© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

CONTENTS

Introduction: The Battle 1

1 The Code 19

2 The Stack 47

3 The Weaponization of Everything 67

4 The End of the Public Interest 89

5 Tech on the Front Lines 116

6 The Framers 140

7 Reclaiming Sovereignty 174

8 Prioritizing the Public 209

Conclusion: Stop the Tech Coup, Save Democracy 249

Notes 257

Acknowledgments 311

Index 313

For general queries, contact info@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Introduction

THE BATTLE

In early 2010, at a café in the eastern part of Turkey, a young man (I'll call him Ali) told me of his escape from Iran. Ali had been arrested the previous summer during the Green Movement, a series of popular protests that erupted after what many Iranians regarded as a fraudulent presidential election. As Ali sat on the sidewalk with his wrists tied, anticipating being picked up by police and pondering his fate, a local woman happened to drive by. She stopped her car, courageously whisked him away, and dropped him off at home. Despite this brief reprieve, Ali knew that the Basiji, part of the infamous Islamic Revolutionary Guard Corps, would soon be knocking on the door of his parents' place, and he decided to flee to a remote area in the north where his family owned a small plot of land.

Ali was one of millions of Iranians who challenged Mahmoud Ahmadinejad's victory in the presidential election that summer. On June 20, 2009, one of these brave demonstrators, Neda Agha-Soltan, was killed by a sniper. Her death came quickly as she sank down to the pavement, blood running from her mouth, people around her screaming in horror.[1] We know this because, unlike many of the brutal incidents that authoritarian regimes carry out in dark

For general queries, contact info@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

prison cells, Neda's death was captured on a bystander's cell phone. Videos of this and other state violence against peaceful protesters were shared around the world, fueling outrage and condemnation. Green Movement demonstrators posted their eyewitness accounts on social media with the hashtag #iranelection, allowing the entire world to witness a revolution unfolding in one of the most repressive countries on the planet.

The role of social media (specifically, Facebook, Twitter, and YouTube) and the use of technology (cell phones and internet connections) quickly became a defining theme in how journalists and politicians around the world understood the protests in Iran. These platforms were filling an important gap left by the Iranian regime's press crackdown. A few days after the protests started, in a desperate move to regain control, authorities banned journalists from doing any street reporting.[2] Ahmadinejad closed twelve newspapers and locked up over one hundred journalists.[3] Twitter (now known as X) emerged as the main platform for citizens to transmit information about the protests and the government's violence. As a result, some even called the Green Movement a "Twitter Revolution."[4] There was a widespread sense of hope about the democratizing potential of these nascent technologies; beyond using social media and cell phones to document and share human rights abuses, activists could also use them to coordinate actions and mobilize their movement. The administration of U.S. president Barack Obama even asked Twitter to delay a planned systems update to avoid temporarily disabling access for protesters in Iran.[5]

This hopefulness about technology as a partner in liberation was bolstered in 2010 as popular protests erupted in Tunisia and Egypt. When Egyptians revolted against the regime of President Hosni Mubarak, Western media proclaimed it a "Facebook revolution," in homage to the gigantic Facebook groups formed by youth protesters to coordinate the demonstrations.[6] Many believed that young people in the Middle East and North Africa would be better equipped to secure justice and rights with the help of U.S.-made technologies.

While Western media and policy circles excitedly buzzed about the democratizing potential of new technologies, the picture on the

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

ground in Cairo, Tehran, and Tunis was not as straightforward. As Iranian journalist Golnaz Esfandiari would later explain, activists typically used word of mouth, text messages, emails, and blog posts to organize protests rather than social media.[7]

Finally, as Ali himself would soon discover, cell phone technology exposed protesters to enormous risks. When he arrived at his hideout destination in the north of Iran, he called his mother to tell her he was safe. Her relief would not last long: Ali's phone signal was picked up by a nationwide monitoring network, and he was arrested soon thereafter, in the middle of nowhere. He ended up in the notorious Evin Prison, known for the brutal rape and torture of inmates.[8] After spending several dreadful months behind Evin's walls, he was able to escape during a furlough and eventually made his way to eastern Turkey. Yet even at the time of our meeting in early 2010, he still changed locations every day, since he knew that the Iranian security services were actively hunting down dissidents across the border.

Those who praised the democratizing possibilities of technology and social media platforms failed to appreciate that repressive authoritarian regimes could be tech-savvy too. In Iran, and later in Syria, state authorities tactically lifted bans on the use of internet services, only to later scan posts to incriminate the messengers. The same technologies that help detect spam assisted state militias with identifying authors of antiregime social media posts. Military intelligence services were able to use location services to spot a group of people gathering on a street corner—real-time information that can be very useful when looking to disperse crowds before they can form.

I was appalled by the suffering the Iranian protestors endured; Neda Agha-Soltan was only four years younger than I was at the time. Their courage also deeply inspired me. I had recently won an election for a seat in the European Parliament by criticizing the Dutch government, while people in Iran were being shot by theirs for doing the same. I felt shocked—not by the behavior of these repressive governments, from whom I expected little else, but by our own double standards. The monitoring and surveillance technology these regimes

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

were using came from Europe: Italian-made hacking systems were the technology of choice for the regime of Bashar al-Assad in Syria, while French technologies helped Muammar al-Gaddhafi in Libya and British systems facilitated the Mubarak regime in Egypt.[9]

Right when European governments were condemning the repression of people and their human rights, European companies were exporting sophisticated monitoring software to Middle Eastern rulers. As Nokia-Siemens Networks would admit in 2010, they sold cell phone surveillance technologies to the Iranian authorities that enabled them to track the protesters—people who were peacefully asking for freedoms that any European today takes for granted.[10] In a hearing before the Subcommittee on Human Rights of the European Parliament, Nokia-Siemens's head of marketing tried to distance the company from Iran's abuses, arguing that, ultimately, "people who use this technology to infringe human rights are responsible for their actions."[11] While this is obviously true—no one disputes that the Iranian government is responsible for its actions—this does not absolve the company of its moral obligation to avoid assisting a repressive government. Engineers of companies with such contracts would have traveled to Iran multiple times to train users or to repair surveillance systems, and they likely received additional pay for staffing a hardship post. Moreover, the human rights violations in Iran were well known and well documented even before the crackdown on protests began in 2009.

As a newly elected member of the European Parliament, I was incensed by Ali's story, as well as by the stories of the other Iranian refugees I met on my trip to Turkey. What meaning did European statements in support of human rights even have when global tools of repression were produced right here at home? These double standards became a galvanizing foundation for much of my work in public service. I would spend the next decade using every policy tool imaginable trying to stop what I then called "digital arms"—software that inevitably violates human rights and ends up harming innocent people.[12] Unfortunately, there is still much more work to be done. Today, newer versions of these commercial hacking systems have only grown in force and scale. Even worse, as I learned more about

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

the sprawling digital arms trade over the past decade, I realized that Iran's Green Movement was merely one battle in the war to protect democracy from technological overreach.

The Reveal

When the Pegasus Project released a series of articles about government espionage in the summer of 2021, the news filled me with a mix of horror and hope.[13] Pegasus is the flagship spyware product of NSO Group—an Israeli technology firm that holds the pole position in the billion-dollar global spyware market. Sold as a counterterrorism and crime-fighting solution all over the world, spyware often ends up being used like a privatized intelligence service to stalk and repress critical voices. The investigative journalists who worked as part of the Pegasus Project revealed NSO Group's hit list: over fifty thousand phone numbers of the potential targets that the organization had been hacking on behalf of their clients.[14] For many, the Pegasus Project displayed the deep impact of hacking and surveillance technologies for the first time.

The leaks revealed the existence of highly sophisticated surveillance and hacking systems that made the tracking and tracing of Ali in Iran look wildly outdated. Pegasus can transform a target's phone or laptop into a live surveillance tool by remotely turning on microphones and cameras without the user's knowledge. These "zero-click" attacks, as they are known, are highly effective because the targeted individual does not even have to click on an infected link or do anything themself for the infiltration to begin. Once NSO Group gains access, its customers can extract contacts, call logs, messages, photos, web browsing history, and settings, and they can gather information from popular communications and chat apps.[15] Unsurprisingly, authoritarian governments across the world have been keen customers. NSO Group was valued at $2.3 billion before the Pegasus Project put a critical spotlight on the company.[16]

Beyond revealing what the technology could do and who was targeted, the leaked documents also showed who was involved with NSO Group. Former officials from the Obama administration and the

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

French government, for instance, had taken lucrative roles as senior advisers with the company—even as the phones of the president of France, the editor in chief of the *Financial Times*, and Hungarian opposition leaders were breached and monitored.[17] Nokia-Siemens's facilitation of Ali's arrest and NSO Group's ongoing dealings with autocrats beg a question: Why wasn't more being done to stop the development and sale of these technologies by democratic governments from within whose borders these companies operated?

One reason, though far from the only one, is that for too long our political leaders have been in the grip of an overly optimistic and self-centered view of new technologies. The data-driven strategies that were part of the successful campaign of Barack Obama in 2008 generated off-the-charts excitement among elected officials the world over. Politicians were keen to embrace new ways to communicate with citizens and constituents. I know this firsthand because communicating on social media platforms certainly helped me win my seat to the European Parliament. As a newcomer on the political stage, I may have never reached potential voters had it not been for Facebook and Twitter. Once elected, these platforms also offered a helpful way to update people on activities that would not be reported in newspapers or TV news bulletins. In my early days in the European Parliament, technological disruption was largely seen as a positive development.

But even as more information about the true nature and shadow sides of these technologies was revealed, and as companies grew massively, public officials did little. By the time the Pegasus Project revelations made headlines in 2021, I had spent a decade fighting the spyware sector and the toxic industry still had not been brought to a halt. Yes, we managed to get the European Union (EU) to adopt export controls, restricting the overseas sales of surveillance tools, but imports and thus domestic use remained untouched.

Naively, I initially thought that my fellow political leaders were not taking action on tech regulation because they simply didn't understand these rapidly evolving technological systems operating below the radar. Though such ignorance may have played a contributing

For general queries, contact info@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

role in their inaction, the primary reason was much more cynical: democratic governments wanted to deploy these technologies too, to spy on their own populations. At the time, Europeans were practically apoplectic over U.S. intelligence services snooping on European leaders, including German chancellor Angela Merkel.[18] The governments of EU member states pushed new legislation to protect people from falling prey to American surveillance practices. Yet despite these governments' very public outrage, their own police forces quietly procured sophisticated infiltration systems to go after criminals and terror suspects. To this day, few European government agencies will admit to using Pegasus or similar systems. Later, in 2022, additional significant cases of spyware abuse, including the hacking of opposition leaders, judges, and journalists by the governments of Greece, Poland, and Spain were revealed.[19] Researchers from the Carnegie Endowment for International Peace created an index showing that seventy-four governments had contracted with commercial firms to obtain spyware or digital forensics technology.[20] In my home country, freedom of information requests to Dutch police went unanswered, but sources told investigative journalist Huib Modderkolk that Pegasus was used to hack the devices of Ridouan Taghi, the country's most notorious fugitive Mafia boss.[21]

In the United States, broader awareness about mass surveillance practices of U.S. intelligence services hardly led to decisive legal change. A decade after Edward Snowden's revelations, journalists, parliamentarians, and citizens are still barely capable of bringing transparency to the procurement of tech systems and services by democratic governments. It is a vivid reminder of how 9/11 continues to cast a long shadow over security policy, leading to disastrous moral confusion. On the one hand, there is the illusion of a clear line between democratic countries and their enemies. In the name of security, illiberal surveillance practices continue to erode civil liberties at the heart of democratic societies. On the other hand, to my frustration, the plight of human rights defenders and journalists in the Global South—many of whom were first to have been targeted by Western-made spyware—generated too little urgency to address the issue.

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

The failure of the Green Movement in Iran, as well as the lack of proper policy responses by democratic governments, made something manifestly clear during my first year in office: if technology was to serve people and promote democracy as it promised, laws were needed to turn those hopes into realities and to guard against both corporate opportunism and authoritarian capture. Merely assuming that information and communication technology (ICT) would foster the spread of democracy was clearly a failed strategy. Defending and advancing democratic principles would require intentionally updating and creating laws to express, revive, and protect those principles from both external threats and threats within our own borders. Indeed, today's attacks on democracy do not come from just authoritarian states or a loss of trust in the democratic process. The gradual erosion of democracy in our time is being accelerated by the growing, unaccountable power of technology companies, of which NSO Group is only one, albeit extreme, example.

The Global Shift

The unaccountable power of technology companies and the threat that they pose to democracy are by now familiar refrains. The newspapers are littered daily with scandals that cover the latest revelation of problems at one or another social media platform, search engine, or retail platform. The purpose of this book is not to preach to the choir and rehash those stories, however significant and urgent they may be. Instead this book begins from the premise that these incidents point to systemic problems that need unpacking: the fact that our social, professional, and civil lives are increasingly digitized and, essentially, *all* aspects of digitization are in the hands of private companies; that certain technologies have inherently antidemocratic characteristics, while laws to protect democratic values and the rule of law are lagging; and that, most important, democratic governments' outsourcing of key functions has led to a hollowing out of governments' core capabilities. These systematic problems are now undermining the core principles of democracy: free and fair elections, the rule of law, the separation of powers, a well-informed

For general queries, contact info@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

public debate, national security and the protection of civil liberties such as freedom of expression, the presumption of innocence, and the right to privacy. Undermining principles have practical consequences; as we'll see in the coming chapters, tech's metastatic and unchecked growth has resulted in real-world violence, instability, and division.

The digital revolution has seen private companies increasingly take on functions normally assumed by states, leading to a concerning erosion of agency and accountability. For instance, Elon Musk's Starlink satellites, which dominate satellite-based internet services worldwide, have military chiefs worried, and with good reason: in the middle of the Russian war of aggression, Musk personally denied a request from Ukraine to turn on Starlink near Crimea. The Ukrainian government would need the connectivity to launch surprise attacks on Russian occupying naval vessels. But Musk decided the risk of Russian retaliation in the form of a nuclear attack was too great—a significant political decision from a businessman, and one he had the power to make. On Twitter the billionaire bragged, "Between Tesla, Starlink and Twitter, I may have more real-time economic data in one head than anyone ever."[22] Governments are beginning to realize that the tech sector's outsize influence is a major problem. President Joe Biden admitted as much on August 25, 2021, after inviting tech CEOs to a White House summit on cybersecurity: "The reality is," he noted, "most of our critical infrastructure is owned and operated by the private sector."[23] The U.S. president, arguably the most powerful leader in the world, conceded that the government alone cannot protect the homeland, and it needs tech companies to lend a hand.

That private companies, rather than the government, are responsible for such basic tasks as protecting national security and gathering intelligence may not have sunk in with the general public quite yet. Without public outcry, the needed regulation, oversight, and accountability are not moving along at the necessary speed.

During my years in the European Parliament, I progressively came to see technology through the lens of power. Technology could help emancipate people and raise unheard voices, or it could

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

transform disruptors into monopolists who ruthlessly pursued efficiency, surveillance, scale, and profit. In either case, technology is not neutral. As I will elaborate in this book, systems are themselves designed with values built into them, even if that is unintended. Additionally, given that most technologies are developed by private companies, these technologies are ultimately deployed for profit maximization, and profit maximization incentives are often misaligned with what is best for society. Sam Altman's Worldcoin, for example, aspires to build a global identity database by asking people in developing countries to scan their irises, in return for a bit of cryptocurrency; the firm is either blind or completely cavalier to the risks of concentrating so much sensitive biometric data under one roof.[24] Social media platforms seek to extend online engagement time of their users with little concern for the negative effect on teenagers' mental health.[25] Tech firms and their products now also make potentially life-altering decisions. Commercial algorithms designate triage statuses in hospitals and analyze medical images.[26] All the while, democratically elected representatives remain in the dark about key details of how these products work, since independent research is often impossible. For too long, too much trust has been placed in tech companies without making sure that their technology operates within the parameters of the rule of law and supports democratic outcomes.

An abdication of responsibility on the part of democratically elected leaders is what led to Pegasus being used to track members of the opposition in Poland and what enabled the Iranian government's monitoring of Ali. Laws are not updated to ensure that digital means of repression or intrusion are banned in the way that physical means would be. For instance, a conventional raid of an opposition party politician's home would immediately set off alarm bells, yet when hacking tools are deployed, there is less clarity or concern over the same kind of digital "raid." The introduction of new technologies seems to blur lawmakers' vision; they cannot fathom that violations of fundamental rights—like privacy and free expression—in the digital world are just as grave, while at times they are made much more easily and can be more vast in scope. Corporate leaders and aspiring

For general queries, contact info@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

autocrats alike take advantage of this situational blindness and push the boundaries of the law. As digitization progresses, we see a gradual shift in responsibility and power away from democratic leaders. This shift accelerates two trends: growing digital authoritarianism and a wholesale decline in democratic governance.

In comparison to the European and U.S. governments, who have largely allowed private tech companies to operate as they please, the Chinese Communist Party (CCP) has made sure that new technologies serve its political system and values. It has spent the last two decades deploying them toward its own political advantage. The artificial intelligence (AI) sector, for instance, is powered by the limitless data collected by the Chinese government, whose repressive practices are fueling innovations from facial recognition applications to new ways of influencing and controlling massive amounts of people. During the COVID-19 pandemic, tracking apps were mandatory in China and used to survey whether people stayed at home in quarantine.[27] Similarly, the state uses sophisticated monitoring methods to verify and incarcerate the Uyghur minority population, both developing and entrenching state power.[28]

It is a model that China eagerly exports through the Digital Silk Road, as well as its other development projects. By investing in infrastructure and offering cloud computing to other countries, China keeps them connected with their data and development. Egypt, for example, has relied heavily on Chinese investment to modernize its telecommunications infrastructure and even construct a new smart city. The North African country has now also adopted China's model of internet governance via a new cybercrime law, and Egyptian government officials routinely attend Beijing's censorship training.[29]

The strategic marriage of geopolitics and technology in China lays bare how far technology governance lags on the part of democratic countries, a discrepancy that not only impacts the citizens of those countries but also affects the ability of nations to come to shared rules and solutions. It is difficult for the United States to lead the international community toward consensus on robust technology regulations, for example, given its laissez-faire approach toward Silicon Valley. China offers a cohesive, top-down governance model,

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

ready to be copied. This mismatch further entrenches the agency of both corporate powers and authoritarian states.

The entangled nature of technology—linking economics, security, and rights—requires an integrated political vision. Yet democratic leaders have too often responded to disruptions with inaction or a piecemeal approach, and they struggle to articulate an alternative to the technology industry's preferred hands-off approach to regulation. Without a blueprint for how to enshrine democratic standards domestically, a credible foreign policy agenda is impossible. To rein in the outsize power of technology companies, regain control over their products' basic functions, and protect democratic values on the world stage, democratic countries need to develop more robust legal and governance frameworks, effective institutions, and strong incentives that avoid abuses of power on the part of states or companies using technologies.

The Task

Reinventing democratic governance to match the challenges of digitization will not be an easy task. Today's policy processes are running out of sync with the pace and scale of corporate operations. This mismatch is a growing problem for those who believe democracy should not be disrupted, no matter how exciting the shiny new objects from Bangalore, Shenzhen, or Silicon Valley might look. It means that democratic governance should be revived and updated.

During my time in office, the more I worked on technology-related issues, the clearer it became that there was a huge and growing gap between corporate power, on the one hand, and democratic regulatory and oversight capability, on the other. In some cases, this is mainly about money. As of January 2024, Apple had a market capitalization of $3 trillion, making it more valuable than the stock markets of Australia and Germany combined.[30] As a result of such resource disparity, the public sector has fallen so far behind the tech sector in innovative capabilities (not to mention salaries, computing power, knowledge, and talent) that its ability to set rules for and by the people is severely hampered.

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

In other cases, lawmakers' lack of access to information impedes evidence-based rulemaking. Software is complex: large legacy programs can have tens of millions of lines of code, and machine learning systems may develop rules that even their own creators do not completely grasp. Moreover, companies have learned to use intellectual property law to protect the opacity of proprietary algorithms and to shield their treasured workings behind trade secret protections. In general, existing legal protections, made in an era before the internet even existed, disproportionately benefit companies. The same laws that help Coca-Cola protect its secret recipe also protect technology firms from disclosing how their algorithms function.

Let's consider new challenges to the Freedom of Information Act (FOIA), which journalists use to uncover information about government services. When government services are outsourced to technology companies, FOIA requests regarding those services can be denied when companies invoke intellectual property protections or even privacy standards as an exception to providing openness and accountability. In other cases, government officials will simply not feel bound to preserve records when using private, nongovernmental channels of communication. For instance, the EU's ombudsman had to issue an official ruling to underline that text messages exchanged by EU leaders on WhatsApp are subject to record-keeping and transparency rules, just as official emails and letters are. Just months after its lobbying blitz, Mistral AI announced a partnership with Microsoft, further consolidating AI assets in Silicon Valley.[31]

In some cases, corporate reticence takes absurd forms, as I learned on a trip to Silicon Valley in 2016 with my European Parliament colleague Kaja Kallas, who has gone on to serve as the prime minister of Estonia. We were working on new legislation that concerned illegal speech on online platforms and traveled halfway around the world to meet with representatives of Facebook, Google, and Yahoo. At most companies, legal teams walked us through the company policies for dealing with illegal and harmful content and underlined how they worried about protecting freedom of expression. But our experience at 1 Hacker Way, Facebook's headquarters in Menlo Park, California, was altogether different. We began the day with a long tour of the

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

campus as guides steered us around like tourists at Disneyland, pointing out every piece of whimsical art and the all-you-can-eat cafeterias in the vast, multicolored office building. When we finally took our seats in a meeting room, our hosts broached a conversation about *Lean In,* the new and highly influential book from Facebook's then-COO, Sheryl Sandberg, that considered the gender-based challenges facing women in the workplace. The conversation might have been interesting for a weekend book club, but we had not come all this way to talk about *Lean In*. When we reminded our hosts that we were there to discuss what responsibility the social media platform had to moderate content uploaded by users, they responded with polite smiles and nods: "Oh, we are terribly sorry, but for that subject you would need to talk to our legal team," to which we replied, "Well exactly, that is why we are here." Unfortunately, we were told, the people with expertise and authority to speak with us were not available.

This visit, peculiar in its own right, also spoke to a far more fascinating dynamic in Silicon Valley. Corporate giants did not feel accountable to lawmakers like me. They thought that they could dodge real policy and enforcement questions with free frozen yogurt and inspirational buzzwords—and we hadn't yet proven them wrong. As democratic governance long failed to impose guardrails on companies like Facebook, they had grown to believe that they operated above the law.

The Delivery

In 2019, after serving more than a decade in the European Parliament, I stepped down from politics and moved to the belly of the beast: Silicon Valley and Stanford University. I wanted to help bridge the gaps between the worlds of politics, policy, and technology.

Not long after I arrived at Stanford, I attended a presentation that confirmed just how badly such bridges were needed. The speaker, an engineer who had just left Instagram, shared fascinating experiences about curation of content through algorithms and how taste and culture could be shaped by decisions of what photos were posted on the front page of a user's feed. In other words, technology could be used to shape behavior and consumption. The engineer then discussed

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

how this allowed companies of a certain size to move and affect markets. By putting a post of a celebrity with a cosmetics product on the homepage, the company significantly increased the likelihood that the product would see an uptick in sales.

When the time came for questions, I took the microphone. Did that ability to move and create markets, I asked, also imply the possibility of influencing, shaping, or moving political beliefs, values, and behavior more widely? Could it also move masses? A popular meme ridiculing a candidate in a political race, a call by a popular influencer to go shopping instead of voting on Election Day, or the sale of merchandise from the Black Lives Matter movement or the National Rifle Association, for instance, could be increasingly powerful if their reach was amplified. As it is not always easy to define clearly what qualifies as political content online, I wanted to know about the discussions among engineers and whether the societal or political impacts were ever considered when designing recommendation algorithms that cater to billions of people. The engineer admitted that they did not understand the question. In a way, that was the clearest answer I could have asked for.

The fulfillment of the democratic promise by politicians and states has never been perfect. But the Churchillian adage, that democracy is the worst form of government except for all others, still holds. We must preserve democracy, and to do that, our governments must regain control over our society's technological capabilities. While there are some encouraging signs in terms of new laws, regulatory proposals, and citizen initiatives, they remain too slow and ad hoc to truly shift the status quo and restore the balance of power between public authorities and private companies. These alone won't stop the privatization of the entire digital sphere. While many like to contrast the EU's and the United States' different legal and political cultures, I prefer to emphasize the unfortunate paralysis and tendency toward inaction that they have in common. The entire democratic world has been too slow to build a democratic governance model for technologies, and countries have not done so together. Ash Carter, the late former U.S. secretary of defense, lamented the "ethos of public purpose that has become dangerously decoupled from many of today's leading tech endeavors."[32] I agree.

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Democracy is not flawless, nor does it claim to be. What the political system possesses, however, is the ability to improve. As Samantha Power explains, "Democracy wins out in the long run because it offers a chance to fix its own mistakes. It is the only system built on the premise that if something is not working, people can actually correct it, from the bottom up. Democracy works best when people are given the opportunity to constantly monitor and repair the kinks in the machinery."[33] At its best, democracy is deliberate, self-correcting, and compromise-generating. It is never static but is a process in motion. And that should give us hope for its future.

It is time to normalize the way we think about updating laws and adopting regulations to match the power of technology companies. To understand what this could look like, we can look to another tool that saw exponential growth over the past century: cars. People and governments are aware of the benefits of cars. But it would have been shortsighted if, out of fear of stifling automobile growth, governments refrained from requiring driver's licenses, imposing safety regulations, or addressing the environmental harms and other negative externalities produced by driving. Moreover, when a particular model of car systematically breaks down, no one expects individual drivers to take responsibility. No one believes that merely by starting the engine, the driver has agreed to accept any underlying flaws or dangers in the car's design. No one would believe a simple statement by the car manufacturer that the car is safe, environmentally friendly, and energy efficient. All these elements, standards, and commitments are independently tested to make sure that people are safe and the environmental damage is limited. Companies are not blindly trusted to preserve the public interest, and when corporate leaders violate these standards—for instance, as when Volkswagen lied about emissions while tampering with emissions software—parliamentary inquiries seek to bring accountability. Even though cars are complex technologies, rules about their qualifications were put in place and guardrails around their use adopted. Doing the same for digital technologies is both urgently needed and practically possible.

The history of the car's influence on society also offers another important lesson for the task we confront in this book. Today we

For general queries, contact info@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

have huge roads, bridges, and parking structures; we have enormous factories for the production of cars; natural resources are drilled and burned to ensure that cars can be driven; and we have traffic rules that apply on public roads. All this existing infrastructure is difficult to reverse or ignore. The same will happen with digital infrastructure soon enough, and the laws we adopt today will determine the path of emerging technologies and the trajectory of their associated infrastructure. We must act wisely. Without rules to protect people's safety, to regulate behavior in public spaces, or to ensure that companies are doing as they say and saying as they do, the harm to society and indeed to democracy will be significant.

This is a book about the impact of digital disruption on democracy. This is, of course, far from the only problem with the tech industry. However, I am choosing a focused lens here, as I am convinced that a loss of insight, agency, and oversight on the part of citizens and public institutions cannot be compensated for with the exciting perspectives of economic growth or innovation benefits. I am not under the illusion that technology can be stopped. It should not be, and I am hopeful and excited about what technology can continue to bring to us all. Yet I am very critical of a powerful, unaccountable industry that, to date, has been almost entirely without guidance or guardrails from democratic authorities. Solving the accountability gap is particularly urgent because technology is not a sector but a layer that impacts almost all sectors.

In Support of Democracy

This is not a book against technology but in favor of democracy. It is a call to rebalance technology's role in democratic societies to ensure better protection of democratic values. It urges democratic governments to safeguard the public sphere, to develop future-proof solutions, and to revive and reinvent its approach to tech regulation, knowing that new technologies will continue to challenge and disrupt. We do not have time to address these harms in an ad hoc manner: endlessly debating whether Facebook's community standards are helpful or not shifts our attention away from broader and more

For general queries, contact info@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

systemic issues. A new approach to tech policy needs to be holistic, looking at the bigger picture and always in service of strengthening democratic principles. In other words, it is time to tackle the causes, not the symptoms.

The Tech Coup shifts the spotlight from Big Tech's scandals to the systematic erosion of democracy as private companies run ever more parts of our digital lives. You, as a democratic citizen, are invited to help shape an agenda that puts the survival of democratic principles ahead of short-term economic benefits. States can remain very powerful actors if they choose to be, as unfortunately illustrated by the bitter success of authoritarian models of governing in the digital world. Revitalizing democracy will require new approaches to lawmaking and innovative forms of governance designed to explicitly support democratic principles in new contexts. And it will demand that we craft and enforce policies that better equip democracy for surviving the twenty-first century. While technological fixes are necessary, they alone are insufficient, and for any of them to work, we need a broader, functional political infrastructure to serve the people.

Restoring democratic governance over technological systems—instead of allowing privatized governance over our digital world—will go a long way toward making the world a more fair, just, and equitable place.

For general queries, contact info@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

INDEX

Aadhaar (biometric system), 202–3, 204
Abed, Gabriel, 90
Abure, Julius, 129
accountability mechanisms, 238, 239–40, 240–42
Advanced Research Projects Agency Network, 29
Advanced Semiconductor Materials Lithography (ASML), 53, 191
Afghanistan, 81, 95
African Union (AU), 199, 200
Agha-Soltan, Neda, 1–2, 249
Ahmadinejad, Mahmoud, 1, 2
AI. *See* artificial intelligence
AI Act, 176, 182, 212, 223
AI application, 215–16, 246–47; AI law (2021), 209; bias and discrimination, 246–47; classification of, 209–10; decoupling, 192; high-risk, defined, 210; nondiscrimination law, 252; precautionary principle, 218
AI arms races, 167–68
AI-based chatbots, 164
AI companies, 169–70, 215, 218
AI-generated content, 227
AI law (2021), 209–12. *See also* AI Act
AI regulation, 168–70, 182, 212
Airbnb, 40
AI-trained systems, reliance on, 168
Alameda Research, 99
Alcatel-Lucent, 57
Alexander, Keith, 69
Algemene Inlichtingen- en Veiligheidsdienst, 229
Ali, 3, 10
Alibaba, 175, 194, 198
Alipay, 37
Allan, Richard, 40
Alphabet, 41, 57
al-Shabaab, 120, 122
Altmaier, Peter, 175
Altman, Sam, 10, 169–71, 223
Amazon: GDPR, response to, 180; government contracts, value of, 233; lobbying spending, 160; market capitalization, 41; systemically important technology institution, 238; undersea cables, 57; U.S. Department of Defense subcontracts, 29; water usage, data centers, 62
Amazon Pay, 205
Amazon Web Services (AWS), 62–63, 134
American Civil Liberties Union, 31
American Data Privacy and Protection Act, 177
American surveillance practices, 7
Amini, Mahsa, 249
Andreessen, Marc, 19, 95, 255
Anduril, 131
Anguilla, 49
Annan, Kofi, 121
Anonymous, 72
Ant Group, 198
Anti-Corruption Foundation, *Putin's Palace*, 116
antidemocratic technologies and practices, 219–20; cryptocurrencies, 224–25; data brokers, 221–22; facial recognition systems, 223–24; spyware, 220–21
antigovernment attitudes, 24, 26–28
antiregulation rhetoric. *See* framing
antitrust regulation, 189
Apple, 12, 36, 41, 160, 196–97
Araud, Gerard, 40
Ardern, Jacinda, 157
Argentina, 95, 181
artificial intelligence (AI): antiregulation rhetoric, 29; back to the core, 253–255; Bard, 167; BlenderBot 3, 163–64; CCP, 11; chatbot trolls, 166; content moderation, 165–66; discrimination, 246–47; Executive

For general queries, contact info@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

artificial intelligence (AI) (*continued*) Order on AI, 170; GPT-4, 164–65, 167; GPT-5, 167; identify, 226–27; large language model, 164–65, 166; Microsoft, 162; mistakes, 165; OpenAI saga, 170–71; Palantir, 109; pattern recognition, 164; precautionary principle, 215–19; prioritizing the public, 209–10, 212; regulation, AI leaders call for, 168–69; regulation, need for, 166–67; regulation, OpenAI rebuffs, 169–70; self-justifying, 165; self-regulation, 144, 163; sovereignty, reclaiming, 176, 192, 195, 198, 208, 282; tech coup, reversing, 251, 252; test corpus, 164; transparency, 228–29, 232; untested AI products, releasing, 167; who rules, 163–71. *See also* AI Act; Clearview AI; generative AI

Ashcroft, John, 34

ASML. *See* Advanced Semiconductor Materials Lithography (ASML)

Assad, Bashar al-, 4

Assembly Bill 5 (California), 160

attribution, 134–35

AU headquarters, Chinese-made IT, 199

AWS. *See* Amazon Web Services (AWS)

Baird, Ross, 44

Balticconnector, 55

Bank for International Settlements (BIS), 97, 102

Bankman-Fried, Sam, 98–100

Bannon, Steve, 141

Barbados dollar, 90

Bard, 167

Barlow, John Perry, 23–24

Bass, Karen, 126

Belt and Road Initiative, 184, 199, 200

Benjamin, Ruha, 155

Berners-Lee, Tim, 22, 23, 31, 157

Bezos, Jeff, 37

Bharti Airtel, 205

Bhatia, Karan, 198

bias: AI application, 246; Clearview, 111, 113; commonsense solution to, 107; facial recognition systems, 105–6; maliciously and accidentally, 111; Tay (chatbot), 165; Trump accusation, 37

Biden, Joe: Big Tech, regulation of, 177; China, weakening tech capabilities, 191; Colonial Pipeline ransomware attack, 76–77; DarkSide, warning to, 78; Defend Forward strategy, 137; internet governance, 38–39; regulation, alternative pathways, 189–90; Section 230 (Communications Decency Act), 38; tech governance, 38–39; tech sector influence, 9; technology, promoting of, 230; TikTok, view of, 186; Twitter account hacked, 79. *See also* Biden White House

Biden, Joe, administration, 192, 227, 235

Biden White House, 78, 133, 189–90

Big Tech, 28–29, 41–42, 144–49

Bildt, Carl, 19

Bimodal Voter Accreditation System, 128–29

Binance, 99, 225

Bing search engine, 167, 218

biometric data: Clearview AI, 104, 107; cybersecurity nightmare, 203; facial recognition systems, 223; India, 202–3; Kenyans, 124; regulation of, 223; Safran, 123; Uyghurs, 195; Worldcoin, 10, 223

biometric identification, 123, 202–3

biometric identification, Safran (Kenya), 123

biometric identification system, India, 202

biometric profiles, Clearview AI, 107

biometric system, India, 202

biometric voter registration, Kenya, 124

biometrics, Clearview AI, 104

Bitcoin: catfish, 101; crash, 96–97; criminal use of, 101; cyberattacks, 79–80; downside of, 102; El Salvador, 95; Jalisco Cartel, 101; overview, 91–92; Sinaloa Cartel, 101; speculative investment asset, 98. *See also* blockchain; cryptocurrencies

"Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto), 94

Bitcoin mining, 102

Bitcoin wallet, 79, 97

Black, Ed, 34

black hat hackers, 85

Black Lives Matter protests, 105

blacklisting mechanism, 235–36

Blavatnik School of Government, 162

BlenderBot 3 (Meta), 163–64, 165, 166

Blinken, Antony, 250

blitzscaling, 25–26

blockchain, 89–90, 91–95, 100, 102, 103

Blockchain Revolution (Tapscott and Tapscott), 90

BlockFi, 100

Blueprint for an AI Bill of Rights (White House Office of Science and Technology Policy), 157

Booz Allen Hamilton, 112

botnets, 136

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Bourla, Albert, 230
Bouverot, Anne, 123
Bowden, Mark, *The Finish*, 111
Box, 142
Branson, Richard, 89, 101
Brazil, Clean Network Initiative, 191
breaches: Aadhaar, 203; the battleground, 81, 83–85; FireEye, 88; Microsoft, 236; Mitto, 71; threats to the public interest, 114; the weaponization of everything, 68, 71
Breton, Thierry, 183, 209
Broadband Privacy Act, 37
Brockman, Greg, 171
Bromley, James, 99–100
Brown, Shontel, 99
Brussels, 181–82
Brussels Effect, 180, 182
BSA / the Software Alliance, 39
Buchanan, James, 54
Build America, Buy America Act, 235
Bukele, Nayib, 95
Buolamwini, Joy, 105–6
Bureau of Industry and Security, 191
Bureau of Investigative Journalism, 231
Burt, Tom, 161
Bush, George W., administration, 33–34
Buttarelli, Giovanni, 181
Buttigieg, Pete, 77
BuzzFeed, 61, 105
Byler, Darren, 195

Cadwalladr, Carole, 141, 155
California Delete Act, 222
calls, 156, 157–58
Cambridge Analytica, 140–43
Canvas (online teaching platform), 63
Carney, Jay, 40
Carter, Ash, 15
Carter, Jimmy, 119
Carter Center, 119, 124
catfish, 101
Cato Institute, 31
CCP. *See* Chinese Communist Party (CCP)
Celsius, 97, 100, 102
censorship: China, 11, 177, 190, 241; EU, 32; India, 178, 204; Iran, 250; media, 42; Navalny's app, 117; Russia, 116–17; social media, 148
Center for Strategic and International Studies, 191
Central Bank Digital Currency (CBDC), 103
Cerf, Vint, 22, 33
CERN, 22
Chan Zuckerberg Initiative, 40
Chander, Anupam, 32
Chaos Computer Club (CCC), 86–87
chatbot trolls, 166
ChatGPT, 164, 218
Chatham House rule, 20
Cheney, Dick, 34
Chew, Shou Zi, 185
Chicago Tribune, 180
Children's Online Privacy Protection Act, 147
China: AI arms race, 167–68; cryptocurrency, banning, 102–3, 225; Digital Silk Road, 11, 177–78, 200–201, 207; Global South, 7, 177, 199–200, 241; long-term espionage operation, 135; microchip supply chain, 51–52; National Intelligence Law, 175; Palantir, 110; semiconductor demand, 51; surveillance model, exporting globally, 177; surveillance state, 177; technologies, for political goals, 177–78; ZTE, 177, 199, 200. *See also* Huawei
China, building the surveillance state: Africa, 199–200; American companies, banning, 197–98; Ant Group, 198; Apple operations, 196; apps, removing, 196–97; Belt and Road Initiative, 199, 200; citizens, rights curtailed, 195; content moderators, 195; data flows, 198, 201; decoupling, 195–96; digital repression, 195; intellectual property theft, 194; joint venture obligation, 197; Made in China 2025, 198, 199; operating in, benefits and drawbacks, 196–97; Safe City technology, 195; tech dominance, rise to, 194; technological revolution, instrument of communist system, 194–95; technology, exporting, 199–201; technology industry, regulating, 193–94; Uyghur Muslim minority, repression of, 195; WeChat, 198; Weibo, 195, 198
China, decoupling with United States, 167, 178, 192, 195–96, 207
Chinese Communist Party (CCP), 11, 37, 102–3, 177–78, 185, 207. *See also* China; TikTok
Christchurch Call, 157
Cinia Group, 49
CISA. *See* Cybersecurity and Infrastructure Security Agency (CISA)
Citigroup, 238
Citrix, 73–75

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Clarke, Yvette, 227
Clean Apps, 191
Clean Cable, 191
Clean Cloud, 191
Clean Network Initiative (CNI), 190–91
Clean Path, 191
Clean Store, 191
ClearSky, 75
Clearview, 107, 131, 223–24
Clearview AI, 103–8, 112–13, 223
Clegg, Nick, 40, 151
Clinton, Hillary Rodham, 40
cloud computing: carbon footprint, 62; China, 11, 195; data centers, 48, 64; providers, 62, 175; security concerns, 62–63; significant public power, 243–44; universities, 243
Cloudflare, 72
CO_2 footprint, 235
code, the, 19–22; the corporates, 26–30; the net result, 42–46; the pioneers, 22–26; the politicians, 30–39; the revolving door, 39–42
code of conduct on countering illegal hate speech online, 156
code of practice, 156
Cohen, Jared, 40
Coinbase, 225
Collins, Damian, 155
Colonial Pipeline ransomware attack, 76–78
commercial attribution, 83, 135
Commission Nationale de l'Informatique et des Libertés (CNIL), 107
Commodity Futures Trading Commission, 99
Communications Decency Act (CDA), 31–32
COMPAS (risk assessment tool), 168
conclusion, 249–56
Congressional Budget Office, 236
Congressional Research Service, 51, 236
Consumer Financial Protection Bureau, 188
Consumer Protection Division (FTC), 154
Content Advisory Council (TikTok), 153–54
content moderation: artificial intelligence, 165–66; Digital Services Act, 157; European Union, 176, 206; Facebook's Supreme Court, 149–50; India, 204–5; social media platforms, 156, 254; tech governance, 31; Twitter, 154; Ukraine, 153
content moderators, 166, 195
Cook, Tim, 37
cooling-off period, 237
core, the, back to, 253–56
corporate reticence, 13–14
corporate-state power balance, 29
Corruption Index, 129
covert investments, 228–29
COVID-19 pandemic, 67, 96, 110, 230
Cowen, Tyler, 164
Cox, Christopher, 31
crime prediction software, 106
criminal motives, 80
Crockett, Jasmine, 99
Cross, David B., 134
Cruz, Ted, 140
cryptocurrencies: Afghanistan, 95; Argentina, 95; China, 102–3, 225; criminals, use by, 101; dark side, 90–91; direct or indirect bans, 103; Dubai, 96; FTX, 98–100; investment figures, 96–97; Islamic State of Iraq and Syria (ISIS), 101; Jalisco Cartel, 101; Middle East, 96; overview, 91–96, 224–25; rogue states, 101–2, 224; Sinaloa Cartel, 101; Singapore, 95–96
cryptocurrencies, use of the term, 97–98
cryptocurrencies crash, 96–103
cryptocurrency mining, 62, 64
cryptocurrency scams, cost of, 101
Curse of Bigness, The (Wu), 38
cyberattacks: arbitration court, 239–40; Ashley Madison, 80; civilian targets (Ukraine), 135–36; CyberPeace Institute, 161; Finland, 79; front lines, on the, 133–38; International Committee on the Red Cross, 79; Iranian nuclear facilities, 80; LastPass password manager, 88; Mirai malware, 72–73; New Zealand stock exchange, 79; Norwegian Parliament, 79; NSA, 80; Sony Pictures, 79; status of, in conflict and war, 133; Ukraine war, 133; U.S. Office of Personnel and Management, 79; Vatican, 79. *See also* weaponization of everything, the
Cyber Defenders Council, 134
Cyber Threat Intelligence team (Accenture), 80
cyberoperations, 88, 137
CyberPeace Institute (CPI), 161–62
Cybersecurity and Infrastructure Security Agency (CISA), 37, 188, 234
Cybersecurity Tech Accord, 157
cyberspace: benign neglect of, 33; companies and governments, 149–58; currency for, 94; Declaration of Independence of Cyberspace, 24; definition of, 24; governments,

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

behavior in, 136; International Strategy for Cyberspace, 35; Microsoft, 161–62; threats to, fending off, 115. *See also* China
cyberwarfare, 82, 133–34
cyberwarfare and threshold of war, 133
cypherpunk movement, 23
cypherpunks, 23, 94, 103

Dahan, Mariana, 90
dark web, 77, 78, 80, 101
DarkSide, 77, 78, 85
data brokerage, 222
data brokers, 221–22
data centers: Apple in Iowa, 61; cloud computing, 62; energy consumption, 62; locating, 61; Netherlands, 58–59; Noord-Holland, 65; oversight, insight to provide, 65–66; polder model, 58–59; political pushback, 63–64; Princess Ariane Wind Farm, 60; Project Osmium (Microsoft), 60; residual heat, 61; secretive lobbying, 60; security concerns, 62–63; transparency, land acquisitions, 229; water use, 61–62; Zeewolde hyperscale data center, 59–60
data-driven decisions, 109
data flows, 55, 198, 201
data-slicing, 108, 110, 111
Decentralized finance (DeFi), 92–94, 95, 101
Declaration of Independence of Cyberspace (1996), 24
Declaration for the Future of the Internet (DFI), 207, 240, 242
De Correspondent Dutch, 103
decoupling, 167–68, 178, 192–93, 195–96, 207
deepfake watermarking, 227
Defend Forward strategy, 137
Defense Advanced Research Projects Agency, 29
Defense tech, 130–31
Dell, Curt, 97, 102
Dell, Victoria, 97
democracy, 8–9, 15–17, 17–18, 118
democracy, battle for, 117–18
democracy and authoritarianism, global competition between, 117–18
democracy's house, renovating, 213–15
democratic governance, 252–56; cryptocurrencies, 102; decline in, 11, 18; democracy's house, renovating, 213–15; public accountability extension, 229–32; the task, 12–14. *See also* sovereignty, reclaiming
democratic governance, reinventing, 12–14
democratic governance model, 15
Democrats, 30, 98, 177, 190
Denham, Jeff, 154
Denmark, 62, 64
Department of Homeland Security, 34
Deutsche Telekom, 175
devolution of power, 33
Diamond, Larry, 19
digital arms (software), 4
digital colonialism, 200
digital commons, 245–46
Digital Europe, 179
digital exceptionalism, 133, 187–88
Digital Geneva Convention, 162
digital governance, 203–4, 240–42
digital Great Wall of China, 201
Digital Markets Act, 182
Digital Peace Now, 162
Digital Personal Data Protection Act, 204
digital public sphere, reinvigorate, 243–44; knowledge to the people, 247–48; public stack, building a, 244–46; regulation-enforcement model, 246–47
digital revolution, 9, 31, 213
digital roads, 66
Digital Services Act, 157, 182, 232, 239
Digital Silk Road, 11, 177–78, 200–201, 207
Digital Sovereignty Initiative, 183–84
digital world: cryptocurrencies, 92; global shift, 10–11; India, 207; India Stack, 203–4; International Strategy for Cyberspace, 35; offense as a means of defense, 137–38; public interest, threats to, 112–15; the stack, 47–49; warfare, revamping laws governing, 138–39
digitization, 8, 10–11
Dillet, Romain, 158
Dimon, Jamie, 97
discrimination, 106, 187, 188, 246–47, 252
disinformation: AI applications, 218; artificial intelligence, 226–27; Biden, 38; cyberattacks, use in, 80; Facebook, 141–42, 150; Hiroshima Process, 241; Msando murder, 124; Real Facebook Oversight Board, 155; TikTok, 187; Trump, 36–37; 2020 U.S. election, 155
distributed denial-of- service (DDoS) attack, 72–73, 133
Dobbs v. Jackson Women's Health Organization, 221, 222
Doctorow, Cory, 45
Dolev, Dan, 97

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Domain Name System, 48–49
domain names, 48–49
Don't Think of an Elephant! (Lakoff), 145–46
Dorsey, Jack, 204
doxing, 38, 222
Dragonfly, 198
Dubai, 96
Dutch Data Protection Authority (DDPA), 181

E-Commerce Directive (2000), 32
Economist, 217
eG8 forum, 145
Egypt, 2–3, 4, 11
8Chan, 156
EirGrid, 63
Eisenhower, Dwight D., 109
election observers, 119, 121, 129
elections: Bankman-Fried, 98–99; digital technologies, 253–54; disinformation, 226; Federal Elections Commission, 227; Kenya, 119–30; outsourcing, 230–31; Russia, 116–17; tech companies and, 41, 118; Zeewolde, 64
electricity usage, 60, 62, 63, 125
El Salvador (Bitcoin), 95
Enact Africa, 130
Enria, Andrea, 113
Ernst & Young, 102, 235
Esfandiari, Golnaz, 3
EU Chips Act, 184
Euronews, Thierry Breton interview, 209
European Commission, 28, 53, 156–57, 209, 230
European External Action Service, 129
European Parliament hearing (Zuckerberg), 143–44
European Parliamentary Technology Assessment Network, 238
European Parliament's Research Service, 236
European privacy bill, 181
European sovereignty, 183
European Union, 178–79, 185; AI regulation, 182; antitrust sanctions, 179; Digital Sovereignty Initiative, 183–84; EU Chips Act, 184; European sovereignty, 183; Gafa, 183; GDPR, 179–81; Global Gateway, 184; lobbying bonanza, 179–80; NextGenerationEU, 184; politics, technology involving, 184–85; regulation, day-to-day side of, 182–83; superregulator, 182; uniform charging outlet, 183
European Union (EU): the battle, 6, 7, 13; the code, 28, 32; the end of public interest, 102, 103, 110, 113; the framers, 144, 157, 160, 169–70; prioritizing the public, 211, 217, 220, 231, 233, 239; reclaiming sovereignty, 175, 176–77, 193, 206; the stack, 51–53; tech on the front lines, 120, 122, 129, 133
Europol, 110
EU-U.S. Trade and Technology Council, 193
Evin Prison, 3
Exchange Server Hack, 79
Executive Order on Artificial Intelligence (October 2023), 227
executive orders, 37, 78, 170, 189–90, 227, 230

fabrication plants (fabs), 50
Facebook: Cambridge Analytica scandal, 141–42, 153; Capitol Insurrection (January 6, 2021), 43; corporate reticence, 13–14; curating speech and amplifying content, 27; EU lobbying, 179–80; India, 205; Iranian protests, 2; lobbying spending, 160; market capitalization, 41; Oversight Board, 149–53, 154, 155; revolving door, 40; used by scrapers, 104; users (2008), 33. *See also* Meta
Facebook Receipts, 155
Facebook revolution, 2
Facebook's Supreme Court, 149–51
Facemash, 33. *See also* Facebook
facial recognition: CCP, 11; embedded bias, examples, 106; model, 164; predictive policing, 107; software, 104; systems, 105–6, 210, 223–24; technologies, 91; tools, 131; Ukraine war, 131. *See also* Clearview
facial recognition accuracy, 105–6
facial recognition systems, 223–24
Farook, Syed Rizwan, 36
Farrow, Ronan, 130
FDA. *See* U.S. Food and Drug Administration (FDA)
Federal Aviation Administration, 154
Federal Bureau of Investigation (FBI): Apple's refusal to unlock phone, 36, 197; Big Tech contracts, 28–29; Colonial Pipeline ransomware attack, 76; DarkSide, 77; Mirai attack, 72–73; Pegasus spyware, purchase of, 220; Silkroad, 101
Federal Bureau of Prisons, 28
Federal Communications Commission, 37, 187, 227
Federal Elections Commission, 227

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Federal Trade Commission (FTC), 27–28, 35, 101, 154, 188–89
fiber optic cables, 47, 48, 54–58
Financial Accounting Standards Board, 154
financial crisis of 2008–2009, 93
Financial Times, 6, 69, 77, 141, 202, 203
Finish, The (Bowden), 111
Finland, 55, 79
FireEye, 83, 88
first principles approach, 247
Fletcher, Peter, 68
Forbes, 67
Foreign Policy magazine, *Securing Our Digital Future*, 161
4Chan, 156
framers, the, 140–44; artificial intelligence, who rules, 163–71; companies mimic governments, 149–58; outmaneuvering the state, 159–63; regulatory void, effect of, 171–73; the spinning game, 144–49
framing, 145–49, 168
France, 175
Francis (pope), 210
Frederik, Jesse, 103
Freedom House, 129
Freedom of Information Act (FOIA), 13
Frontex, 231
FTC. *See* Federal Trade Commission (FTC)
FTX, 98–100

G7 Summit 2023, 241
Gaddhafi, Muammar al-, 4
Gafa (Google, Amazon, Facebook, and Apple), 183
Gaia-X, 110, 175
Garland, Merrick, 136
Gates, Melinda, 159
Gebru, Timnit, 105–6
General Data Protection Regulation (GDPR), 176, 179–81, 182, 246
generative AI, 71, 188–89, 209–12, 219, 226
genetically modified organisms (GMOs), 216, 217
Geneva Conventions, 132
Germany, 32, 175
Global Commission on the Stability of Cyberspace, 162
Global Commission on Internet Governance, 19
Global Gateway, 184
Global Positioning System (GPS), 29, 81
Global South, 7, 177, 199–200, 241
Good, John, 104
Google: the battle, 13–14; the code, 29, 33, 35, 36, 38–39, 40; the framers, 158, 160, 167; prioritizing the public, 233, 238; reclaiming sovereignty, 180, 198, 205; the stack, 60, 61, 62; tech on the front lines, 116–17, 131; the weaponization of everything, 82–83
Google Cloud, 62
Google Ideas (now Jigsaw), 40
Google Pay, 205
Gordon, Bart, 154
Government Communications Headquarters (GCHQ), 200
GPDR. *See* General Data Protection Regulation (GDPR)
GPS, 29, 81
GPT-4, 164–65, 167
GPT-5, 167
Graham, Lindsey, 255
gray-area tactics, 136
Greece, 7, 107
Green Movement, 1, 2, 8, 249
Greenblatt, Jonathan, 155
Greyball, 27–28, 29
Guterres, António, 242

“hack and leaks,” 38
HackerOne, 85
hackers, separating good from bad, 80–81
Harris, Brent, 149
Hatch, Orrin, 143
hate speech, 32, 142, 150, 156–57
Haun, Katie, 90
Heikkila, Melissa, 163
Heinrich, Thomas, 23
“Here’s How Facebook Actually Won Trump the Presidency” (*Wired*), 141
High Court of Kenya, 129
Hill, Kashmir, 103–4
Hiroshima Process, 241
HKMapLive, 196
Hoffman, Reid, 25
Holder, Eric, 40
Huawei, 37, 175, 177, 195, 199, 200
Hughes, Chris, 35
Hussey, Pears, 63
hyperscale data centers, 59–60, 63–64. *See also* data centers
Hypponen, Mikko, 68

IBM, Principles for Trust and Transparency, 158
ICANN’s Governmental Advisory Committee, 118

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

ICT. *See* information and communication technology (ICT)
Immigration and Customs Enforcement (ICE), 28–29, 105, 108–9
incentives, 10, 12, 84–85, 86, 184
Independent Electoral and Boundaries Commission (IEBC), 123, 126–27
India: Aadhaar, 202–3; biometric identification, 202–3; content moderation (censorship), 204–5; democratic backsliding, 178, 201–2; Digital Personal Data Protection Act, 204; digitization, 205–6; foreign stakeholders, 205; GDP, 178; Information Technology Act (2000), 204; internet shutdowns, 178, 202; Modi government, 204; Mumbai terrorist attacks (2008), 204; Netflix effect, 43; operating in, 205; protocol-forward model, 203–4; Punjab, 201–2; takedown requests, 205; TikTok, banning, 204–5
India Stack, 203–4
influence operations, 134, 135, 158, 185, 195, 250. *See also* censorship; lobbying
information and communication technology (ICT), 8, 39, 123, 200
Interactive Citizens' Handbook, An (website), 31
Initiative for Digital Public Infrastructure, 245
Innovation Policy Committee, 38
In-Q-Tel, 109
Insanet, 43–44
Instagram, 14, 104, 250, 251
intellectual property law, 13
intellectual property protections, 13, 231–32
intellectual property rights, 218, 237
intellectual property theft, 194
International Committee of the Red Cross, 79
international conventions, 132
International Criminal Court, 120, 135–36
International Monetary Fund, 224
international regulatory ecosystem, 172
International Strategy for Cyberspace, 35
International Telecommunications Union, 118
Internet Corporation for Assigned Names and Numbers (ICANN), 33
internet governance, 19–20, 33, 59, 194, 207–8, 240
Internet of Things, 45, 114
Internet Protocol (IP) addresses, 48, 74
internet regulation, framing, 147–48
internet shutdowns, 178, 250
internet tax exemption bill, 33
Interxion, 49
introduction, 1–5; the delivery, 14–17; democracy, in support of, 17–18; the global shift, 8–12; the reveal, 5–8; the task, 12–14
investor–state dispute settlement (ISDS) mechanisms, 239
IP addresses. *See* Internet Protocol (IP) addresses
iPhone, 33, 51, 197
Iran: Ali's escape, 1, 3; Citrix hack, 74–75; internet services, tactical use of, 3; Iranian nuclear facilities, 80; Mahsa Amini, death of, 249–50; monitoring and surveillance technology, 3–4; Neda Agha-Soltan, assassination of, 1–2, 249
Ireland, 63, 181
Irish Data Protection Commission, 181
Irish Social Democrats, 63
Islamic State of Iraq and Syria (ISIS), 101
Israel, 43–44

Jalisco Cartel, 101
Japan, 52, 110, 241
Jio Platforms, 205
joint democratic forces, 240–42
joint venture obligation (China), 197
Jonge, Egge Jan de, 60
Jonge, Hugo de, 230
Jordan, Michael, 196
Jourová, Věra, 180
JPMorgan Chase, 79, 97, 238
JPMorgan UK, 224

Kallas, Kaja, 13
Kanter, Jonathan, 38
Kardashian, Kim, 101
Karman, Tawakkol, 152–53
Karp, Alex, 108, 111, 218
Kaye, David, 228
Kemp, Brian, 77
Kennedy, John (senator), 169
Kenya, tech, trust, and elections, 119–20; al-Shabaab, 120, 122; biometric data, potential abuse of, 124; biometric technologies, 123; Carter Center final report, 124; Chris Msando, murder of, 123–24; Corruption Index, 129; data protection legislation, 129; data protection safeguards, lack of, 124–25; digital election day

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

playbook, 125; digital systems security failure, 124; digital technology, embracing, 122–23; digitizing election infrastructure, 123; Freedom House rating, 129; IEBC servers, manipulation complaint, 126; IEBC servers, official review of, 127; political process, improvements to, 129; Safran, 123, 127, 128, 129; Smartmatic, 129–30; wrongdoing, accusation of, 126
Kenya elections: cost of, 128; election annulled, 127; election day, 125; election observers, 121; 2007 election, 120; 2013 election, 120; 2017 election, 122; 2017 election rerun, 127–28; 2022 election, 129–30
Kenya Integrated Elections Management System, 123
Kenyan National Assembly, 129
Kenyan Supreme Court, 126–27
Kenyatta, Uhuru, 120, 126
Kerry, John, 119, 126
Khan, Lina, 38, 189
Khosrowshahi, Dara, 20
Killer App (Palantir), 111
kinetic attacks, 136, 137, 138
King, Jen, 163
Klein, Doug, 73
Klobuchar, Amy, 160
knowledge to the people, 247–48
Krach, Keith, 190–91
Krebs, Chris, 37
Kurz, Sebastian, 40

Lakoff, George, *Don't Think of an Elephant!*, 145–46
Lamothe, Laurent, 90
large language model (LLM), 164–65, 166
LastPass (password manager), 88
Le Monde Afrique, 199
lead by example, 232–38
leadership, need for, 206, 207–8
League of Legends, 98
Lean In (Sandberg), 13, 180
legitimacy, 44, 114–15, 121, 128
Lessig, Lawrence, 33
Levie, Aaron, 142
Lewis, James Andrew, 174
Libya, 4
LinkedIn, 104, 113
Liu, Mark, 51
lobbying, 39, 159–63
lock-in contracts, 243
Los Angeles Times, 180
lost, what is, 112–15
Luminate, 155

Ma, Jack, 198
MacKinnon, Rebecca, 196
Macron, Emmanuel, 40, 157, 192, 221
Made in China 2025, 198, 199
Madoff, Bernie, 94
Maex, Karen, 243
Magaziner, Ira, 32–33
Magna Carta for the web, 157
Mahama, John, 126
Mandiant (Google), 135, 226
Marjory Stoneman Douglas High School, 156
Markets in Crypto Assets regulation, 103
Markle, Meghan, 43
Martin, Ciaran, 81
Masnick, Mike, *Techdirt*, 148
mass shootings, 156
Maxar, 131
May, Tim, 23
Mbeki, Thabo, 119, 126
McCain, John, 35
McDowell, Robert M., 148
McKinsey & Company, 112
McMorris Rodgers, Cathy, 185
McNamee, Roger, 166
mercantilism, 200
MERCOSUR countries, 181
Merkel, Angela, 7
Meta, 57, 64, 95, 238
microchip supply chains, 52–53
microchips (semiconductors), 48, 49, 50–54, 190, 191
Microsoft: AI Now, 162; Blavatnik School of Government, 162; cyberattacks by Russia, 135; CyberPeace Institute, 161–62; Digital Geneva Convention, 162; Digital Peace Now, 162; email accounts, hacked by Chinese entities, 236; government contracts, value of, 233; international regulatory ecosystem, shaping, 172; lobbying, 159–60, 161–63; market capitalization, 41; Oxford Process on International Law Protections in Cyberspace, 162; Responsible AI Principles, 158; security breaches, 79–80; security business revenues, 79; software vulnerabilities, 70; Sydney (chatbot), 167; systemically important technology institution, 238; Ukraine war, 131; UN office, 159; undersea cables, 57; U.S. Department of Defense subcontracts, 29; water usage, data centers, 62

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Microsoft Azure, 62
Microsoft Research, 162
Miliband, David, 120
military-industrial complex, 109–10
Minecraft, 72–73
Mirai malware, 72–73
Mistral AI, 30
MIT Technology Review, 163
Mitchell, Paul, 159
Mitto, 71
Modderkolk, Huib, 7, 229
Modest Proposal, A (Swift), 166
Modi, Narendra, 178, 202
Mogherini, Federica, 119
MoneyGram, 89
monitoring and surveillance technology, 3–4
Moses, Beth, 90
Mozilla Foundation, 204
Msando, Chris, 123
Mubarak, Hosni, 2, 4
Multistakeholder Advisory Group, 159
Mumbai terrorist attacks (2008), 204
Musk, Elon: AI, for and against, 255; chatbots, regulation of, 168–69; content moderation council, 154; framing, leveraging, 148; Iran, 250; press attention, 228; Starlink, 9; Starlink, in Iran, 250; Twitter acquisition, 188; Ukraine Starlink offer, 130, 132; Ukraine war, political decision, 9; xAI, 255
Mwilu, Philomena, 127
Myanmar, 142

Nadella, Satya, 79, 171, 203
Nairobi, 119, 122, 200
Nakamoto, Satoshi, 94
Nakasone, Paul, 133
National AI Advisory Committee, 38–39
National Association of Criminal Defense Lawyers, 106
National Cyber Security Center (NCSC), 74, 85
National Intelligence Law (China), 175
National Telecommunications and Information Administration (NTIA), 188, 237
NATO, 137, 138
Navalny, Alexei, 116–17
Navalny's app, 117
Nerds in the Parliament, 86
net neutrality, 37, 148
Netflix effect, 43
Netherlands, 7, 58–59, 65, 97, 123, 128
Neumann, Linus, 86–87
New York Post, 105
New York Times: Biden, revocation of Section 230, 38; Cambridge Analytica Data Scandal, 141; Clearview AI, 103–4, 106; cryptocurrencies meltdown, 96; gray-area tactics, 136–37; Greyball, use of, 28; Sydney (chatbot), 167; Ursula von der Leyen, suing for message access, 230
New_Public, 244–45
NextGenerationEU, 184
Nigeria, 123, 128–29
Nightline, 97
Nixon, Richard, 146
Noble, Safiya, 155, 188
nodes (blockchain), 94
Nokia-Siemens Networks, 4
nondisclosure agreements, 150, 229
nongovernmental organizations (NGOs), 62
Noord-Holland, data centers, 65
North Korea, 72, 102, 186
NotPetya, 79
Novi (cryptocurrency payments wallet), 95
Novichok, 116
NSO Group, 40, 68–69, 81, 85, 229. *See also* Pegasus
NSO Group hit list, 5
Nyabola, Nanjala, 129, 200

Obama, Barack, 2, 6, 34–36, 45–46, 79
Obama administration, 5–6, 35, 36, 39–40
Observer, 141
Odinga, Raila, 127
Office of Technology Assessment, 238
One Internet (Global Commission on Internet Governance), 19
open source, 86, 113, 131
OpenAI, 164, 166, 169–71, 218
Oracle SaaS Cloud, 134
Oregonian, 61
Organisation for Economic Co-operation and Development (OECD), 230–31
Organization Designation Authorization, 154
Our Principles (Google), 158
outsourcing: Apple to China, 196; governmental functions, 8, 91, 112–13, 229–31; hacking, 85–86; integrating technology and, 87; Kenya elections, 124, 128, 185; public accountability extension, 230–31
outsourcing, cost of, 230–31
oversight, digital critical infrastructure, 65
Oversight Board (Facebook), 149–53, 154, 155
Oxford Process on International Law Protections in Cyberspace, 162

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Pai, Ajit, 37
Palantir, 26, 108–12
paper voting, 128
Pappas, Vanessa, 153–54
Paris Call for Trust and Security in Cyberspace, 157
Parscale, Brad, 142
pattern recognition, 164
PayPal, 26
Pegasus: the reveal, 5, 7; banning, 190; cell phone spyware, 69; FBI, purchase by, 220; overview, 5–6; public accountability extension, 229; revolving door, 40
Pegasus Papers, 221
Pegasus Project, 5
permissionless innovation, 219
Personal Democracy Forum, 244
Pfizer, 230
phishing, 70–71, 72, 134
Pichai, Sundar, 250
pinkwashing, 180
plausible deniability, 80, 211, 226
Plouffe, David, 39–40
Poland, 7, 10, 207
polder model, 58–59
Polder Networks (Meta), 59–60
polders, 58
Power, Samantha, 16
precautionary principle, 215–19
predictive policing services, 105, 106, 107
PredPol, 105, 107
Princess Ariane Wind Farm, 60
Principles for Trust and Transparency (IBM), 158
Privacy International, 111
privatized policing, 103–8
procurement contracts, 29, 169, 234
procurement requirements, 234–35
Project Osmium, 60
Proposition 22 (California), 160
proprietary black boxes, 129
proprietary data, 66, 82
proprietary digitized systems, 82, 112
proprietary networks, 82–83
proprietary products, 107
proprietary secrets, stealing, 194
proprietary software, 226
proprietary technologies, lack of access to, 219
proprietary technology stacks, 13, 113
Protect Our Future (super PAC), 99
public, the, prioritizing, 209–12; accountability mechanisms, 238–42; antidemocratic technologies and practices, 219–25; democracy's house, 213–15; digital public sphere, 243–48; lead by example, 232–38; precautionary principle, 215–19; transparency, 225–32
public accountability extension, 229–32
public attribution, 83, 84, 135
public interest, end of, 89–91; cryptocurrencies, 91–96; cryptocurrencies, crash of, 96–103; privatized policing, 103–8; public interest, threats to, 112–15; security state, segmenting the, 108–12
public interest, threats to, 112–15
Public Spaces, 245
public stack, 244–46
purchasing power, leverage, 233–36
Putin's Palace (Anti-Corruption Foundation), 116

Qatar, 110
Quartz news app, 196
Quran app, 196

Raimondo, Gina, 53, 236
ransomware, 72, 76–78
ransomware attacks, 82, 101–2
rare earth materials, 51–52, 196, 200, 201, 229
Rasiej, Andrew, 244
Read, Ben, 226
Real Facebook Oversight Board (RFOB), 155–56
red teams, 85
regulation-enforcement model, 246–47
Reich, Rob, 25; *System Error*, 22
Reid, Randal, 106
Reliance Jio, 205
Republicans, 30, 98, 129–30, 177, 189, 190
Resecurity, 74, 75
Responsible AI Principles (Microsoft), 158
Ressa, Maria, 155
Restricting the Emergence of Security Threats That Risk Information and Communications Technology Act (RESTRICT Act), 186
Rice, Condoleezza, 20, 40
rights and freedoms, erosion of, 112–15
RightsCon, 150
Robinhood, 96
Robinson, Rashad, 155, 188
Roe v. Wade, 221
Roose, Kevin, 167
Rossiello, Elizabeth, 90
Roszak, Matt, 90

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Rudd, Neil, 61

Russell, Stuart, 254

Russia: Anti-Corruption Foundation, 116; censorship, Navalny's app, 117; DarkSide affiliation, 77; *Putin's Palace*, 116; tech companies, intimidation of, 117; Ukraine, DDoS attacks against, 72; Ukraine energy grid, cyberattack on, 83; Ukraine invasion, 130–31, 132, 133, 135–36, 137–38; U.S. cross-border malware takedown, 136–37

Ruto, William, 120

Rutte, Mark, 230

R-Ventures, 90

Safe City technology, 195, 200

Safran (formerly Morpho), 123, 127, 128, 129

Sahami, Mehran, 25; *System Error*, 22

San Jose Water Company, 68

Sandberg, Sheryl, 145, 180; *Lean In*, 13, 180

Sarkozy, Nicolas, 144–45

Saudi spies (Twitter), 228

Schatz, Brian, 143

Schmidt, Eric, 30, 145, 162, 192

Schreckinger, Ben, 96

Schreinemacher, Liesje, 191

science, technology, engineering, and mathematics (STEM) workforce, 53, 191

Science and Technology Options Assessment, 238

Section 230 (CDA), 31–32, 38, 46

"Section 230 and the International Law of Facebook" (Chandler), 32

Securing Our Digital Future (*Foreign Policy* magazine), 161

Securities and Exchange Commission (SEC), 99, 188

security state, segmenting, 108–12

security vulnerabilities, 67–68

self-regulation, 153–55, 171–73. *See also* calls

Semiconductor Manufacturing International Corporation, 37

semiconductor manufacturing plants (fabs), 50

semiconductors, 48, 49, 50–54, 190, 191

Senate Committee on Homeland Security hearing, 167

Sequoia Capital, 98

Sherlock spyware, 44

Shield AI, 131

ShotSpotter, 105, 106

Signal (messaging app), 27

significant public power, 243–44

Silkroad (online black market), 101

Sinaloa Cartel, 101

Singapore, 63, 95–96

SK Hynix, 49

Smartmatic, 129–30

Smith, Brad, 161–62

Smith, Travis, 60

Smithsonian magazine, 76

Snowden, Edward, 36, 44

social engineering, 71

social media: AI applications, classification, 209–10; authoritarian regimes, 3; Biden, 38; Chris Msando (Kenya), 124; content moderation practices, 156; foreign influence on, 186; Green Movement (Iran), 2–3, 239; Obama, 34; Oversight Board, 153; political campaigns, 142–43; politicians, 6, 148; private governance, 253; public political debate, 42; regulating, 148; Russia, 116–17; scrapers, 104; Trump, 36–38; VPNs, 74; Weibo, 195; xAI, 255. *See also* Oversight Board (Facebook); United States, regulating through national security

social media platforms: the battle, 3; companies mimic governments, 156; content moderation, 254; Facebook, controversial challenges, 153; the framers, 142–44; the global shift, 10; low-risk application (AI law), 209; Obama, 34–35; the reveal, 6; the revolving door, 42; Russia, 116–17; scrapers, 104; United States, 186–87; VPN, 74; the weaponization of everything, 68

SolarWinds, 79, 84

Sound Thinking (formerly PredPol), 105, 107

sovereign power, 131–32, 139

sovereignty, reclaiming, 174–78; China, 193–201; European Union, 178–85; India, 201–6; leadership, need for, 206–8; United States, 185–93

Space Norway, 55–56

SpaceX, 130, 131, 250

Spain, 7, 162, 198

Spotify, 33

spyware, 5–7, 190, 216, 220–21, 235. *See also* NSO Group; Pegasus

spyware abuse, 5–8

stack, the, 47–49; cable, 54–58; data centers, 58–65; definition of, 48; microchips, 50–54; oversight, insight to provide, 65–66; proprietary technology stacks, 113

Stanford University, 14, 19, 22, 67, 98, 151

Starlink, 9, 130, 250

For general queries, contact info@press.princeton.edu

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Starlink satellites, 9
State Service of Special Communications and Information Protection, 136
state sovereignty, challenge to, 132
state sovereignty, principle of, 131
state-sponsored threats, 133–34
Stikker, Marleen, 245
strategic ambiguity, 138
Strava, 81
Study the Strong Country (app), 195
Stuxnet, 80
Subcommittee on Human Rights of the European Parliament, 4
Suleyman, Mustafa, 114
superforecasters, 217
superregulator, 182
surveillance, 7, 23, 36, 44, 108. *See also* Pegasus; virtual private network (VPN)
surveillance cameras, 68
surveillance programs (G. W. Bush), 34
surveillance state. *See* China, building the surveillance state
surveillance technology, 3, 4, 5, 250. *See also* Clearview
surveillance tools, 6
Swift, Jonathan, 164
Sydney (chatbot), 167
synthetic media, 210–11, 226
Syria, 3, 4
System Error (Reich, Sahami and Weinstein), 25
systemically important financial institutions, 238

Taghi, Ridouan, 7
Taiwan, 50, 51–52
Taiwan Semiconductor Manufacturing Company (TSMC), 51
Takagi, Koichiro, 167–68
Tapscott, Alex, 90; *Blockchain Revolution*, 90
Tapscott, Don, 90; *Blockchain Revolution*, 90
targeted regulations, 147
TaskRabbit, 165
Tay (chatbot), 165
tech companies: accountability mechanisms, 239; artificial intelligence, who rules, 165; the code, 19–46; code of practice (hate speech online), 156–57; companies mimic governments, 156–57; data centers, 61, 63; democracy, save, 250–51; the framers, 144; the gap, 88; global shift, 8–12; international conventions, abiding by, 132; precautionary principle, 217, 222; prioritizing the public, 212; privatized policing, 107; public accountability extension, 230; public interest, threats to, 113; purchasing power, leverage, 233–35; self-regulation, 171–73; sovereignty, reclaiming, 174–208; spinning game, 146, 148–49; the state, outmaneuvering, 159–61, 163; tech on the front lines, 116–18, 130–39; technology regulation, 189; transparency, 228, 229
tech coup, reversing, 251–53
Tech for Good Call, 157
Tech for Good initiative, 158
Tech for Good Summit, 143
tech governance, laissez-faire approach to, 30–39
tech industry: Biden administration, 38–39; G. W. Bush administration, 33–34; lobbying, 160; market size, 41–42; Obama administration, 34–36; the pioneers, 22–26; political campaigns, 41; self-regulation, 149–58, 171–73; sovereignty, reclaiming, 174–208; transparency, lack of, 225–32; Trump administration, 36–38. *See also* lobbying
Tech Inquiry, 28
tech on the front lines, 116–19; Kenya, tech, trust, elections, 119–30; technology on the front lines, 130–39
tech regulation, 181–82, 187, 188–91, 201, 203–4
Tech4Democracy, 162
TechCrunch, 158
Techdirt (Masnick), 148
technological expert services, create, 236–38
technology expertise, leaking of, 40
technology governance, 11, 172, 207, 241–42, 252
Terra/Luna, 100
Tesla, 9, 41, 211
test corpus, 164
Thiel, Peter, 26, 40, 43, 109
Thorning-Schmidt, Helle, 153
Threads, 184
Threat Analysis Group (Google), 134
threats to the public interest, 112–15
TikTok, 37, 43, 153–54, 185–87, 250
Tiwari, Udbhav, 204
Ton-That, Hoan, 104
trademark protections, 231–32
Transatlantic Commission on Election Integrity, 151

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Transmission Control Protocol / Internet Protocol (TCP/ IP), 22
transparency, 225–26; artificial intelligence, identify, 226–27; CO_2 footprint, 235; commercial software, 107; cryptocurrencies, 100; investment and bids, 228–29; lack of, 66; Palantir, 111; predictive policing, 107; public accountability extension, 229–32
Treaty of the European Union, article 191, 217
Tree of Life Synagogue, 156
Trump, Donald: Cambridge Analytica, 140, 141; Defend Forward strategy, 137; Facebook suspension, 153; Palantir (ICE), 108; social media, use of, 36–38; tech companies, regulating, 36–38; TikTok, attempt to ban, 186
Tulip (subsidiary of Meta), 59–60
Tunisia, 2–3, 207
2020 U.S. presidential election, 128, 130, 155, 211
Twitter (now known as X), 2–9; artificial intelligence, 165; the battleground, 79; China, 197; companies mimic governments, 154, 156–57; content moderation council, 154; the corporates, 27; India, 204; investments and bids, transparency of, 228; name change, 228; privatized policing, 104; the public, prioritizing, 211; the stack, 48; United States, 186–87, 188
Twitter revolution, 2

Uber, 24–25, 27–28, 95
U.K. National Cyber Security Center, 81
U.K. National Health Service, 110
Ukraine, Russian invasion of, 83, 130–31, 132, 133, 135–38
UN Charter, 131, 132
UN High-Level Panel on Technology, 159
UN Human Rights Office, 159
UN Internet Governance Forum, 159, 241–42
UN Sustainable Development Goals, 159
uniform charging outlet, 183
United Kingdom, 54, 55, 107, 110, 140, 155
United Nations Advisory Body on Artificial Intelligence, 241
United Nations Development Programme, 123
United Nations (UN), 114, 133, 159, 203, 241–42
United States: the battle, 7, 11, 15; the code, 21–22, 30, 32, 35–36, 37; end of public interest, 99, 103, 105, 109, 110; the framers, 155, 167–68; prioritizing the public, 216, 220, 230, 232, 235, 242; reclaiming sovereignty, 185–94, 197, 199, 206, 208; regulating through national security, 185–86, 187–90, 190–93; the stack, 36, 51–53, 54, 62; tech on the front lines, 133, 136–38; the weaponization of everything, 72, 78, 88
U.S. Army, 109
U.S. Census Bureau, 74
U.S. Central Intelligence Agency, 109
U.S. Chamber of Commerce, 168–69
U.S. CHIPS and Science Act, 53
U.S. CLOUD Act, 175
U.S. cross-border malware takedown, 136–37
U.S. Cyber Command, 69, 133
U.S. Department of Commerce, 37, 191
U.S. Department of Defense, 29, 79, 109, 137, 211, 233
U.S. Department of Justice, 28, 77, 90, 99, 105
U.S. Department of Transportation, 147
U.S. Digital Service, 238
U.S. Drug Enforcement Administration, Big Tech contracts, 29
U.S. Federal Communications Commission, 182
U.S. federal government, 83, 160, 233
U.S. Food and Drug Administration (FDA), 109, 209
U.S. GDP, 41, 231
U.S. House of Representatives' Energy and Commerce Committee, 185
U.S. National Security Agency (NSA), 69, 80, 236
U.S. presidential elections, 130, 140, 211
U.S. Senate hearing (Zuckerberg), 142–43
U.S. Senate Judiciary Committee, 254
U.S. Space Force, 29
U.S. Special Forces, 109
U.S. Supreme Court, 31, 81, 189, 221
U.S. tech companies, 116–17, 206, 207
Usenet, 23
Uyghur Muslim minority, 11, 195

Vance, J. D., 186
Van Overtveldt, Johan, 225
Vattenfall, 60
very large online platforms (designation), 239
very large online search engines (designation), 239
Victoria (queen), 54, 180
Village Capital, 44
virtual private network (VPN), 74–75
Visa, 95

© Copyright, Princeton University Press. No part of this book may be distributed, posted, or reproduced in any form by digital or mechanical means without prior written permission of the publisher.

Vodafone, 205
Volkswagen, tampering with emissions software, 16
Von der Leyen, Ursula, 53
Voyager Digital, 100
vulnerabilities, 70

Wales, Jimmy, 145
Walker, Kent, 20
Wall Street Journal, 100, 177
Walmart (El Paso, Texas), 156
Walton, Bill, 73
WannaCry, 79
war crimes, 120, 132, 136
warrantless wiretapping, 34
Warren, Elizabeth, 38, 222, 255
Washington, George, 91
Washington Post, 148
water usage, data centers, 61–62
Waxahachie Daily Light, 60
weaponization of everything, the, 67–69; the arsenal, 69–73; the battleground, 78–86; the dark side, 76–78; the gap, 86–88; the impact, 73–75
WeChat, 198
Weibo, 195, 198
Weinstein, Jeremy, 25; *System Error*, 22
Wennink, Peter, 191
West Virginia v. EPA, 189
Western Union, 89
WhatsApp, 13, 143, 230
Wheeler, Tom, 182
Whetstone, Rachel, 20
white hat hackers, 85, 86, 129
White House Office of Science and Technology Policy, 162; *Blueprint for an AI Bill of Rights*, 157
Whittaker, Meredith, 87–88
Wiebes, Eric, 59
Williams, Michael, 106
Wirecard, 235
World Bank, 95, 123, 203
World Wide Web, 22, 23, 31
Worldcoin, 10, 223
Wozniak, Steve, 168
Wu, Tim, 38; *The Curse of Bigness*, 38
Wyden, Ron, 31–32, 236; Section 230, influence of, 46
Wylie, Christopher, 140–41

X (formerly Twitter). *See* Twitter (now known as X)
xAI, 255
Xi Jinping, 195, 197, 199–200

Yahoo, 13–14
Yassaee, Fariba, 150–51
Yellen, Janet, 192
YouTube: Children's Online Privacy Protection Act, 147; code of practice, 156–57; Marjory Stoneman Douglas High School attack, 156; mass shootings, 156; protests, Iranian, 2; *Putin's Palace*, 116; scrapers, used by, 104; takedown requests (India), 204–5; technology on the front lines, 134, 227

"Zan. Zendegi. Azadi." (Woman. Life. Freedom.), 250
Zeewolde hyperscale data center, 59–60, 60–61, 64
Zelenskyy, Volodymyr, 226
zero-click attacks, 5
zero-day vulnerabilities, 69–70, 76, 85
zero days, 69–70, 82, 85
Zero Trust, 233–34
zero-trust network architecture, 190
Zhao, Changpeng, 99, 225
Zhdanov, Ivan, 117
Zhora, Victor, 136
ZTE, 177, 199, 200
Zuboff, Shoshana, 155, 214
Zuckerberg, Mark, 26–27, 95, 142–44, 145, 150
Zuckerman, Ethan, 245

For general queries, contact info@press.princeton.edu