the effort it puts in, and the client usually cannot see exactly how the work is done. Service-level agreements, performance bonuses and penalties, audits, and the credible threat of moving to another vendor are the familiar tools of monitoring and incentive design, applied to a relationship between firms.

Two forces are reshaping the outsourcing landscape as this edition goes to press. The first is geopolitics. The pandemic's supply shocks, rising tensions between major powers, and war in Europe have made resilience as important as cost, prompting a shift from pure offshoring toward nearshoring, moving work to nearby countries, and friendshoring, concentrating it among political allies. Governments have joined in with tariffs and subsidies intended to bring production home, but these carry costs of their own: studies of the tariffs the United States imposed in 2018 found that their cost was passed almost entirely on to American importers and consumers rather than borne by foreign exporters, a reminder that the political appeal of reshoring is not the same as its economic case. The second is artificial intelligence, which strikes at the very heart of the outsourcing model. Much of what made business-process outsourcing attractive, large volumes of routine, rule-based work in call centres and back offices, is exactly what AI now automates. This threatens to hollow out parts of the industry in the countries that built their economies on it, even as it creates new demand for higher-skill work overseeing and improving the automated systems. The outsourcing question is no longer only where work should be done, but whether a person needs to do it at all.

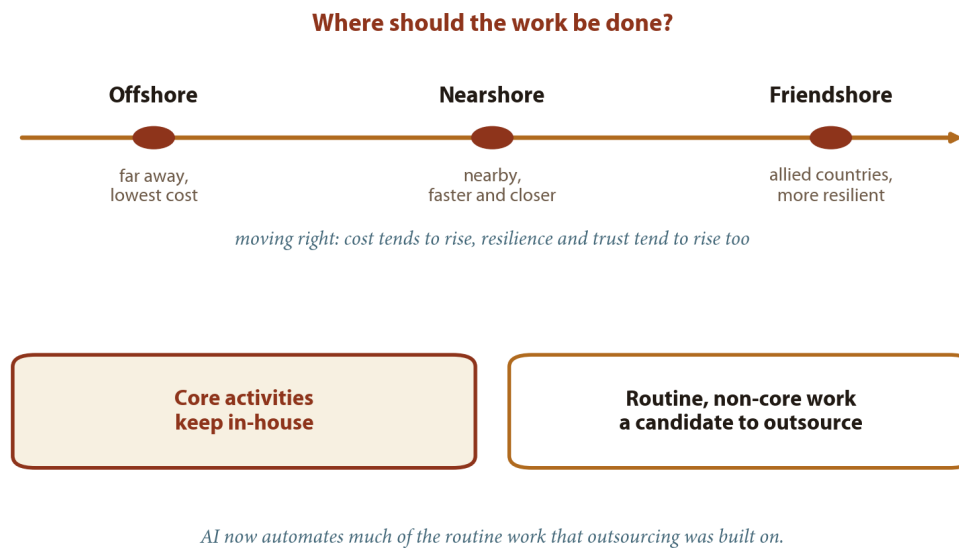


Figure 16. The outsourcing decision: where to locate work, and what to keep in-house.

In brief

- Specialisation across firms. Outsourcing applies the division of labour by contracting parts of the work to third parties.
- Several motives at once. Cost, focus on core competencies, access to expertise, scalability, and risk-sharing.
- A ladder of work. Business-process, IT, and knowledge-process outsourcing rely increasingly on trust over mere cost.
- Real risks and ethics. Quality, communication, dependency, security, hidden costs, labour conditions, and jobs at home.
- Geopolitics reshapes location. Resilience drives nearshoring and friendshoring alongside, or instead of, lowest-cost offshoring.
- AI reshapes the model itself. Automation of routine back-office work questions whether a person is needed at all.

Case study: Apple and the global supply chain

Apple designs some of the most recognisable and profitable products in the world, yet it manufactures almost none of them itself. Instead it orchestrates a vast global network of suppliers and assemblers to build them, a network concentrated for many years in China. Contract manufacturers such as Foxconn and Pegatron operate enormous facilities that assemble Apple's devices, while specialised firms across several countries supply the displays, processors, camera modules, and countless other components. Apple is, in effect, the conductor of an orchestra it does not own.

This is outsourcing as competitive strategy rather than mere cost-cutting. By contracting out manufacturing, Apple concentrates its own people and capital on what it judges itself best at, product design, software, and marketing, while leaving production to partners with the scale and expertise to do it at staggering volume and precision. The arrangement gives Apple flexibility to raise or cut output as demand shifts without owning the factories, and it keeps manufacturing costs low relative to the premium prices its products command, which is a large part of why its margins are the envy of the industry. The same arrangement also illustrates the textbook risk of dependency: a network this concentrated is exposed to disruption, as the world learned when pandemic shutdowns and component shortages rippled through it.

The strategy has drawn sustained ethical criticism, and the criticism maps precisely onto this chapter's warnings. Reports of long hours, harsh conditions, and worker distress at major assembly plants, together with environmental concerns across the supply chain, have dogged Apple for years and pushed it to publish supplier-responsibility standards and to audit its partners, with mixed and contested results. Outsourcing did not let Apple outsource responsibility, a lesson every firm that delegates production eventually confronts.

Most telling for the present moment is how the calculus is shifting. Trade tensions between the United States and China, tariffs, and a general drive for supply-chain resilience have pushed Apple to diversify its assembly beyond China toward countries such as India and Vietnam, the very move from offshoring toward nearshoring and friendshoring described earlier in the chapter. Cost is no longer the only variable; political risk and resilience now weigh heavily in the decision of where work should be done. And looming over the whole industry is the other force reshaping outsourcing, artificial intelligence, which is beginning to automate the routine call-centre and back-office work that built the outsourcing economies of South and Southeast Asia in the first place. Apple's supply chain, long the textbook example of why firms outsource, is becoming a live case study in how and why that logic is now changing.

Review and practice

Discussion questions

1. Apple outsources manufacturing but not design. What does that choice reveal about where it believes its value lies?
2. Is a firm responsible for the labour conditions at its outsourced suppliers? Where, if anywhere, does that responsibility end?
3. If AI automates the routine work on which outsourcing economies were built, what happens to those economies, and whose problem is it?

Exercises

1. For a company you know, identify one process it could sensibly outsource and one it should keep in-house, and justify each choice.
2. List the hidden costs that can erode the headline savings from outsourcing, and suggest how a manager should budget for them.
3. Explain the difference between offshoring, nearshoring, and friendshoring, and give a reason a firm might choose each.

Self-check

- Name three motives for outsourcing besides cost.
- Distinguish business-process, IT, and knowledge-process outsourcing.
- What is the risk of becoming dependent on a single vendor?
- Why is artificial intelligence described as a threat to the outsourcing model itself?
- According to Coase, why do firms exist at all?
- Why is an outsourcing contract a principal-agent relationship, and how can it be managed?

Further Reading

Alfaro, L., & Chor, D. (2023). *Global supply chains: The looming “great reallocation”* (NBER Working Paper No. 31661).

National Bureau of Economic Research.

<https://www.nber.org/papers/w31661>

Amiti, M., Redding, S. J., & Weinstein, D. E. (2019). The impact of the 2018 tariffs on prices and welfare. *Journal of Economic Perspectives*, 33(4), 187-210.

<https://doi.org/10.1257/jep.33.4.187>

Antràs, P. (2020). *De-globalisation? Global value chains in the post-COVID-19 age* (NBER Working Paper No. 28115).

National Bureau of Economic Research.

<https://www.nber.org/papers/w28115>

Coase, R. H. (1937). The nature of the firm. *Economica*, 4(16), 386-405.

<https://doi.org/10.1111/j.1468-0335.1937.tb00002.x>

European Union. (2024). *Directive (EU) 2024/1760 on corporate sustainability due diligence*. Official Journal of the European Union.

<https://eur-lex.europa.eu/eli/dir/2024/1760/oj>

Gereffi, G., Humphrey, J., & Sturgeon, T. (2005). The governance of global value chains. *Review of International Political Economy*, 12(1), 78-104.

<https://doi.org/10.1080/09692290500049805>

Goodman, P. S. (2024). *How the world ran out of everything: Inside the global supply chain*. Mariner Books.

Schniederjans, M. J., Schniederjans, A. M., & Schniederjans, D. G. (2010). *Outsourcing and insourcing in an international context*. Routledge.

<https://doi.org/10.4324/9781315701936>

Williamson, O. E. (1985). *The economic institutions of capitalism*. Free Press.

Part III. The Rules of the Digital Economy

Part III turns to the rules that govern the information economy: intellectual property, data protection, the regulation of online speech, and the contest between the largest technology firms and the states that try to govern them. Every rule examined here responds to a real problem, and every rule carries risks of its own. The aim throughout is to weigh the market failures that regulation targets against the government failures it can create, case by case.



10. Intellectual Property

Learning objectives

- Explain why ideas behave like public goods and why intellectual property exists.
- Distinguish patents, trademarks, copyright, and trade secrets.
- Analyse patent thickets and the political economy of intellectual-property terms.
- Discuss the challenges that artificial intelligence poses for intellectual property.

Intellectual property is the law's attempt to make ideas behave a little more like physical things. A loaf of bread can be eaten by only one person, but an idea, once disclosed, can be used by everyone at once without diminishing the original. That is wonderful for society and awkward for the inventor, who may struggle to recoup the cost of creating something that others can copy for nothing. Intellectual property rights respond by granting creators a temporary, limited exclusivity, a deliberate bargain that trades a period of monopoly for the incentive to create and, crucially, to disclose. In the terms of Chapter 1, ideas are close to public goods: one person's use does not reduce what is left for others, and it is hard to stop anyone from using an idea once it is known, which is why markets alone tend to produce too few of them.

The bargain takes several forms suited to different creations. Patents protect inventions and processes, typically for around twenty years, after which the invention enters the public domain for anyone to use. Trademarks protect the names, logos, and symbols that identify a product's source, and can last indefinitely so long as they remain in use, because their purpose is to prevent confusion rather than to reward invention. Copyright protects original works of authorship, writing, music, film, software, automatically and for a long term, covering the expression of an idea but not the idea itself. Trade secrets protect valuable confidential information, a formula or a method, for as long as it stays secret, with no registration and no expiry, but no protection at all once the secret leaks.

Patents		Trademarks	
Protects:	inventions, processes	Protects:	names, logos, symbols
Term:	about 20 years	Term:	indefinite, while used
Example:	a new engine design	Example:	a brand name

Copyright		Trade secrets	
Protects:	original works	Protects:	confidential information
Term:	life plus decades	Term:	while it stays secret
Example:	a novel, software	Example:	a formula

Figure 17. The four main forms of intellectual property.

For a business these rights are strategic assets, not mere legal formalities. They can confer a durable competitive advantage, generate revenue through licensing and franchising, and add substantially to a firm's valuation, especially in technology and pharmaceuticals, where the intangible assets may be worth more than the factories. Managing them well means choosing the right form of protection for each innovation, maintaining it, trademarks must be defended, patents carry fees, and deciding how to extract value, whether by commercialising directly, licensing to others, or some combination. It also means respecting the rights of others, since infringement is costly whether one is the victim or the inadvertent perpetrator, and due diligence on intellectual property is a central part of any merger or acquisition.

Two features complicate the picture. Protection is territorial: a patent granted in one country confers no rights in another, so firms operating globally must navigate a patchwork of national systems and international treaties. And not everything is proprietary. A vast and growing commons of open-source software, open data, and public-domain works is available for use, though usually under licence terms that must be understood and honoured rather than ignored.

The hardest questions now come from artificial intelligence, which strains the system at both ends. At the input end, generative models are trained on enormous quantities of existing text, images, and code, much of it copyrighted, and the question of whether such training requires permission or payment is being fought out in court, in high-profile cases brought by news publishers, image libraries, and authors against AI developers. The EU's AI Act has begun to respond by requiring providers of general-purpose models to publish summaries of their training data and to respect rights-holders' reservations. At the output end, the question is who, if anyone, owns what a machine produces, with copyright offices in several jurisdictions taking the view that a work needs a human author to qualify for protection, leaving purely machine-generated output in an uncertain space. A related, more consumer-facing fight is the right-to-repair movement, which argues that aggressive use of intellectual property to block independent repair harms competition and consumers, and which has won legislative ground on both sides of the Atlantic.

Underlying all of this is a single tension that the rest of the chapter only sharpens: intellectual property must be strong enough to reward creation but not so strong that it strangles the follow-on innovation

that builds on what came before. Strike the balance too far in either direction and society loses, either the incentive to create or the freedom to improve.

It is worth remembering that intellectual property is a monopoly created and enforced by the state, and so it is exposed to the same political pressures as any other government privilege. Copyright terms show the pattern. The first American copyright law, in 1790, granted fourteen years, renewable once; today protection runs for the author's life plus seventy years, and the Copyright Term Extension Act of 1998 added twenty years even to works that already existed, after intensive lobbying by rights-holders, although no extension can encourage the creation of a work that has already been made. The European Union similarly extended protection for sound recordings from fifty to seventy years in 2011. Patent systems have distortions of their own, from patent thickets to firms, often called patent trolls, that acquire patents not to make anything but to extract settlements from those who do. Critics such as Michele Boldrin and David Levine go further and argue that the costs of these monopolies frequently outweigh their benefits. One need not accept that conclusion to see the point: the right level of protection is an economic question, but it is settled in a political arena in which the beneficiaries of stronger rights are organised and the public that pays for them is not.

In brief

- A deliberate bargain. Temporary exclusivity is granted to reward creation and encourage disclosure of ideas that others could otherwise copy freely.
- Four main forms. Patents, trademarks, copyrights, and trade secrets protect different creations for different terms.
- Strategic assets. IP drives competitive advantage, licensing revenue, and valuation, and must be actively managed.
- Territorial and partial. Rights stop at borders, and a large commons of open and public-domain works sits alongside proprietary works.
- AI strains the system. Training on copyrighted data and ownership of machine output are unsettled and being litigated.
- Balance is everything. Protection must reward creation without strangling the innovation that builds on it.

Case study: the Wright brothers' patent war, then and now

The Wright brothers earned their place in history twice over: once for achieving the first powered, controlled flight in 1903, and again, less happily, for showing how intellectual property can throttle the very field it was meant to nurture. Having solved the central problem of flight, three-axis control of an aircraft, the brothers secured broad patents and then set about enforcing them aggressively against anyone they believed was infringing.

Their chief target was Glenn Curtiss, a brilliant rival who used ailerons, hinged surfaces on the wings, for lateral control. The Wrights argued that this fell within their patent, and the dispute became a grinding legal war. The consequences reached well beyond the parties. American aviators who wanted to build aircraft faced a choice among paying costly licence fees, fighting expensive litigation, or engineering awkwardly around the patented techniques using inferior methods. Capital and talent that might have gone into flying went into lawyers instead. Many historians argue that this patent war slowed American aviation during a crucial decade, even as European builders, free of the dispute, advanced rapidly and pulled ahead.

The deadlock broke only under the pressure of war. When the United States entered the First World War in 1917 and urgently needed aircraft, the government could not tolerate an industry paralysed by litigation. It pressed the manufacturers to form a patent pool, the Manufacturers Aircraft Association, through which the major holders cross-licensed their patents to one another for modest, agreed royalties. With the legal logjam cleared, development resumed. The episode is a near-perfect illustration of the chapter's central tension: intellectual property exists to reward and encourage invention, but pushed too far it does the opposite, turning a spur to innovation into a barrier against it.

The pattern is not a historical curiosity; it recurs whenever a field becomes dense with overlapping patents, a situation lawyers call a patent thicket. The smartphone wars of the 2010s, in which Apple, Samsung, and others sued one another across the globe over thousands of patents, were a modern Wright-versus-Curtiss on a vast scale, consuming billions in legal costs. Today the frontier has moved again, to artificial intelligence, where courts are wrestling with whether training a model on copyrighted works requires permission and who, if anyone, owns what the model produces. The names and technologies change, but the underlying question is the one the Wright brothers posed a century ago: how do we protect creators enough to reward them, without protecting them so much that we stop everyone else from building on what they made?

Review and practice

Discussion questions

1. The Wright brothers' patents may have slowed aviation. When does intellectual property stop encouraging innovation and start blocking it?
2. Should training an AI model on copyrighted works require permission or payment? Make the strongest case for creators, then for AI developers.
3. Who, if anyone, should own a work produced by a machine, and what rests on the answer?

Exercises

1. Match four creations, a brand name, a novel, a secret recipe, and a new engine design, to the form of intellectual property that best protects each, and state the term of protection.
2. Explain how a patent thicket forms, using either the early aviation industry or the smartphone wars as your example.
3. Argue for and against a strong right to repair from the standpoints of consumers, manufacturers, and innovation.

Self-check

- Name the four main forms of intellectual property and what each protects.
- Why is intellectual property described as a bargain?
- What does it mean to say that intellectual property is territorial?
- State the central tension that intellectual-property law must balance.
- Why is the length of copyright protection a political as well as an economic question?

Further Reading

- Boldrin, M., & Levine, D. K. (2008). *Against intellectual monopoly*. Cambridge University Press.
- European Patent Office. (2023). *New study reveals how IP helps startups raise finance*.
<https://www.epo.org/en/news-events/news/new-study-reveals-how-ip-helps-startups-raise-finance>
- European Union. (2019). *Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/dir/2019/790/oj>
- European Union Intellectual Property Office. (2025). *The development of generative artificial intelligence from a copyright perspective*. Publications Office of the European Union.
<https://doi.org/10.2814/3893780>
- Grinvald, L. C., & Tur-Sinai, O. (2019). Intellectual property law and the right to repair. *Fordham Law Review*, 88(1), 63-127.
<https://ir.lawnet.fordham.edu/flr/vol88/iss1/2/>
- Perzanowski, A. (2022). *The right to repair: Reclaiming the things we own*. Cambridge University Press.
- Samuelson, P. (2023). Generative AI meets copyright. *Science*, 381(6654), 158-161.
<https://doi.org/10.1126/science.adi0656>
- World Intellectual Property Organization. (n.d.). *What is intellectual property?*
<https://www.wipo.int/about-ip/en>



11. Big Data, Privacy, and GDPR

Learning objectives

- Explain the value and the risks of big data as a reversed information asymmetry.
- State the GDPR's main principles and the rights it gives individuals.
- Describe how the GDPR is enforced and why its influence extends beyond the EU.
- Evaluate the unintended effects of privacy regulation on competition.

Data is the raw material of the information economy, and there has never been so much of it. Every purchase, search, message, step, and click leaves a trace, and the sum of these traces, the phenomenon usually called big data, has become a resource that firms mine for insight, prediction, and advantage. The same abundance that makes data valuable also makes it dangerous, because information about people is information about people, and the line between useful analytics and intrusive surveillance is easily crossed. This chapter is about that tension and about the law the European Union built to manage it.

Big data is usually described by its volume, its variety, and the velocity at which it arrives. It is gathered from social media, e-commerce, sensors, payment systems, and countless other sources, and analysed for patterns that would be invisible at a smaller scale: which customers are about to leave, which transactions are fraudulent, which treatments work for which patients. The value is real. So is the risk. Datasets that seem harmless in isolation can, when combined, re-identify individuals who believed they were anonymous and reveal things, health, location, beliefs, relationships, that people never meant to disclose.

In the language of Chapter 2, big data reverses the classic asymmetry. Here it is the firm that is the better-informed party, and the individual who cannot see what is known about them or how it is used. The regulation described below can be read as an attempt to rebalance that asymmetry through mandatory transparency and a set of individual rights.

The European Union's response, the General Data Protection Regulation, took effect in 2018 and has become the most influential privacy law in the world. Its premise is that personal data belongs, in an important sense, to the person it describes, and that organisations may process it only under clear rules. Those rules rest on a set of principles: data must be processed lawfully, fairly, and transparently; collected for specified purposes and not used in incompatible ways; limited to what is necessary, the principle of data minimisation; kept accurate and up to date; retained no longer than needed; and held securely. Above all, organisations must not only comply but be able to demonstrate compliance, which is the principle of accountability.

Processing must rest on a lawful basis, of which consent is the most discussed. Where consent is relied upon, it must be explicit, informed, and freely given, which rules out pre-ticked boxes and obligations buried in dense terms and conditions. The regulation also grants individuals a suite of rights: to access the data held about them, to have errors corrected, to have data erased in certain circumstances, the much-cited right to be forgotten, to receive their data in a portable format so they can move it elsewhere, to object to certain uses, and not to be subject to consequential decisions taken solely by automated means without recourse. Organisations of a certain scale must appoint a data protection officer, and serious breaches must be reported to the supervisory authority within seventy-two hours.

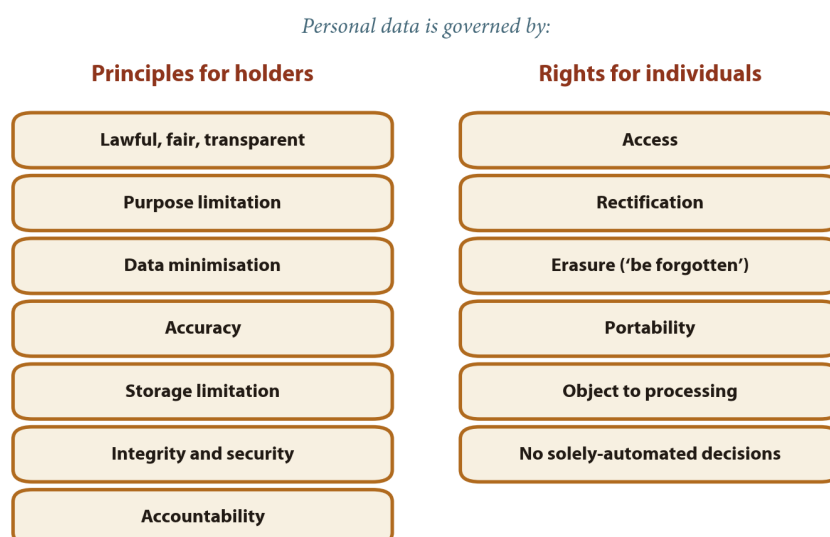


Figure 18. The GDPR in brief: principles for data holders and rights for individuals.

What gives these rules teeth is the penalty regime and the reach. Fines can run up to twenty million euros or four per cent of global annual turnover, whichever is greater, and the largest cases have been very large indeed: in 2023 the Irish regulator fined Meta 1.2 billion euros over transfers of European users' data to the United States. The regulation also applies extraterritorially, binding any organisation anywhere that handles the data of people in the EU, which is why its standards have rippled across the globe, an influence often called the Brussels effect. Recent years have brought a maturing enforcement practice, a renewed transatlantic data-transfer framework agreed in 2023, and a growing overlap with the AI Act, since training and deploying AI systems almost always involves personal data. There is also an active debate, visible in EU simplification proposals during 2025 and 2026, about how to reduce compliance burdens without weakening the underlying protections.

Regulation of this kind also has unintended effects, and they deserve as much attention as its aims. Studies of the GDPR's first years found that websites cut the number of outside technology vendors they

used and that the largest vendors, Google among them, gained market share, because big firms could absorb compliance costs and obtain consent more easily than small ones; another study found a fall in venture investment in European technology start-ups after the regulation took effect. A rule meant to discipline the most powerful holders of data can, in practice, entrench them, which is why the debate about simplification is not only about cost but also about competition.

In brief

- Data is the raw material. Big data is defined by volume, variety, and velocity, and is mined for prediction and advantage.
- Value and risk are inseparable. Combining datasets can re-identify people and expose what they never meant to disclose.
- GDPR sets the rules. Lawfulness, purpose limitation, data minimisation, accuracy, security, and accountability govern all processing of personal data.
- Strong individual rights. Access, rectification, erasure, portability, objection, and protection from solely automated decisions.
- Serious penalties, global reach. Fines reach 4% of global turnover, and the law binds anyone handling EU residents' data, the Brussels effect.
- Converging with AI rules. Data protection increasingly overlaps with the AI Act, even as simplification of the regime is debated.

Case study: a GDPR fine in Romania

It is tempting to think of the GDPR as a problem for technology giants, something that concerns Google, Meta, and the handling of millions of records. The reality is that the regulation applies to almost every organisation that processes personal data, including the small business on the corner, and a modest Romanian case makes the point better than any headline fine.

In July 2022 the Romanian supervisory authority, the National Supervisory Authority for Personal Data Processing, known by its initials ANSPDCP, concluded an investigation into a company referred to in its decision as DN SRL. The case began with a complaint from an ordinary individual who noticed that clients were being filmed by video-surveillance cameras while they received cosmetic treatments. What sounds like a small matter turned out to involve several of the regulation's core principles at once.

The authority found that the company ran cameras both inside and outside its premises, monitoring staff and clients alike, including in the room where treatments were carried out. It had no valid legal basis for filming people in that setting, and it had not properly informed those being recorded, as the regulation requires. The company could point to no history of incidents, theft or otherwise, that might have justified such intrusive surveillance, so its claimed legitimate interest did not outweigh the privacy of the people it was filming. The footage it collected went well beyond what any legitimate purpose required, breaching the principles of lawfulness and fairness, of transparency, and of data minimisation, the rule that you should collect only what you actually need.

The consequences were proportionate to a small business. The company was fined the equivalent of roughly one thousand euros for failing to inform the people it filmed and about one thousand five hundred euros for the unlawful and excessive processing itself. It was also ordered to take corrective steps: to inform data subjects properly, to remove the camera in the treatment room, to secure its surveillance system, and to cut off remote internet access to the recordings. The amounts are small, but the lesson is large. The GDPR's abstract principles, have a lawful basis, be transparent, collect only what you need, are not reserved for data centres and algorithms. They reach down to the most ordinary act of installing a camera in a shop, and any organisation that handles personal data, however small, is expected to be able to justify what it collects and why.

Review and practice

Discussion questions

1. Should personal data be treated as something a person owns, something they merely license, or something else entirely? What follows from each view?
2. The GDPR's reach extends worldwide, the so-called Brussels effect. Is it legitimate for the EU to set privacy standards for companies based anywhere?
3. Because AI training depends on personal data, do the GDPR and the AI Act pull in the same direction or against each other?

Exercises

1. For a small online shop, list the lawful bases it might rely on to process customer data and the GDPR rights it must be ready to honour.
2. Take the Romanian surveillance-camera case and identify exactly which principles were breached, and why.
3. Draft a plain-language consent notice for an app that collects location data, one that would satisfy the GDPR's requirement for informed consent.

Self-check

- Name four principles that govern the processing of personal data under the GDPR.
- What is the maximum fine the GDPR allows?
- What does data minimisation require?
- List three rights the GDPR gives individuals.
- How can a privacy regulation end up favouring the largest firms?

Further Reading

European Data Protection Board. (n.d.). *Guidelines, recommendations and best practices*.

https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

European Union. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*. Official Journal of the European Union.

<https://eur-lex.europa.eu/eli/reg/2016/679/oj>

European Union. (2023). *Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act)*. Official Journal of the European Union.

<https://eur-lex.europa.eu/eli/reg/2023/2854/oj>

Goldberg, S. G., Johnson, G. A., & Shriver, S. K. (2024). Regulating privacy online: An economic evaluation of the GDPR. *American Economic Journal: Economic Policy*, 16(1), 325-358.

Goldfarb, A., & Que, V. F. (2023). The economics of digital privacy. *Annual Review of Economics*, 15, 267-286.

Jia, J., Jin, G. Z., & Wagman, L. (2021). The short-run effects of the General Data Protection Regulation on technology venture investment. *Marketing Science*, 40(4), 661-684.

Johnson, G. A., Shriver, S. K., & Goldberg, S. G. (2023). Privacy and market concentration: Intended and unintended consequences of the GDPR. *Management Science*, 69(10), 5695-5721.

National Supervisory Authority for Personal Data Processing. (n.d.). [Official website of the Romanian data protection authority, ANSPDCP].

<https://www.dataprotection.ro/?lang=en>

Robertson, V. H. S. E. (2020). Excessive data collection: Privacy considerations and abuse of dominance in the era of big data. *Common Market Law Review*, 57(1), 161-189.

<https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/57.1/COLA2020006>



12. Social Media and Fake News

Learning objectives

- Distinguish misinformation from disinformation.
- Use externalities and incentives to explain why falsehood spreads.
- Assess the risks that deepfakes and generative AI add.
- Weigh the regulation of online falsehood against the protection of free expression.

Social media did something genuinely new: it let anyone publish to a global audience at no cost and let any message, true or false, travel at the speed of a share. That is a triumph for free expression and a serious problem for the reliability of what we collectively believe. The economics of information explains why, because attention is scarce and engagement is what platforms sell, the systems that distribute information are not optimised for truth.

A first distinction is essential. Misinformation is false or misleading information spread without intent to deceive, the well-meaning share of a rumour. Disinformation is false information spread deliberately to mislead, often for political or commercial gain. The two require different responses, but both are hard to catch, because those who craft disinformation are skilled at mimicking the look of credible sources and at exploiting the emotions, outrage, fear, tribal loyalty, that make people share before they check.

Why does falsehood spread so well? Part of the answer is structural. Recommendation algorithms are tuned to maximise engagement, and content that provokes a strong reaction tends to engage, so sensational and divisive material is amplified almost as a by-product, sometimes at the expense of accuracy. Part is social. People are shown more of what they already agree with, the filter bubble, which hardens belief and insulates falsehoods from challenge. Research on large platforms has found that false stories can travel faster and reach more people than true ones, precisely because novelty and emotion are rewarded. Two ideas from Part I sharpen the diagnosis. Sharing a false story is a negative externality (Chapter 1): the person who shares it bears almost none of the cost of the confusion it causes. And a

platform's incentives, which come from selling attention to advertisers, are only partly aligned with what its users would choose for themselves, the kind of divergence of interests studied in Chapter 3.

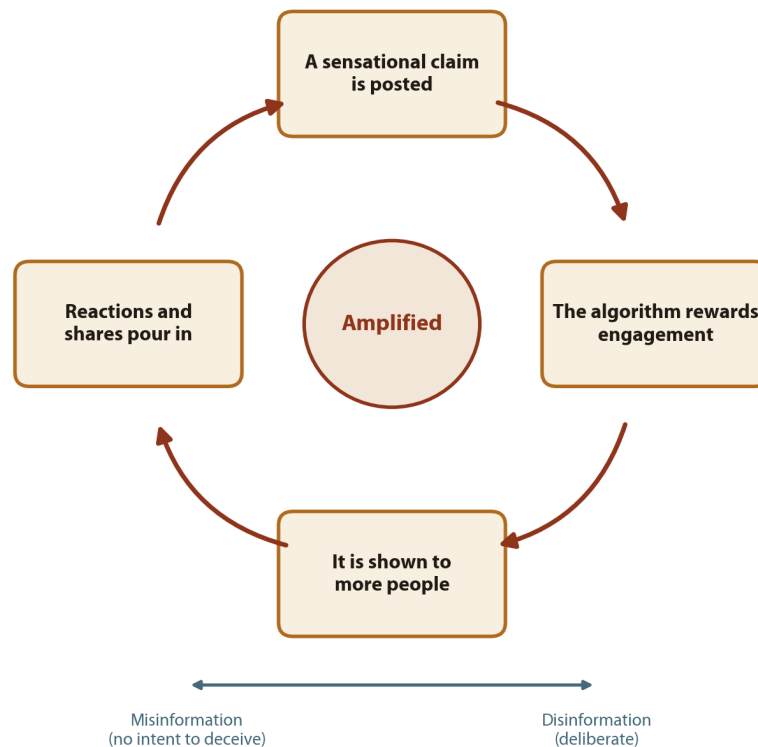


Figure 19. Why falsehood spreads: the amplification loop, and the spectrum of intent.

The consequences reach business and society alike. A false story can damage a company's reputation, move its share price, and prompt decisions based on things that never happened, and the correction, when it comes, rarely travels as far as the original. For democratic societies the stakes are higher still, as coordinated disinformation campaigns seek to manipulate opinion, especially around elections. With much of the world voting in recent years, these concerns have been acute, and businesses that operate online have a genuine responsibility to communicate accurately and to avoid amplifying what they cannot verify.

The newest and most disquieting development is generative artificial intelligence. It is now cheap and easy to fabricate realistic text, images, audio, and video, the so-called deepfakes, that depict people saying and doing things they never said or did. This collapses the old assumption that a photograph or a recording is evidence, and it scales disinformation from a craft into an industrial process. The responses are taking shape on several fronts at once. Technically, the race is on between generation and detection, alongside provenance standards that cryptographically label where media came from. Legally, the European Union's AI Act requires that AI-generated or manipulated content be disclosed and machine-readably marked, and its Digital Services Act obliges the largest platforms to assess and mitigate systemic risks including disinformation. None of these will be a complete cure, which is why the most durable defence remains the one this textbook keeps returning to: a literate, sceptical reader who checks the source before believing, and before sharing.

Regulation is not a free remedy here either, because the cure for false speech can easily become the control of speech. Someone has to decide what is false, and neither officials nor platforms are infallible. In May 2021 Facebook stopped removing posts claiming that the virus behind COVID-19 was man-

made, a claim it had treated as misinformation, after the question of the virus's origin was reopened by scientists and governments. Laws against fake news have also been turned against critics: Malaysia's Anti-Fake News Act of 2018 was repealed the following year amid concern that it could be used to silence the government's opponents, and Singapore's 2019 law, which lets ministers order corrections to online statements, has been applied to opposition politicians and critical outlets. This is why European rules such as the Digital Services Act concentrate on platforms' processes, transparency, and risk assessment rather than giving the state power to declare what is true, and why the balance between fighting disinformation and protecting free expression remains contested.

In brief

- Free reach, fragile truth. Social media lets anything spread at the speed of a share, and engagement-driven systems are not optimised for accuracy.
- Misinformation versus disinformation. The first is spread without intent to deceive, the second deliberately; both are hard to detect.
- Algorithms and bubbles amplify falsehood. Engagement optimisation rewards sensational content, and filter bubbles shield it from challenge.
- Real costs. Reputational and financial damage to firms, and manipulation of opinion in democracies, especially around elections.
- Generative AI raises the stakes. Deepfakes industrialise disinformation and collapse the assumption that media is evidence.
- Layered defences. Detection, provenance standards, AI Act labelling, DSA duties, and, above all, a sceptical reader.

Case study: “Pope Francis endorses Donald Trump”

During the 2016 United States presidential election, a story claiming that Pope Francis had broken with Vatican tradition to endorse Donald Trump spread across social media and was shared, by some counts, around a million times. It was entirely fabricated. The Vatican does not endorse candidates, and no such statement was ever made. The story originated on a website dressed up to look like a real news outlet, and for a great many readers the convincing wrapper was enough.

The episode is worth dissecting because it displays the anatomy of fake news so cleanly. There was a fabricated core claim, designed to be striking. There was an authentic-looking source, built to borrow the credibility of real journalism without earning it. There was an emotionally and politically charged subject that made people want it to be true, or want to share their outrage that others believed it. And there was a high-profile cast, a pope and a presidential candidate, that made the story irresistible to pass on. Each ingredient did its job, and the algorithms that reward engagement did the rest.

What is often forgotten is the economic engine behind it. Many of the most viral political hoaxes of 2016 were traced not to ideologues but to entrepreneurs, including a now-famous cluster of young people in Veles, North Macedonia, who discovered that sensational, false political stories drew enormous traffic and therefore advertising revenue. The lesson is pure economics of information: when attention is monetised and falsehood travels better than truth, there is a direct financial incentive to manufacture lies, and that incentive operates regardless of anyone’s politics.

A decade later the same anatomy persists, but the tools have grown far sharper. A 2016 hoax needed only a believable layout and a catchy headline. A comparable fabrication today can include a photorealistic AI-generated image of the endorsement, a cloned voice delivering it, or a video that looks like genuine footage, produced in minutes and at almost no cost. This is why the regulatory responses discussed in this chapter, the AI Act’s requirement to label synthetic media and the Digital Services Act’s duties on the largest platforms, have become urgent. But no rule will fully close the gap, and the durable defence is the one this whole book keeps returning to. Before believing, and before sharing, check the source, distrust the sensational, and remember that looking real has never been the same as being true.

Review and practice

Discussion questions

1. Why does false news often spread faster than true news, and what can a platform do about it without becoming a censor?
2. Who should be responsible for a deepfake that moves a company's share price: the creator, the platform that hosted it, or no one?
3. Is media literacy a realistic defence against industrial-scale disinformation, or is it wishful thinking?

Exercises

1. Take the "Pope Francis" hoax and list the features that made it spread, then explain how a generative-AI version of the same hoax would differ.
2. Explain the economic incentive that drove the Veles hoax sites, and propose one change to the online advertising system that would weaken it.
3. Outline what the AI Act and the Digital Services Act each require in relation to synthetic content and disinformation.

Self-check

- What is the difference between misinformation and disinformation?
- How do engagement-optimising algorithms end up amplifying falsehood?
- What is a deepfake, and why does it raise the stakes?
- Name two of the layered defences against fake news discussed in the chapter.
- Why can laws against fake news become a threat to free expression?

Further Reading

Annenberg Public Policy Center. (n.d.). *FactCheck.org*.

<https://www.factcheck.org>

Baptista, J. P., & Gradim, A. (2020). Understanding fake news consumption: A review. *Social Sciences*, 9(10), Article 185.

<https://doi.org/10.3390/socsci9100185>

European Union. (2022). *Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act)*. Official Journal of the European Union.

<https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

Fisher, M. (2022). *The chaos machine: The inside story of how social media rewired our minds and our world*. Little, Brown.

Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. *Trends in Cognitive Sciences*, 25(5), 388-402.

<https://doi.org/10.1016/j.tics.2021.02.007>

Rathje, S., Van Bavel, J. J., & van der Linden, S. (2021). Out-group animosity drives engagement on social media. *Proceedings of the National Academy of Sciences*, 118(26), Article e2024292118.

<https://doi.org/10.1073/pnas.2024292118>

van der Linden, S. (2023). *Foolproof: Why misinformation infects our minds and how to build immunity*. W. W. Norton.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146-1151.

<https://doi.org/10.1126/science.aap9559>



13. Big Tech vs Big Government

Learning objectives

- Present the strongest case on each side of the contest between platforms and states.
- Describe the first enforcement under the Digital Markets Act and the US Google ruling.
- Analyse the trade-offs in content moderation, encryption, and taxation.
- Apply the book's test of weighing a market failure against the government failure that might replace it.

Few relationships will shape the information economy more than the uneasy one between the largest technology companies and the states that try to govern them. A handful of firms now operate the infrastructure through which much of the world searches, shops, communicates, and forms its opinions. Governments, for their part, claim the authority to set the rules of that infrastructure. Each side has a legitimate case, and each carries real risks, and a thoughtful student should be able to argue both rather than cheering for one. This chapter draws together threads from across the book: the network effects that make platforms powerful (Chapter 5), the data they collect (Chapter 11), the content they distribute (Chapter 12), and, throughout, the question raised in Chapters 1 and 3 of whether a given market failure is more or less serious than the government failure that might replace it.

Flashpoint	The platform's case	The government's case	The overreach risk
Privacy and data	we secure data best	independent oversight is needed	state surveillance
Market power	our dominance is earned	network effects entrench it	shielding national champions
Content moderation	our platform, our rules	too little, or too much	censorship of dissent
Encryption	strong encryption protects all	lawful access to evidence	a backdoor for everyone
Taxation	we follow the law	pay where profit is earned	punishing disfavoured firms

Figure 20. Big Tech and Big Government: the case on each side, and the risk of overreach.

Take privacy and data. The large platforms point to the protections and controls they offer users and argue that they are better placed than any regulator to secure data at scale. Governments reply that firms whose business depends on data cannot be the sole guardians of it, and that independent oversight is needed to prevent misuse. Yet government itself can be the threat: the same powers used to protect citizens can enable surveillance that erodes the privacy they are meant to defend. The question is rarely whether to have rules but who watches the watchers.

On market power the argument has moved from theory to enforcement. The platforms defend their dominance as the earned reward of building products people prefer, and warn that heavy-handed intervention will slow the very innovation that benefits consumers. Competition authorities counter that network effects can entrench incumbents and choke off the next generation of challengers, and they have begun to act. The European Union's Digital Markets Act designates the biggest firms as gatekeepers and, in April 2025, produced its first fines, 500 million euros against Apple over its App Store rules and 200 million against Meta over its consent model, with further investigations continuing. In the United States a federal court found in 2024 that Google had unlawfully monopolised search, and in 2025 ordered remedies that stopped short of breaking up the company but curbed its exclusive default-placement deals and required it to share certain data with rivals, with the rise of generative-AI competitors explicitly shaping the judge's reasoning. The risk on the other side is that enforcement becomes a tool for protecting national champions or settling political scores rather than serving competition, a charge aired loudly in transatlantic disputes over whether such rules unfairly target American firms.

Content moderation is harder still, because it pits two goods against each other. Platforms claim the right to set and enforce community standards on what is, after all, private property, and governments worry both that they moderate too little, leaving up harassment, fraud, and incitement, and too much, suppressing lawful speech. The European Union's Digital Services Act now imposes duties of transparency and risk management, especially on the largest platforms, while leaving the underlying tension unresolved. The danger of government involvement is obvious: a state that can compel removal can also suppress dissent, and the line between fighting disinformation and policing opinion is perilously thin.

Similar trade-offs run through the other flashpoints. On encryption, the platforms stress that strong, unbroken encryption protects everyone, while law-enforcement agencies seek lawful access to investigate serious crime; the technical reality is that a backdoor built for the police is a vulnerability available to everyone, which is why demands for one are so contested. On taxation, governments want firms to pay where profits are earned rather than where they are booked, an aim partly addressed by the OECD's global minimum tax, while firms resist measures they see as targeted; the risk is taxation designed to punish rather than to fund. And on digital sovereignty, the wish of states to control their own digital infrastructure can shade into a fragmentation of the open internet into national enclaves.

The honest conclusion is that there is no settled answer, only a balance to be struck and re-struck. Unconstrained private power over essential infrastructure is genuinely dangerous; so is unconstrained public power over speech, encryption, and enterprise. The task of policy, and the task of the analyst, is to identify the specific harm in view, ask whether a given intervention actually addresses it, and weigh that against the harm the intervention itself may cause.

In brief

- Two legitimate cases, two real risks. Private control of essential infrastructure and public control of speech and enterprise are each dangerous in excess.
- Enforcement is now real. The EU's DMA produced its first fines on Apple and Meta in 2025; a US court found Google's search monopoly unlawful and ordered remedies.
- Content moderation has no clean answer. Platforms can moderate too little or too much, and state power to compel removal can slide into censorship.
- Encryption and access conflict directly. A backdoor for law enforcement is a vulnerability for everyone.
- Tax and sovereignty raise overreach risks. Measures can fund public goods or punish disfavoured firms; sovereignty can protect or fragment the internet.
- Judge interventions case by case. Name the harm, ask whether the remedy fits it, and weigh the remedy's own costs.

Case study: the Digital Markets Act and the first fines on Big Tech

For two decades, the contest between Big Tech and Big Government in Europe was fought mainly through traditional competition law, case by case, after the fact, and at a pace that the digital economy easily outran. By the time an investigation concluded, the market had often moved on. The European Union's Digital Markets Act, which began to bite in 2024, was designed to change that, and the events of 2025 turned it from a piece of legislation into a live test of whether a state can really set the rules for the world's largest platforms.

The Act works by designating the biggest platforms as gatekeepers, companies whose control of an important gateway between businesses and consumers gives them durable power, and imposing on them a set of clear, up-front obligations rather than waiting to prove harm in court. Gatekeepers must, among other things, let business users tell their customers about cheaper options elsewhere, refrain from forcing users into take-it-or-leave-it data bargains, and stop preferencing their own services. These are not vague principles but specific duties, and the penalties for breaking them are severe: fines of up to ten per cent of a company's worldwide turnover, rising to twenty per cent for repeat offences.

In April 2025 the Commission issued its first non-compliance decisions, and they were aimed at two of the largest firms in the world. Apple was fined five hundred million euros for restricting app developers from steering their customers toward purchase options outside the App Store, a practice that kept transactions, and Apple's commission, inside its own walls. Meta was fined two hundred million euros over its consent-or-pay model, under which users of Facebook and Instagram had to either accept personalised-advertising tracking or pay for an ad-free version, a choice the Commission found did not give them a genuine option to use a less data-hungry service. In a related move, the Commission also de-designated Facebook Marketplace, removing it from the Act's scope after concluding it no longer met the thresholds, a reminder that the regime is meant to be calibrated, not blunt.

The case captures every theme of this chapter. It shows Big Government moving from slow, after-the-fact enforcement to fast, structural rules, and it shows Big Tech resisting, both Apple and Meta announced appeals, and warning that the rules harm users and innovation. It shows the geopolitical edge, too: the fines landed amid threats of retaliatory tariffs and accusations from the United States that Europe was unfairly targeting American firms, while the Commission insisted it was applying the law regardless of where a company comes from. And it leaves the central question of the chapter open. Whether the Digital Markets Act genuinely opens these markets to competition, or merely imposes costs that the giants can absorb while the political fallout grows, will be one of the defining stories of the information economy in the years ahead.

Review and practice

Discussion questions

1. Choose one flashpoint, encryption, content moderation, taxation, or market power, and argue first for strong government action, then against it.
2. The DMA fines on Apple and Meta were small relative to their turnover but struck at core business practices. Which matters more for changing behaviour: the size of the fine or the conduct it forbids?
3. When the United States accuses the EU of unfairly targeting American firms, how can an observer tell legitimate regulation from disguised protectionism?

Exercises

1. For a named platform, state one genuine harm that regulation might address and one risk that the regulation itself could create.
2. Explain, in plain terms, why a backdoor built for law enforcement is also a security weakness for everyone.
3. Summarise the remedies imposed in the US Google search case, and explain how the rise of generative AI shaped them.

Self-check

- What does the Digital Markets Act do, and to whom does it apply?
- Why is content moderation described as having no clean answer?
- What did the US court decide about Google, and what remedy followed?
- State the test the chapter proposes for judging any intervention.

Further Reading

- Bessen, J. (2022). *The new Goliaths: How corporations use software to dominate industries, kill innovation, and undermine regulation*. Yale University Press.
- Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.
- Cabral, L., Haucap, J., Parker, G., Petropoulos, G., Valletti, T., & Van Alstyne, M. (2021). *The EU Digital Markets Act: A report from a panel of economic experts*. Publications Office of the European Union.
- Engin, Z., & Treleaven, P. (2019). Algorithmic government. *The Computer Journal*, 62(3), 448-460.
<https://ieeexplore.ieee.org/abstract/document/8852885>
- European Commission. (2025, April 23). *Commission finds Apple and Meta in breach of the Digital Markets Act* [Press release].
<https://digital-strategy.ec.europa.eu/en/news/commission-finds-apple-and-meta-breach-digital-markets-act>
- European Union. (2022). *Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/reg/2022/1925/oj>
- European Union. (2022). *Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
- Petit, N. (2020). *Big Tech and the digital economy: The moligopoly scenario*. Oxford University Press.
<https://doi.org/10.1093/oso/9780198837701.001.0001>
- United States v. Google LLC, No. 1:20-cv-03010 (APM) (D.D.C. Sept. 2, 2025) (memorandum opinion on remedies).
<https://www.justice.gov/atr/case/us-and-plaintiff-states-v-google-llc-2020>

Glossary

This glossary defines the key terms used in the book. Each entry gives the usual Romanian equivalent in *italics*, to help readers who study in a language other than their own, and the chapter in which the term is mainly discussed.

Adverse selection (*selecție adversă*). The problem of hidden information before a transaction, which can leave a market with mainly low-quality goods or high-risk customers. Chapter 2.

Agency cost (*cost de agenție*). The total cost of delegation: monitoring costs, the cost of incentives, and the residual loss that remains. Chapter 3.

Agentic AI (*inteligență artificială agentică*). AI systems that combine models with tools and memory to carry out multi-step tasks with limited supervision. Chapter 7.

Blockchain (*blockchain (registru distribuit)*). A ledger replicated across many computers in which each block of transactions is cryptographically linked to the previous one. Chapter 6.

Brussels effect (*efectul Bruxelles*). The tendency of EU rules, such as the GDPR, to become global standards because firms adopt them everywhere. Chapter 11.

Bundling (*vânzare la pachet*). Selling several goods together for a single price. Chapter 1.

Consensus mechanism (*mecanism de consens*). The rules by which the participants in a blockchain agree on the state of the shared record, such as proof of work or proof of stake. Chapter 6.

Copyright (*drept de autor*). Protection for original works of authorship, covering the expression of an idea but not the idea itself. Chapter 10.

Cross-side network effect (*efect de rețea încrucișat*). The increase in a platform's value to one group of users as the number of users on another side grows. Chapter 5.

Crowdfunding (*finanțare participativă*). Raising money in small amounts from many backers, usually online. Chapter 8.

Crowdsourcing (*crowdsourcing (externalizare către mulțime)*). Inviting a large, usually online group to contribute ideas, content, labour, or money. Chapter 8.

Data minimisation (*reducerea la minimum a datelor*). The GDPR principle that only the personal data necessary for a specified purpose may be collected and processed. Chapter 11.

Deepfake (*deepfake (conținut falsificat cu AI)*). Realistic audio, image, or video fabricated with AI to show people saying or doing things they never did. Chapter 12.

Digital Markets Act (DMA) (*Regulamentul privind piețele digitale*). The EU regulation that imposes up-front competition obligations on the largest platforms, designated as gatekeepers. Chapter 13.

Digital Services Act (DSA) (*Regulamentul privind serviciile digitale*). The EU regulation that sets duties for online platforms on illegal content, transparency, and systemic risks. Chapter 12.

Disinformation (*dezinformare*). False information spread deliberately to mislead. Chapter 12.

Elasticity of demand (*elasticitatea cererii*). How strongly the quantity demanded responds to a change in price. Chapter 1.

Equilibrium (market-clearing) price (*preț de echilibru*). The price at which the quantity demanded equals the quantity supplied. Chapter 1.

Experience good (*bun de experiență*). A good whose quality can be judged only after it has been consumed. Chapter 1.

- Externality** (*externalitate*). A cost or benefit that falls on people who are not party to a transaction. Chapter 1.
- Filter bubble** (*bulă de filtrare*). The tendency of personalised feeds to show people mainly what they already agree with. Chapter 12.
- Friendshoring** (*friendshoring (relocare în țări aliate)*). Moving production or services to politically allied countries. Chapter 9.
- Gatekeeper** (*controlor de acces*). Under the DMA, a large platform whose control of an important gateway between businesses and consumers gives it durable power. Chapter 13.
- GDPR** (*Regulamentul general privind protecția datelor (RGPD)*). The EU's General Data Protection Regulation, which governs the processing of personal data. Chapter 11.
- Government failure** (*eșecul statului*). A situation in which government intervention produces worse outcomes than the problem it was meant to solve, because of poor information, misaligned incentives, or capture. Chapter 1.
- Information asymmetry** (*asimetrie informațională*). A situation in which one party to a transaction knows more than the other. Chapter 2.
- Information good** (*bun informațional*). A good that consists of information, such as software, music, or news, typically with high fixed and near-zero marginal costs. Chapter 1.
- Insourcing** (*reinternalizare*). Bringing previously outsourced work back in-house. Chapter 9.
- Intellectual property** (*proprietate intelectuală*). Legal rights that give creators temporary, limited exclusivity over ideas and their expression. Chapter 10.
- Lemons problem** (*problema „lămâilor”*). Akerlof's account of how hidden quality can drive good products out of a market. Chapter 2.
- Market failure** (*eșecul pieței*). A situation in which a market left to itself allocates resources inefficiently, for example because of externalities, public goods, or information asymmetry. Chapter 1.
- MiCA** (*Regulamentul privind piețele criptoactivelor*). The EU regulation on markets in crypto-assets, Regulation (EU) 2023/1114. Chapter 6.
- Misinformation** (*informare eronată*). False or misleading information spread without intent to deceive. Chapter 12.
- Moral hazard** (*hazard moral*). The problem of hidden action after a transaction, when a party shielded from the consequences changes its behaviour. Chapter 2.
- Multi-homing** (*utilizarea mai multor platforme*). Using several competing platforms at the same time. Chapter 5.
- Nash equilibrium** (*echilibru Nash*). A combination of strategies in which no player can gain by changing its own strategy alone. Chapter 4.
- Nearshoring** (*nearshoring (relocare în țări apropiate)*). Moving work to nearby countries. Chapter 9.
- Network effect** (*efect de rețea*). The increase in a product's value to each user as more people use it. Chapter 5.
- Occupational licensing** (*autorizarea profesiilor*). A legal requirement to hold a licence in order to practise a profession or trade. Chapter 2.
- Offshoring** (*delocalizare (offshoring)*). Moving work to another country, usually to reduce costs. Chapter 9.
- Outsourcing** (*externalizare (outsourcing)*). Contracting a third party to perform part of a firm's work. Chapter 9.
- Patent** (*brevet de invenție*). A temporary exclusive right over an invention or process, typically for around twenty years. Chapter 10.

Patent thicket („hățiș” de brevete). A dense web of overlapping patents that makes it costly to innovate in a field. Chapter 10.

Personal data (*date cu caracter personal*). Any information relating to an identified or identifiable person. Chapter 11.

Platform (multi-sided) (*platformă (piață cu mai multe laturi)*). A business that creates value by connecting two or more groups of users. Chapter 5.

Price differentiation (*diferențiere a prețurilor*). Charging different prices to different buyers for essentially the same good, according to willingness to pay; also called price discrimination. Chapter 1.

Price dispersion (*dispersia prețurilor*). Variation in the prices charged for the same good by different sellers. Chapter 1.

Price signal (*semnal de preț*). The information conveyed by a price about scarcity, value, and cost. Chapter 1.

Price taker (*agent primitor de preț*). A firm too small to influence the market price, which must accept the price the market sets. Chapter 1.

Principal-agent problem (*problema principal-agent (problema de agenție)*). The difficulties that arise when one party delegates a task to another whose interests differ and whose actions it cannot fully observe. Chapter 3.

Prisoner’s dilemma (*dilema prizonierului*). A game in which each player’s individually rational choice leads to an outcome worse for both than cooperation. Chapter 4.

Proof of stake (*dovada mizei*). A consensus mechanism that selects validators in proportion to the assets they pledge. Chapter 6.

Proof of work (*dovada muncii*). A consensus mechanism in which participants compete to solve computational puzzles. Chapter 6.

Public choice theory (*teoria alegerii publice*). The application of economic reasoning to politics and government, treating voters, politicians, and officials as self-interested actors. Chapter 3.

Public good (*bun public*). A good that one person’s use does not diminish and from which non-payers cannot easily be excluded. Chapter 1.

Rational ignorance (*ignoranță rațională*). The choice to remain uninformed when the cost of acquiring information exceeds its expected benefit, as for most voters. Chapter 3.

Regulatory capture (*capturarea autorității de reglementare*). The shaping of regulation mainly in the interest of the industry it is meant to govern. Chapter 2.

Reinforcement learning from human feedback (*învățare prin întărire din feedback uman*). Training an AI model by having people rate its outputs. Chapter 8.

Repeated game (*joc repetat*). A game played many times by the same players, in which the shadow of the future can sustain cooperation. Chapter 4.

Residual loss (*pierdere reziduală*). The loss to a principal that remains after monitoring and incentives have done what they can. Chapter 3.

Robotic process automation (RPA) (*automatizarea robotică a proceselor*). Software that mimics a person’s actions in computer systems to carry out rule-based tasks. Chapter 7.

Screening (*screening (filtrare)*). A choice designed by the less-informed party that leads the other side to reveal its type. Chapter 2.

Search cost (*cost de căutare*). The time and effort needed to find out what different sellers offer and charge. Chapter 1.

Signalling (*semnalizare*). A costly action by the better-informed party that credibly reveals what it knows. Chapter 2.

Smart contract (*contract inteligent*). A program stored on a blockchain that executes automatically when its conditions are met. Chapter 6.

Stablecoin (*monedă stabilă (stablecoin)*). A crypto-asset designed to keep a stable value, usually against a currency such as the dollar or the euro. Chapter 6.

Trade secret (*secret comercial*). Valuable confidential information protected for as long as it remains secret. Chapter 10.

Trademark (*marcă*). A name, logo, or symbol that identifies the source of a product, protected for as long as it is used. Chapter 10.

Transaction costs (*costuri de tranzacție*). The costs of using the market: searching, negotiating, contracting, and enforcing agreements. Chapter 9.

Versioning (*versionare*). Offering the same underlying product in several versions at different prices so that customers sort themselves by willingness to pay. Chapter 1.

Zero-sum game (*joc de sumă nulă*). A game in which one player's gain is exactly another's loss. Chapter 4.

Answers to Self-check Questions

These short answers to the self-check questions are meant for checking your understanding after you have tried each question yourself. They are deliberately brief; the chapters give the full explanation.

Chapter 1. Markets and Price Signals

1. What information does a price transmit?

A price condenses dispersed knowledge about how scarce a good is, how much buyers value it, and how costly it is to produce into a single number. People can respond to that number without knowing the reasons behind it, which lets millions of decisions be coordinated without a central planner.

2. Define the market-clearing price.

It is the price at which the quantity buyers want to purchase exactly equals the quantity sellers want to supply, so that there is neither a shortage nor a surplus.

3. Name three causes of market failure.

Externalities, such as pollution, whose costs fall on third parties; public goods, which are undersupplied because those who do not pay cannot be excluded; and information asymmetries, which can drive good products out of a market (Chapter 2).

4. What is price elasticity, and why does it matter for how a tax is shared?

Elasticity measures how strongly quantity responds to a change in price. A tax falls mainly on whichever side of the market is less able to adjust: if demand is inelastic, buyers bear most of it; if supply is inelastic, sellers do.

5. Give two examples of government failure, and explain why it should be compared with market failure.

Rent controls that shrink the supply of rental housing and licensing rules that protect incumbents from competition are two examples; subsidies that outlive their purpose and regulators captured by the industry they oversee are others. Because intervention is carried out by people with their own incentives and limited information, the real choice is between two imperfect institutions, not between an imperfect market and a perfect state.

6. Why does costly search allow the same good to sell at different prices?

Finding out what different sellers charge takes time and effort, so buyers stop searching once another enquiry is expected to save less than it costs. Many therefore buy without knowing the lowest price, and sellers can charge different prices for the same good, as Stigler showed in 1961.

7. Why are information goods often sold in versions or bundles?

Their first copy is costly but further copies cost almost nothing, so pricing at marginal cost would never recover the fixed cost. Versioning lets customers sort themselves by willingness to pay, and bundling evens out differences in how much customers value individual items, so the seller can recover its costs and serve more customers.

Chapter 2. Information Asymmetry

1. What is the difference between adverse selection and moral hazard?

Adverse selection arises before a deal, from hidden information about quality or type, as in the market for lemons. Moral hazard arises after a deal, from hidden action, when a party shielded from the consequences changes its behaviour where it cannot be observed.

2. For a signal to be credible, what must be true of its cost?

It must be cheaper for the high-quality type to send than for the low-quality type to fake. Otherwise everyone would send it and it would reveal nothing.

3. *Define screening and give an example.*

Screening is a choice designed by the less-informed party that leads the other side to reveal its type. An insurer that offers a low-premium, high-deductible policy alongside a high-premium, low-deductible one finds that low-risk customers tend to choose the first and high-risk customers the second.

4. *Why does a strong brand reduce information asymmetry?*

A brand is a valuable reputation that a firm would lose by selling poor quality, so it works as a credible promise. Buyers can rely on it without inspecting each product.

5. *What is regulatory capture, and why does it matter for remedies against information asymmetry?*

Regulatory capture is the tendency, described by Stigler in 1971, for regulation to be shaped and run mainly in the interest of the industry it governs. Because regulators often know less than the firms they oversee and organised firms lobby harder than dispersed consumers, rules meant to protect the uninformed can end up protecting incumbents instead, as some occupational licensing does.

Chapter 3. The Principal-Agent Problem

1. *Define agency cost and name its three components.*

Agency cost is the total cost of delegating a task to an agent whose interests differ from the principal's. Its components are monitoring costs, the cost of the incentives used to align the agent, and the residual loss that remains.

2. *Why can a principal rarely observe the agent's effort directly?*

Effort happens largely out of sight, and results depend also on luck and on conditions beyond the agent's control, so outcomes are only a noisy guide to effort. Watching continuously would be prohibitively costly.

3. *What is residual loss?*

It is the loss that remains after monitoring and incentives have done what they can: the difference between what a perfectly aligned agent would have achieved and what the actual agent delivers.

4. *Give two ways a contract can better align an agent with a principal.*

Tie the agent's reward to the outcome the principal cares about, for example through commissions that rise with the sale price or performance bonuses, and defer part of the reward, for example through equity or deferred pay, so that the agent shares in long-term results.

5. *Why might voters be rationally ignorant, and what follows for how governments behave?*

A single vote almost never changes an election, so the cost of studying policy in detail exceeds the expected benefit for most voters. Small, organised groups with much at stake follow policy closely instead, so elected officials, as agents, may serve concentrated interests at the expense of the dispersed public, the central insight of public choice theory.

Chapter 4. Game Theory

1. *Name the three ingredients of any game.*

Players, the strategies available to them, and the payoffs that result from each combination of strategies.

2. *Define a Nash equilibrium in your own words.*

It is a combination of strategies in which no player can do better by changing its own strategy alone, given what the others are doing, so the outcome is self-enforcing.

3. *Why can repetition sustain cooperation in a prisoner's dilemma?*

When players expect to meet again, betrayal today can be punished tomorrow, so the value of continued cooperation can outweigh the one-off gain from betrayal.

4. *State one major limitation of game theory in the real world.*

Real players are not perfectly rational and rarely have complete information; real situations involve many players and shifting rules, so game theory disciplines reasoning more than it delivers exact predictions.

Chapter 5. Platforms and the Sharing Economy

1. *Can you define a cross-side network effect?*

It is the effect by which the value of a platform to one group of users rises with the number of users on another side, as when more drivers make a ride-hailing app more useful to riders and more riders make it more attractive to drivers.

2. *Why is trust infrastructure described as the platform's core product rather than an add-on?*

A platform asks strangers to transact, and they will not do so without trust. Ratings, verification, secure payments, insurance, and dispute resolution substitute for personal acquaintance, so without them the network itself unravels.

3. *What do the DSA, the DMA, and the Platform Work Directive each regulate?*

The Digital Services Act sets duties on illegal content, transparency, and user protection, heaviest for the largest platforms. The Digital Markets Act imposes competition obligations on designated gatekeepers. The Platform Work Directive presumes employment where a platform controls the work and requires transparency about the algorithms that manage workers.

4. *Give one positive and one negative externality of the sharing economy.*

Positive: better use of idle assets and services reaching places traditional providers ignored. Negative: short-term lets blamed for raising rents and hollowing out neighbourhoods, or insecurity for gig workers.

5. *How do ratings and reviews relate to the ideas of signalling, screening, and repeated games?*

They are a reputation mechanism that counters adverse selection by revealing quality (Chapter 2); vetting users and requiring deposits are forms of screening; and the prospect of a bad review turns a one-off transaction into something like a repeated game, in which bad behaviour is punished (Chapter 4).

Chapter 6. Blockchain and Smart Contracts

1. *What problem is a blockchain fundamentally trying to solve?*

How parties who do not trust each other can keep a shared, reliable record without depending on a trusted intermediary.

2. *What makes a blockchain immutable, and why is that both a strength and a danger?*

Each block is cryptographically linked to the previous one and the chain is replicated across many computers, so altering a past record would require redoing the work across most of the network. That makes tampering evident, which is a strength, but it also means that mistakes, such as a bug in a smart contract, cannot simply be undone.

3. *When does a blockchain add real value over a conventional database?*

When several parties who do not fully trust each other need a single authoritative record and no neutral, efficient intermediary is available. Where a trusted intermediary already works well, a database is usually simpler and cheaper.

4. *What is MiCA, and what does it govern?*

MiCA is the EU's Markets in Crypto-Assets regulation, Regulation (EU) 2023/1114. It requires crypto-asset service providers to be authorised and imposes reserve and disclosure rules on issuers of stablecoins.

Chapter 7. Robots, RPA, AI and the Future of Work

1. *Can you distinguish RPA, generative AI, and agentic AI, and give an example of each?*

RPA is software that mimics a clerk's keystrokes and follows fixed rules, such as processing supplier invoices. Generative AI produces text, images, code, or audio from instructions in ordinary language, such as drafting a report. Agentic AI chains such models with tools and memory to carry out multi-step tasks, such as researching options and completing a booking.

2. *Why is automation's effect on total employment described as an empirical question rather than a matter of principle?*

Automation displaces some roles, creates new ones, and augments many others at the same time, and which of these movements dominates differs from sector to sector, so the net effect has to be measured rather than deduced.

3. *Which human skills rise in relative value as routine tasks are automated, and why?*

Empathy, persuasion, creative framing, defining problems, judgement under uncertainty, technological literacy, and the disposition to keep learning, because machines still handle these poorly while routine tasks are absorbed first.

4. *Can you name the main phases of the EU AI Act's timeline?*

Entry into force in August 2024; bans and the AI-literacy duty from February 2025; rules for general-purpose models from August 2025; most transparency rules from August 2026; and, after the 2026 Digital Omnibus, high-risk rules from December 2027 for stand-alone systems and August 2028 for AI in regulated products.

5. *Why is delegating a task to an AI system a kind of principal-agent problem?*

The system pursues the objective it was given, which may diverge from what its owner wants, and its reasoning is hard to observe, so the owner faces the same problems of monitoring and incentive design as an employer with an employee.

Chapter 8. Crowdsourcing

1. *Define crowdsourcing.*

Crowdsourcing is the practice of inviting a large, usually online group to contribute ideas, content, labour, or money, instead of relying only on employees or contracted suppliers.

2. *Name the four advantages it offers.*

Diversity, cost-efficiency, speed, and a greater chance of unexpected innovation.

3. *What is the central risk of crowdsourcing, and how does Wikipedia manage it?*

The central risk is quality control. Wikipedia makes every edit visible and reversible, logs every change, can lock disputed pages, insists on cited sources, and relies on volunteer administrators and bots to revert vandalism.

4. *How does crowdsourcing underpin modern artificial intelligence?*

Crowds of workers label images, transcribe audio, rank model outputs, and flag harmful content, and reinforcement learning from human feedback uses people's ratings of answers to train models.

5. *Which ideas from Part I help explain both the promise and the risks of crowdsourcing?*

The promise reflects Hayek's point that knowledge is dispersed among many people (Chapter 1). The risks are principal-agent and information problems (Chapters 2 and 3), because quality and effort are hidden, which is why reputation scores, peer review, and redundancy are used.

Chapter 9. Outsourcing

1. *Name three motives for outsourcing besides cost.*

Focusing on core activities, gaining access to specialised skills and technology, scaling operations up or down with demand, and sharing certain risks with partners.

2. *Distinguish business-process, IT, and knowledge-process outsourcing.*

Business-process outsourcing covers functions such as customer service, human resources, and finance; IT outsourcing covers software development and the running of infrastructure; knowledge-process outsourcing covers expertise-intensive work such as research, analytics, and legal services.

3. *What is the risk of becoming dependent on a single vendor?*

The vendor gains bargaining power, any disruption at the vendor stops the client's operations, and switching becomes costly, especially where the relationship required specific investments.

4. *Why is artificial intelligence described as a threat to the outsourcing model itself?*

Much of what made business-process outsourcing attractive, large volumes of routine, rule-based work, is exactly what AI now automates, so the question becomes whether a person is needed at all, not only where the work is done.

5. *According to Coase, why do firms exist at all?*

Because using the market has transaction costs: finding suppliers, negotiating, contracting, and enforcing agreements. For some activities, directing work inside a firm is cheaper, and a firm grows until organising one more activity internally costs as much as buying it outside.

6. *Why is an outsourcing contract a principal-agent relationship, and how can it be managed?*

The client is the principal and the vendor the agent; their interests diverge and the vendor's effort is hard to observe. Service-level agreements, bonuses and penalties, audits, and the credible threat of switching vendors align the two.

Chapter 10. Intellectual Property

1. *Name the four main forms of intellectual property and what each protects.*

Patents protect inventions and processes; trademarks protect names, logos, and symbols that identify a source; copyright protects original works of authorship; trade secrets protect valuable confidential information.

2. *Why is intellectual property described as a bargain?*

Society grants creators a temporary, limited exclusivity in exchange for the incentive to create and, for patents, the disclosure of how the invention works, after which it passes into the public domain.

3. *What does it mean to say that intellectual property is territorial?*

Rights exist only in the countries that grant them, so a patent or trademark in one country gives no protection in another, and global firms must manage a patchwork of national systems and treaties.

4. *State the central tension that intellectual-property law must balance.*

Protection must be strong enough to reward creation but not so strong that it blocks the follow-on innovation that builds on earlier work.

5. *Why is the length of copyright protection a political as well as an economic question?*

Intellectual property is a monopoly granted by the state, and rights-holders are organised while the public that pays is dispersed. The 1998 US extension, which added twenty years even to existing works that no longer needed an incentive, shows how lobbying can push terms beyond what the economic case supports.

Chapter 11. Big Data, Privacy, and GDPR

1. *Name four principles that govern the processing of personal data under the GDPR.*

Any four of: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and security; and accountability.

2. *What is the maximum fine the GDPR allows?*

Up to twenty million euros or four per cent of global annual turnover, whichever is greater.

3. *What does data minimisation require?*

That an organisation collects and processes only the personal data that are necessary for the specified purpose, and no more.

4. *List three rights the GDPR gives individuals.*

Any three of the rights of access, rectification, erasure (the right to be forgotten), data portability, objection, and the right not to be subject to decisions taken solely by automated means.

5. *How can a privacy regulation end up favouring the largest firms?*

Compliance costs are largely fixed and well-known services find it easier to obtain consent, so large firms cope better than small ones. Studies of the GDPR found that websites concentrated on fewer, larger technology vendors and that venture investment in European start-ups fell.

Chapter 12. Social Media and Fake News

1. *What is the difference between misinformation and disinformation?*

Misinformation is false or misleading information spread without intent to deceive; disinformation is false information spread deliberately to mislead.

2. *How do engagement-optimising algorithms end up amplifying falsehood?*

They promote content that provokes strong reactions, and sensational or divisive falsehoods tend to provoke them, so such content is amplified as a by-product, while filter bubbles shield it from challenge.

3. *What is a deepfake, and why does it raise the stakes?*

A deepfake is realistic text, audio, image, or video fabricated with AI to show people saying or doing things they never did. It undermines the assumption that recordings are evidence and makes disinformation cheap to produce at scale.

4. *Name two of the layered defences against fake news discussed in the chapter.*

Any two of: detection tools, provenance standards that label where media came from, the AI Act's labelling duties, the Digital Services Act's risk-management duties for large platforms, and media literacy.

5. *Why can laws against fake news become a threat to free expression?*

Someone must decide what is false, and officials and platforms make mistakes, as Facebook's reversal on the origin of COVID-19 showed. Such laws have also been used against critics, as in Malaysia and Singapore, which is why rules that focus on platforms' processes are generally preferred to giving the state power to declare what is true.

Chapter 13. Big Tech vs Big Government

1. *What does the Digital Markets Act do, and to whom does it apply?*

It designates the largest platforms as gatekeepers and imposes clear, up-front obligations on them, such as letting business users steer customers to other offers and refraining from favouring their own services, with fines of up to ten per cent of worldwide turnover, or twenty per cent for repeat offences.

2. *Why is content moderation described as having no clean answer?*

It sets two goods against each other: platforms can moderate too little, leaving harassment, fraud, and incitement, or too much, suppressing lawful speech, and giving the state power to compel removal risks censorship.

3. *What did the US court decide about Google, and what remedy followed?*

In 2024 a federal court found that Google had unlawfully monopolised search. In 2025 it ordered remedies that stopped short of a break-up but curbed exclusive default-placement deals and required Google to share certain data with rivals.

4. *State the test the chapter proposes for judging any intervention.*

Name the specific harm, ask whether the intervention actually addresses it, and weigh that against the harm the intervention itself may cause.

References

This list gathers in one place all the works cited in the Further Reading sections throughout this book.

- Acemoglu, D., Autor, D., Hazell, J., & Restrepo, P. (2022). Artificial intelligence and jobs: Evidence from online vacancies. *Journal of Labor Economics*, 40(S1), S293-S340.
<https://doi.org/10.1086/718327>
- Acemoglu, D., & Johnson, S. (2023). *Power and progress: Our thousand-year struggle over technology and prosperity*. PublicAffairs.
- Acemoglu, D., & Restrepo, P. (2019). Automation and new tasks: How technology displaces and reinstates labor. *Journal of Economic Perspectives*, 33(2), 3-30.
<https://doi.org/10.1257/jep.33.2.3>
- Agrawal, A., Gans, J., & Goldfarb, A. (Eds.). (2019). *The economics of artificial intelligence: An agenda*. University of Chicago Press.
<https://www.nber.org/books-and-chapters/economics-artificial-intelligence-agenda>
- Akerlof, G. A. (1970). The market for “lemons”: Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84(3), 488-500.
<https://www.jstor.org/stable/1879431>
- Alfaro, L., & Chor, D. (2023). *Global supply chains: The looming “great reallocation”* (NBER Working Paper No. 31661). National Bureau of Economic Research.
<https://www.nber.org/papers/w31661>
- Amiti, M., Redding, S. J., & Weinstein, D. E. (2019). The impact of the 2018 tariffs on prices and welfare. *Journal of Economic Perspectives*, 33(4), 187-210.
<https://doi.org/10.1257/jep.33.4.187>
- Annenberg Public Policy Center. (n.d.). *FactCheck.org*.
<https://www.factcheck.org>
- Antràs, P. (2020). *De-globalisation? Global value chains in the post-COVID-19 age* (NBER Working Paper No. 28115). National Bureau of Economic Research.
<https://www.nber.org/papers/w28115>
- Arntz, M., Gregory, T., & Zierahn, U. (2020). Digitization and the future of work: Macroeconomic consequences. In K. F. Zimmermann (Ed.), *Handbook of labor, human resources and population economics* (pp. 1-29). Springer.
https://doi.org/10.1007/978-3-319-57365-6_11-1
- Assad, S., Clark, R., Ershov, D., & Xu, L. (2024). Algorithmic pricing and competition: Empirical evidence from the German retail gasoline market. *Journal of Political Economy*, 132(3), 723-771.
<https://doi.org/10.1086/726906>
- Axelrod, R. (1984). *The evolution of cooperation*. Basic Books.
<https://www.basicbooks.com/titles/robert-axelrod/the-evolution-of-cooperation/9780465005642/>
- Baptista, J. P., & Gradim, A. (2020). Understanding fake news consumption: A review. *Social Sciences*, 9(10), Article 185.
<https://doi.org/10.3390/socsci9100185>
- Bebchuk, L. A., & Tallarita, R. (2022). *The perils and questionable promise of ESG-based compensation* (ECGI Law Working Paper No. 671/2022). European Corporate Governance Institute.
https://www.ecgi.global/sites/default/files/working_papers/documents/theperilsandquestionablepromiseofesgbasedcompensationecgi.pdf

- Bergemann, D., Bonatti, A., & Gan, T. (2022). The economics of social data. *The RAND Journal of Economics*, 53(2), 263-296.
- Bergh, D. D., Ketchen, D. J., Orlandi, I., Heugens, P. P. M. A. R., & Boyd, B. K. (2019). Information asymmetry in management research: Past accomplishments and future opportunities. *Journal of Management*, 45(1), 122-158.
<https://doi.org/10.1177/0149206318798026>
- Bessen, J. (2022). *The new Goliaths: How corporations use software to dominate industries, kill innovation, and undermine regulation*. Yale University Press.
- Bichler, M., Knörr, J., & Maldonado, F. (2023). Pricing in nonconvex markets. *Information Systems Research*, 34(2), 652-675.
<https://doi.org/10.1287/isre.2022.1139>
- Boldrin, M., & Levine, D. K. (2008). *Against intellectual monopoly*. Cambridge University Press.
- Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.
- Brown, Z. Y., & MacKay, A. (2023). Competition in pricing algorithms. *American Economic Journal: Microeconomics*, 15(2), 109-156.
<https://doi.org/10.1257/mic.20210158>
- Buchanan, J. M., & Tullock, G. (1962). *The calculus of consent: Logical foundations of constitutional democracy*. University of Michigan Press.
- Cabral, L., Haucap, J., Parker, G., Petropoulos, G., Valletti, T., & Van Alstyne, M. (2021). *The EU Digital Markets Act: A report from a panel of economic experts*. Publications Office of the European Union.
- Chen, L. (2019). Retailers' differentiation strategy and pricing in the rental market of digital content. *Journal of Theoretical and Applied Electronic Commerce Research*, 14(3), 61-75.
<https://www.mdpi.com/0718-1876/14/3/22>
- Coase, R. H. (1937). The nature of the firm. *Economica*, 4(16), 386-405.
<https://doi.org/10.1111/j.1468-0335.1937.tb00002.x>
- Coates, J. C. (2023). *The problem of twelve: When a few financial institutions control everything*. Columbia Global Reports.
- Cohen, S., Kadach, I., Ormazabal, G., & Reichelstein, S. (2023). Executive compensation tied to ESG performance: International evidence. *Journal of Accounting Research*, 61(3), 805-853.
<https://doi.org/10.1111/1475-679X.12481>
- Comuzzi, M., Grefen, P., & Meroni, G. (2023). *Blockchain for business: IT principles into practice*. Routledge.
<https://www.routledge.com/p/book/9781032342467>
- Coyle, D. (2021). *Cogs and monsters: What economics is, and what it should be*. Princeton University Press.
- Dixit, A. K., & Nalebuff, B. J. (2008). *The art of strategy: A game theorist's guide to success in business and life*. W. W. Norton.
<https://wnnorton.com/books/9780393337174>
- Einav, L., Finkelstein, A., & Fisman, R. (2023). *Risky business: Why insurance markets fail and what to do about it*. Yale University Press.
- Engin, Z., & Treleaven, P. (2019). Algorithmic government. *The Computer Journal*, 62(3), 448-460.
<https://ieeexplore.ieee.org/abstract/document/8852885>
- European Commission. (n.d.). *The Digital Services Act package*. Shaping Europe's Digital Future.
<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

- European Commission. (n.d.). *Timeline for the implementation of the EU AI Act*. AI Act Service Desk.
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act>
- European Commission. (2025, April 23). *Commission finds Apple and Meta in breach of the Digital Markets Act* [Press release].
<https://digital-strategy.ec.europa.eu/en/news/commission-finds-apple-and-meta-breach-digital-markets-act>
- European Data Protection Board. (n.d.). *Guidelines, recommendations and best practices*.
https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en
- European Patent Office. (2023). *New study reveals how IP helps startups raise finance*.
<https://www.epo.org/en/news-events/news/new-study-reveals-how-ip-helps-startups-raise-finance>
- European Union. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- European Union. (2017). *Directive (EU) 2017/828 as regards the encouragement of long-term shareholder engagement (Shareholder Rights Directive II)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/dir/2017/828/oj>
- European Union. (2019). *Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/dir/2019/771/oj>
- European Union. (2019). *Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/dir/2019/790/oj>
- European Union. (2022). *Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/reg/2022/1925/oj>
- European Union. (2022). *Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
- European Union. (2023). *Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/reg/2023/1114/oj>
- European Union. (2023). *Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/reg/2023/2854/oj>
- European Union. (2024). *Directive (EU) 2024/1760 on corporate sustainability due diligence*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/dir/2024/1760/oj>
- European Union. (2024). *Directive (EU) 2024/2831 on improving working conditions in platform work*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/dir/2024/2831/oj>
- European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- European Union. (2026). *Regulation (EU) 2026/1744 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial*

- intelligence (Digital Omnibus on AI)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/eli/reg/2026/1744/oj>
- European Union Intellectual Property Office. (2025). *The development of generative artificial intelligence from a copyright perspective*. Publications Office of the European Union.
<https://doi.org/10.2814/3893780>
- Fisher, M. (2022). *The chaos machine: The inside story of how social media rewired our minds and our world*. Little, Brown.
- Gereffi, G., Humphrey, J., & Sturgeon, T. (2005). The governance of global value chains. *Review of International Political Economy*, 12(1), 78-104.
<https://doi.org/10.1080/09692290500049805>
- Gneezy, U. (2023). *Mixed signals: How incentives really work*. Yale University Press.
- Goldberg, S. G., Johnson, G. A., & Shriver, S. K. (2024). Regulating privacy online: An economic evaluation of the GDPR. *American Economic Journal: Economic Policy*, 16(1), 325-358.
- Goldfarb, A., & Que, V. F. (2023). The economics of digital privacy. *Annual Review of Economics*, 15, 267-286.
- Goodman, P. S. (2024). *How the world ran out of everything: Inside the global supply chain*. Mariner Books.
- Government of Romania. (2019). *Ordonanța de urgență nr. 49/2019 privind activitățile de transport alternativ cu autoturism și conducător auto*. Monitorul Oficial al României.
<https://legislatie.just.ro/Public/DetaliiDocument/215598>
- Greenstone, M., He, G., Jia, R., & Liu, T. (2022). Can technology solve the principal-agent problem? Evidence from China's war on air pollution. *American Economic Review: Insights*, 4(1), 54-70.
<https://doi.org/10.1257/aeri.20200373>
- Grinvald, L. C., & Tur-Sinai, O. (2019). Intellectual property law and the right to repair. *Fordham Law Review*, 88(1), 63-127.
<https://ir.lawnet.fordham.edu/flr/vol88/iss1/2/>
- Harvey, C. R., Ramachandran, A., & Santoro, J. (2021). *DeFi and the future of finance*. Wiley.
- Hayek, F. A. (1945). The use of knowledge in society. *The American Economic Review*, 35(4), 519-530.
<https://www.jstor.org/stable/1809376>
- Howe, J. (2008). *Crowdsourcing: Why the power of the crowd is driving the future of business*. Crown Business.
<https://www.penguinrandomhouse.com/books/192616/crowdsourcing-by-jeff-howe/>
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305-360.
[https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
- Jia, J., Jin, G. Z., & Wagman, L. (2021). The short-run effects of the General Data Protection Regulation on technology venture investment. *Marketing Science*, 40(4), 661-684.
- Johnson, G. A., Shriver, S. K., & Goldberg, S. G. (2023). Privacy and market concentration: Intended and unintended consequences of the GDPR. *Management Science*, 69(10), 5695-5721.
- Klein, T. (2021). Autonomous algorithmic collusion: Q-learning under sequential pricing. *The RAND Journal of Economics*, 52(3), 538-558.
- Lehdonvirta, V. (2022). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. MIT Press.
- McIntyre, D. P., Srinivasan, A., Afuah, A., Gawer, A., & Kretschmer, T. (2021). Multisided platforms as new organizational forms. *Academy of Management Perspectives*, 35(4), 566-583.

- Milgrom, P. R. (2021). Auction research evolving: Theorems and market designs. *American Economic Review*, 111(5), 1383-1405.
<https://doi.org/10.1257/aer.111.5.1383>
- Muldoon, J., Graham, M., & Cant, C. (2024). *Feeding the machine: The hidden human labour powering AI*. Canongate Books.
- Murgia, M. (2024). *Code dependent: Living in the shadow of AI*. Picador.
- National Academies of Sciences, Engineering, and Medicine. (2024). *Artificial intelligence and the future of work*. The National Academies Press.
<https://doi.org/10.17226/27644>
- National Supervisory Authority for Personal Data Processing. (n.d.). [Official website of the Romanian data protection authority, ANSPDCP].
<https://www.dataprotection.ro/?lang=en>
- Osborne, M. J. (2003). *An introduction to game theory*. Oxford University Press.
<https://global.oup.com/ushe/product/an-introduction-to-game-theory-9780195128956>
- Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. *Trends in Cognitive Sciences*, 25(5), 388-402.
<https://doi.org/10.1016/j.tics.2021.02.007>
- Perzanowski, A. (2022). *The right to repair: Reclaiming the things we own*. Cambridge University Press.
- Petit, N. (2020). *Big Tech and the digital economy: The moligopoly scenario*. Oxford University Press.
<https://doi.org/10.1093/oso/9780198837701.001.0001>
- Ponti, M., & Seredko, A. (2022). Human-machine-learning integration and task allocation in citizen science. *Humanities and Social Sciences Communications*, 9, Article 48.
<https://doi.org/10.1057/s41599-022-01049-z>
- Rathje, S., Van Bavel, J. J., & van der Linden, S. (2021). Out-group animosity drives engagement on social media. *Proceedings of the National Academy of Sciences*, 118(26), Article e2024292118.
<https://doi.org/10.1073/pnas.2024292118>
- Rietveld, J., & Schilling, M. A. (2021). Platform competition: A systematic and interdisciplinary review of the literature. *Journal of Management*, 47(6), 1528-1563.
<https://doi.org/10.1177/0149206320969791>
- Robertson, V. H. S. E. (2020). Excessive data collection: Privacy considerations and abuse of dominance in the era of big data. *Common Market Law Review*, 57(1), 161-189.
<https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/57.1/COLA2020006>
- Samuelson, P. (2023). Generative AI meets copyright. *Science*, 381(6654), 158-161.
<https://doi.org/10.1126/science.adi0656>
- Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, 103(2), 153-174.
<https://doi.org/10.20955/r.103.153-74>
- Schniederjans, M. J., Schniederjans, A. M., & Schniederjans, D. G. (2010). *Outsourcing and insourcing in an international context*. Routledge.
<https://doi.org/10.4324/9781315701936>
- Schor, J. (2016). Debating the sharing economy. *Journal of Self-Governance and Management Economics*, 4(3), 7-22.
<https://greattransition.org/publication/debating-the-sharing-economy>

- Shapiro, C., & Varian, H. R. (1999). *Information rules: A strategic guide to the network economy*. Harvard Business School Press.
- Spence, M. (1973). Job market signaling. *The Quarterly Journal of Economics*, 87(3), 355-374.
<https://doi.org/10.2307/1882010>
- Stigler, G. J. (1961). The economics of information. *Journal of Political Economy*, 69(3), 213-225.
<https://doi.org/10.1086/258464>
- Stigler, G. J. (1971). The theory of economic regulation. *The Bell Journal of Economics and Management Science*, 2(1), 3-21.
<https://doi.org/10.2307/3003160>
- Suciu, M. C., Năsulea, C., & Năsulea, D. F. (2019). Towards developing a friendlier regulatory framework for blockchain-based businesses. *Theoretical and Applied Economics*, Special Issue, 15-24.
<https://www.researchgate.net/publication/335755763>
- Suciu, M. C., Năsulea, C., & Năsulea, D. (2020). Knowledge decentralization in the age of blockchain: Developing a knowledge-transfer system using digital assets. In F. Matos, V. Vairinhos, I. Salavisa, L. Edvinsson, & M. Massaro (Eds.), *Knowledge, people, and digital transformation* (pp. 261-274). Springer.
https://doi.org/10.1007/978-3-030-40390-4_17
- Suciu, M. C., Năsulea, D. F., & Năsulea, C. (2020). Smart city innovation within the sharing economy. *Proceedings of the International Conference on Business Excellence*, 14(1), 1147-1157.
<https://doi.org/10.2478/picbe-2020-0107>
- Sutherland, W., & Jarrahi, M. H. (2018). The sharing economy and digital platforms: A review and research agenda. *International Journal of Information Management*, 43, 328-341.
<https://doi.org/10.1016/j.ijinfomgt.2018.07.004>
- Syed, R., Suriadi, S., Adams, M., Bandara, W., Leemans, S. J. J., Ouyang, C., ter Hofstede, A. H. M., van de Weerd, I., Wynn, M. T., & Reijers, H. A. (2020). Robotic process automation: Contemporary themes and challenges. *Computers in Industry*, 115, Article 103162.
<https://doi.org/10.1016/j.compind.2019.103162>
- Taherdoost, H. (2023). Smart contracts in blockchain technology: A critical review. *Information*, 14(2), Article 117.
<https://doi.org/10.3390/info14020117>
- U.S. Department of the Treasury Office of Economic Policy, Council of Economic Advisers, & U.S. Department of Labor. (2015). *Occupational licensing: A framework for policymakers*. The White House.
https://obamawhitehouse.archives.gov/sites/default/files/docs/licensing_report_final_nonembargo.pdf
- United States v. Google LLC, No. 1:20-cv-03010 (APM) (D.D.C. Sept. 2, 2025) (memorandum opinion on remedies).
<https://www.justice.gov/atr/case/us-and-plaintiff-states-v-google-llc-2020>
- van der Linden, S. (2023). *Foolproof: Why misinformation infects our minds and how to build immunity*. W. W. Norton.
- Vermicelli, S., Cricelli, L., & Grimaldi, M. (2021). How can crowdsourcing help tackle the COVID-19 pandemic? *R&D Management*, 51(2), 183-194.
<https://doi.org/10.1111/radm.12443>
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146-1151.
<https://doi.org/10.1126/science.aap9559>
- Webb, M. (2019). *The impact of artificial intelligence on the labor market* [Working paper]. SSRN.
<https://doi.org/10.2139/ssrn.3482150>

Williamson, O. E. (1985). *The economic institutions of capitalism*. Free Press.

World Intellectual Property Organization. (n.d.). *What is intellectual property?*
<https://www.wipo.int/about-ip/en>

Zhao, M., Wang, S., & Xia, T. (2025). The social welfare effect of e-commerce product reputation information asymmetry from the perspective of network externality. *PLOS ONE*, 20(1), Article e0313852.
<https://doi.org/10.1371/journal.pone.0313852>